NEC

GVT-070000-001-00 1.32

QX-W2230AC アクセスコントローラ

コマンドマニュアル

改版履歴

版数	日付	改版内容
1.0	2018/08	初版発行
1.1	2018/12	・「02-WLAN」の「1 章 AP 管理」に以下のコマンドを追加しました。 ・**bridge-aggregation** ・**port-isolate enable** ・**port link-aggregation group** ・**remote-configuration synchronize** ・「02-WLAN」の「3 章 WLAN アクセスの設定」に **wlan nas-port-id format** コマンドを追加しました。 ・「02-WLAN」の「5 章 WLAN 認証」に以下のコマンドを追加しました。 ・**client-security accounting-start trigger** ・**client-security accounting-delay time** ・**client-security accounting-update trigger** ・「02-WLAN」の「5 章 WLAN 認証」から **client-security ignore-authentication** コマンドを削除しました。 ・「02-WLAN」に「16 章　WLAN 最適化」を追加しました。 ・誤記訂正
1.2	2019/02	・「01-はじめに」の「7 章 ソフトウェア管理」の **boot-loader file** コマンドのパラメータを修正しました。 ・「02-WLAN」の「5 章 WLAN 認証」の以下のコマンドに **mac-and-dot1x** パラメータを追加しました。 ・**client-security authentication-mode** ・誤記訂正

1.3	2019/08	・「01-はじめに」の「11 章 ライセンス管理」の下記のコマンドに関する注意事項を追加しました。 ・**license activation-file uninstall** ・「02.-WLAN」の「2 章 無線管理の設定」の下記のコマンドに関するメモを削除しました。 ・**mu-txbf** ・**su-txbf** ・「02-WLAN」の「6 章 WIDS の設定」の下記のコマンドに関するパラメータを修正しました。 ・**ap-timer** ・**client-timer** ・「02-WLAN」の「16 章 WLAN 最適化」に以下のコマンドを追加しました。 ・**option client hide-node-protection**
1.4	2020/01	・「01-はじめに」の「7 章 ソフトウェアのアップグレード」の下記コマンドに関する注意事項を追記しました。 ・**boot-loader file** ・「02-WLAN」の「1 章 AP 管理」の以下のコマンドに関するメモ書きを追加・修正しました。 ・**bridge-aggregation** ・**port access vlan** ・**port hybrid pvid** ・**port hybrid vlan** ・**port-isolate enable** ・**port link-aggregation group** ・**port link-type** ・**port trunk permit vlan** ・**port trunk pvid** ・**vlan** ・「02-WLAN」の「1 章 AP 管理」に以下のコマンドを追加しました。 ・**qos priority** ・**qos trust** ・「02-WLAN」の「1 章 AP 管理」の以下のコマンドの説明を見直し、デフォルト状態を修正しました。 ・**wlan detect-anomaly enable**

		・「02-WLAN」の「4 章 WLAN セキュリティ」の以下のコマンドに関するパラメータを追加しました。 **・cipher-suite** ・「02-WLAN」の「4 章 WLAN セキュリティ」に以下のコマンドを追加しました。 **・wps3** ・「02-WLAN」の「5 章 WLAN 認証」に以下のコマンドを追加しました。 **・fail-permit template** ・「02-WLAN」の「6 章 WIPS の設定」に以下のコマンドを追加しました。 **・apply countermeasure policy** **・countermeasure adhoc** **・countermeasure attack all** **・countermeasure attack deauth-broadcast** **・countermeasure attack disassoc-broadcast** **・countermeasure attack honeypot-ap** **・countermeasure attack hotspot-attack** **・countermeasure attack ht-40-mhz-intolerance** **・countermeasure attack malformed-packet** **・countermeasure attack man-in-the-middle** **・countermeasure attack omerta** **・countermeasure attack power-save** **・countermeasure attack soft-ap** **・countermeasure attack unencrypted-trust-client** **・countermeasure attack weak-iv** **・countermeasure attack windows-bridge** **・countermeasure external-ap** **・countermeasure mac-address** **・countermeasure misassociation-client** **・countermeasure misconfigured-ap** **・countermeasure policy** **・countermeasure potential-authorized-ap** **・countermeasure potential-external-ap**

		・**countermeasure potential-rogue-ap** ・**countermeasure rogue-ap** ・**countermeasure unauthorized-client** ・**countermeasure uncategorized-ap** ・**countermeasure uncategorized-client** ・**display wips virtual-security-domain countermeasure record** ・**reset wips virtual-security-domain countermeasure record** ・**select sensor all** ・「02-WLAN」の「8 章 WLAN ローミングの設定」に以下のコマンドを追加しました。 ・**ft enable** ・**ft method** ・**ft reassociation-timeout** ・「02-WLAN」の「13 章 WLAN 高可用性の設定」に以下のコマンドを追加しました。 ・**ap-license-synchronization enable** ・**display wlan ap-license-group** ・**local ip** ・**member ip** ・**proirity** ・**wlan ap-license-group** ・「12-IRF スタック」の「1 章 IRF スタック」に以下のコマンドを追加しました。 ・**wlan ap-backup hot-backup enable global** ・**wlan client-backup hot-backup enable**

1.5	2020/08	・「01-はじめに」に「2 章 RBAC」を追加しました。 ・「02-WLAN」の「1 章 AP 管理」に以下のコマンドを追加しました。 **・data-tunnel encryption** **・tunnel encryption** ・「02-WLAN」の「3 章 WLAN アクセスの設定」の以下のコマンドの説明を修正しました。 **・client forwarding-location** ・「02-WLAN」の「5 章 WLAN 認証」の以下のコマンドのパラメータを一部削除しました。 **・client-security authentication location** ・「02-WLAN」の「5 章 WLAN 認証」に以下のコマンドを追加しました。 **・fail-permit enable** **・radius-server test-profile** ・「02-WLAN」の「5 章 WLAN 認証」の以下のコマンドの説明を追加しました。 **・fail-permit template** ・「16 章 WLAN RRM」の以下のコマンドのパラメータの設定値を拡張しました。 **・calibrate-power min** ・「02-WLAN」に「17 章 WLAN 無線ロードバランス」を追加しました。 ・「02-WLAN」に「18 章 WLAN メッシュの設定」を追加しました。 ・「11-システム管理」に「11 章 NetMeister」を追加しました。 ・誤記訂正

1.6	2020/11	・「02-WLAN」の「2 章 無線管理の設定」の下記コマンドにパラメータを追加しました。 **・type** ・「02-WLAN」の「2 章 無線管理の設定」に以下のコマンドを追加しました。 **・dot11ax mandatory maximum-nss** **・dot11ax multicast-nss** **・client dot11ax-only** ・「02-WLAN」の「3 章 WLAN セキュリティ」に以下のコマンドを追加しました。 **・enhanced-open enable** **・enhanced-open transition-mode service-template** ・「02-WLAN」の「5 章 WLAN 認証」の以下のコマンドのパラメータを追加しました。 **・client-security authentication location** ・「11-システム管理」の「11 章 NetMeister」に以下のコマンドを追加しました。 **・netmeister proxy** ・誤記訂正
1.7	2020/12	・「02-WLAN」の「7 章 WLAN QoS の設定」に下記のコマンドに関する説明を追加しました。 **・client-rate-limit enable** ・誤記訂正

1.8	2021/05	・「02-WLAN」の「1 章 AP 管理」の下記コマンドの説明を一部削除しました。 **・reset wlan ap** ・「02-WLAN」の「1 章 AP 管理」の下記コマンドのデフォルト値を変更しました。 **・wlan tcp mss** ・「02-WLAN」の「2 章 無線管理の設定」に下記コマンドを追加しました。 **・bss-color** **・dl-ofdma** **・twt negotiate** **・ul-ofdma** ・「02-WLAN」の「2 章 無線管理の設定」の下記コマンドのデフォルト状態を変更しました。 **・mu-txbf** **・su-txbf** ・「02-WLAN」の「7 章 WLAN QoS の設定」に下記コマンドを追加しました。 **・u-apsd enable**
1.9	2021/06	・「02-WLAN」の「1 章 AP 管理」の下記コマンドの注意書きを追記しました。 **・remote-configuration synchronize** ・「02-WLAN」の「2 章 無線管理の設定」の下記コマンドの装置ごとのデフォルト値を追記し、QX-W1100 シリーズの Radio3 に関するメモ書きと QX-W1120 のメモ書きを追加しました。 **・type** ・「02-WLAN」の「11 章 チャネルスキャンの設定」の下記コマンドのデフォルト値を変更しました。 **・scan max-service-time** ・「02-WLAN」の「14 章 WLAN RRM」の下記コマンドのデフォルト値を変更しました。 **・wlan rrm calibration-channel interval** ・「02-WLAN」の「18 章 WLAN メッシュの設定」の下記コマンドのパラメータを一部削除しました。 **・display wlan mesh-link ap** ・「05- IP サービス」に「13 章 NAT」を追加しました。 ・誤記訂正

1.10	2021/09	・「01-はじめに」の「12 章 ライセンス管理」の下記コマンドにパラメータを追加しました。 **・display license** **・display license device-id** **・license activation-file install** **・license activation-file uninstall** **・license compress** ・「02-WLAN」の「1 章 AP 管理」の下記コマンドにメモ書きを追加し、バージョンごとの書式を記載しました。 **・display wlan ap connection record** **・display wlan ap files** **・display wlan ap online-time** **・display wlan ap reboot-log** **・display wlan ap running-configuration** **・display wlan tunnel latency ap name** ・「02-WLAN」の「1 章 AP 管理」に下記コマンドを追加しました。 **・wlan timezone-sync enable** ・「02-WLAN」の「2 章 無線管理の設定」の下記コマンドのパラメータの設定範囲を追記しました。 **・max-power** ・「02- WLAN」の「3 章 WLAN アクセスの設定」に下記コマンドを追加しました。 **・display wlan bss** ・「02- WLAN」の「3 章 WLAN アクセスの設定」の下記コマンドのパラメータの説明を見直しました。また、使用可能な特殊文字を記載しました。 **・ssid** ・「02- WLAN」の「4 章 WLAN セキュリティ」の下記コマンドにメモ書きを追加しました。 **・pmf** ・「02-WLAN」の「5 章 WLAN 認証」に下記コマンドを追加しました。 **・mac-authentication fast-connect enable** ・「02-WLAN」の「4 章 WLAN セキュリティ」の下記コマンドのメモ書きにメモを追加しました。また、説明の内容を見直しました。 **・wpa3**

		・「02-WLAN」の「14 章 WLAN RRM」の下記コマンドの説明を一部見直しました。 **・display wlan rrm-history ap** ・「04-アクセス」の「2 章 リンクアグリゲーション」の下記コマンドのデフォルト値及びパラメータの設定範囲を修正しました。 **・link-aggregation selected-port maximum** ・「04-アクセス」の「2 章 リンクアグリゲーション」の下記コマンドのパラメータの設定範囲を修正しました。 **・port link-aggregation group** ・「05-IP サービス」の「3 章 proxy ARP」の下記コマンドの説明を一部見直しました。 **・local-proxy-arp enable** ・「09-セキュリティ」に「4 章 パスワード管理」を追加しました。 ・誤記訂正
1.11	2021/11	・「02-WLAN」の「1 章 AP 管理」の下記コマンドのメモ書きの内容を見直しました。 **・remote-configuration** ・「02-WLAN」の「1 章 AP 管理」の下記コマンドの説明を修正しました。 **・wlan timezone-sync enable** ・「02-WLAN」の「3 章 WLAN アクセスの設定」の下記コマンドにメモ書きを追加しました。 **・map-configuration** ・「02- WLAN」の「7 章 WLAN QoS の設定」に下記コマンドを追加しました。 **・atf**
1.12	2021/11	・「02-WLAN」の「5 章 WLAN 認証」に「Web 認証(ポータル認証)設定コマンド」を追加しました。 ・「02-WLAN」の「8 章 WLAN ローミングの設定」に下記コマンドを追加しました **・bss transition-management disassociation** **・bss transition-management enable** **・sacp anti-sticky**

1.13	2021/12	・「01-はじめに」の「9 章 装置管理」に下記コマンドを追加しました。 **・diag boot-info display** ・「02-WLAN」の「2 章 AP 管理」に下記コマンドを追加しました。 **・display wlan ap reboot-record** ・「02-WLAN」の「2 章 無線管理の設定」の下記コマンドのデフォルト値を修正しました。 **・type** ・「02-WLAN」の「2 章 無線管理の設定」の下記コマンドのパラメータを修正しました。 **・display wlan ap continuous-mode** **・display wlan ap radio** ・「02-WLAN」の「2 章 無線管理の設定」に下記コマンドを追加しました。 **・display wlan statistics ap radio** ・「02-WLAN」の「2 章 無線管理の設定」の下記コマンドを削除しました。 **・display wlan ap radio statistics** **・reset wlan ap radio statistics** ・「02-WLAN」の「3 章 WLAN アクセスの設定」の下記コマンドの説明を修正しました。 **・display wlan client**
1.14	2022/02	・「02-WLAN」の「16 章 WLAN 最適化」に下記コマンドを追加しました。 **・rrop anti-bmc rate-limit** **・rrop anti-bmc rate-limit pps**

1.15	2022/03	・「02-WLAN」の「1 章 AP 管理」に下記コマンドを追加しました。 **・display wlan ap diagnostic-information** ・「02-WLAN」の「1 章 AP 管理」に下記コマンドにメモ書きを追加しました。 **・data-tunnel encryption** ・「02-WLAN」の「2 章 無線管理の設定」の下記コマンドの出力結果説明文を更新しました。 **・display wlan statistics ap radio** ・「02-WLAN」の「3 章 WLAN アクセスの設定」の下記コマンドのデフォルト値と設定可能な値の範囲を修正しました。 **・client max-count** ・「02-WLAN」の「4 章 WLAN セキュリティ」の下記コマンドのメモ書きに、KDF の設定に関する記述を追記しました。 **・pmf** ・「02-WLAN」の「5 章 WLAN 認証」の下記コマンドのデフォルト値と設定可能な値の範囲を修正しました。 **・dot1x max-user** **・mac-authentication max-user** ・「02-WLAN」の「8 章 WLAN ローミングの設定」の WLAN 802.11v コマンドのメモ書きの誤記を修正しました。 ・「02-WLAN」の「12 章 バンドナビゲーションの設定」の下記コマンドの説明を修正しました。 **・wlan band-navigation balance access-denial** ・「02-WLAN」の「WLAN RRM」の下記コマンドのデフォルト値を記載しました。 **・interference-threshold** ・「02-WLAN」の「16 章 WLAN 最適化」に下記コマンドを追加しました。 **・rrop anti-bmc network** ・「02-WLAN」の「17 章 WLAN ロードバランス」に下記コマンドを追加しました。 **・radio-load-balance band-navigation enable** ・誤記修正

1.16	2022/05	・「02-WLAN」の「1 章 AP 管理」の下記コマンドの出力説明に内容を追記しました。 **・display wlan ap** ・「02-WLAN」の「1 章 AP 管理」の下記コマンドのパラメータ説明に、指定可能な AP モデルの表を追加しました。 **・ap-model** **・wlan ap** ・「2 章 無線管理の設定」に下記コマンドを追加しました。 **・reset wlan statistics ap radio** ・「2 章 無線管理の設定」の下記コマンドの説明に QX-W1110 の情報を追記しました。 **・max-power** **・type** ・「02-WLAN」の「4 章 WLAN セキュリティ」の下記コマンドに QX-W1100 シリーズでの gcmp パラメータのサポートに関するメモ書きを追記しました。 **・cipher-suite** ・「02-WLAN」の「4 章 WLAN セキュリティ」下記コマンドに QX-W1100 シリーズでの WPA3 エンタープライズ 192bit セキュリティモードのサポートに関するメモ書きを追記しました。 **・wpa3** ・「02-WLAN」の「5 章 WLAN 認証」下記コマンドに最大接続数制限の動作に関するメモ書きを追加しました。 **・dot1x max-user** **・mac-authentication max-user** ・「02-WLAN」の「10 章 WLAN 無線リソース計測の設定」の下記コマンドに **spectrum**、**tpc** パラメータを追加しました。 **・measure** ・「02-WLAN」の「14 章 WLAN RRM」に下記コマンドを追加しました。 **・calibrate-bandwidth self-decisive** **・wlan rrm calibration-bandwidth interval** ・「09- セキュリティ」の「3 章 MAC アドレス認証」に下記コマンドを追加しました。 **・mac-authentication authentication-method** ・「09- セキュリティ」の「11 章 ユーザアイソレーション」の下記コマンドの説明に、登録可能な MAC アドレス数上限に関する記述を追記しました。 **・user-isolation vlan permit-mac**

		・「11- システム管理」の「11 章 NetMeister」に下記コマンドを追記しました。 ・**netmeister mode** ・**netmeister parent-mode mqtt port** ・**netmeister parent-mode sitename** ・「11- システム管理」の「11 章 NetMeister」 下記コマンドの出力例を更新しました。 ・**display netmeister** ・「11- システム管理」 の「11 章 NetMeister」下記コマンドの説明を見直しました。 ・**netmeister account** ・**netmeister parent ip** ・誤記修正
1.17	2022/06	・「02-WLAN」の「1 章 AP 管理」の下記コマンドに **apid** のパラメータを追加しました。 ・**display wlan ap** ・「02-WLAN」の「2 章 無線管理の設定」 下記コマンドのデフォルト値の記載を変更しました。 ・**bss-color** ・**dl-ofdma** ・**twt negotiate** ・**ul-ofdma** ・「02-WLAN」の「8 章 WLAN ローミングの設定」に下記コマンドを追加しました。 ・**ft mobility-domain-id** ・「09 – セキュリティ」の「1 章 AAA」 に下記コマンドを追加しました。 ・**description** ・「09- セキュリティ」の「1 章 AAA」 下記コマンドに test-profile のパラメータを追加しました。 ・**primary authentication** ・**secondary authentication** ・「11-システム管理」の「11 章 NetMeister」 に下記コマンドを追加しました。 ・**netmeister event log enable** ・誤記修正

1.18	2022/09	・「02-WLAN」の「1 章 AP 管理」に下記コマンドを追加しました。 ・**wlan ap-image-deploy** ・**wlan image-load filepath** ・「02-WLAN」の「2 章 無線管理の設定」に下記コマンドを追加しました。 ・**channel-usage threshold** ・「02-WLAN」の「3 章 WLAN アクセスの設定」に下記コマンドを追加しました。 ・**display wlan client failure** ・**user-profile** ・**wlan client failure history aging** ・**wlan permit-ssid** ・「02-WLAN」の「5 章 WLAN 認証」の下記コマンドに 802.1X 認証での失敗許可機能に関する説明を追加しました。 ・**fail-permit template** ・「02-WLAN」の「8 章 WLAN ローミングの設定」に下記コマンドを追加しました。 ・**authentication-mode** ・**display wlan mobility** ・**display wlan mobility group** ・**display wlan mobility roam-track mac-address** ・**group enable** ・**member ip** ・**source ip** ・**tunnel-type** ・**wlan mobility group** ・**wlan mobility-group-isolation enable** ・「08-ACL and QoS」の「2 章 QoS ポリシー」に下記コマンドを追加しました。 ・**qos apply policy global** ・「09-セキュリティ」に「13 章 ユーザプロファイル」を追加しました。 ・誤記訂正
1.19	2022/12	・「02-WLAN」の「1 章 AP 管理」に下記コマンドを追加しました。 ・**display wlan ap statistics image-download** ・「02-WLAN」の「1 章 AP 管理」 下記コマンドの undo 実行時の動作説明を修正しました。 ・**wlan tcp mss**

		・「02-WLAN」の「1 章 AP 管理」の下記コマンドは、QX-W シリーズでは使用しないため削除しました。 **・control address** **・control address enable** ・「02-WLAN」の「3 章 WLAN アクセスの設定」に下記コマンドを追加しました。 **・access-control acl** **・display wlan client device-information** ・「02-WLAN」の「4 章 WLAN セキュリティ」に下記コマンドを追加しました。 **・akm sae pwe** ・「02-WLAN」の「4 章 WLAN セキュリティ」 下記コマンドのデフォルト値を変更しました。 **・gtk-rekey enable** **・ptk-rekey enable** ・「02-WLAN」の「4 章 WLAN セキュリティ」 下記コマンドに WEP に関する重要事項を記載しました。 **・cipher-suite** **・wep key** **・wep key-id** **・wep mode dynamic** ・「02- WLAN」の「7 章 WLAN QoS の設定」に下記コマンドを追加しました。 **・mu-edca client** ・「02-WLAN」の「13 章 WLAN 高可用性の設定」の 下記コマンドの説明を見直しました。 **・wlan tunnel-preempt** ・「02-WLAN」の「14 章 WLAN RRM の設定」に下記コマンドを追加しました。 **・calibrate-power 2.4g max** **・calibrate-power 2.4g coverage rssi-threshold** **・calibrate-power 2.4g coverage weak-signal-client ratio** **・calibrate-power 2.4g coverage weak-signal-client threshold** **・calibrate-power 2.4g coverage weak-signal-packet ratio** **・calibrate-power 2.4g coverage weak-signal-packet threshold** **・calibrate-power 5g max** **・calibrate-power 5g coverage rssi-threshold** **・calibrate-power 5g coverage weak-signal-client ratio**

		・**calibrate-power 5g coverage weak-signal-client threshold** ・**calibrate-power 5g coverage weak-signal-packet ratio** ・**calibrate-power 5g coverage weak-signal-packet threshold** ・**calibrate-power coverage enable** ・「02-WLAN」に「19 章 コンフィグレーションプロファイルの設定」を追加しました。 ・「02-WLAN」に「20 章 IoT 機能の設定」を追加しました。 ・「05-IP サービス」の「6 章 DHCP サーバの設定」に下記コマンドを追加しました。 ・**class option group** ・**dhcp class** ・**dhcp option group** ・**if-match** ・「08-ACL and QoS」の「1 章 ACL」に下記コマンドを追加しました。 ・**packet-filter** ・誤記訂正
1.20	2023/04	・「01-はじめに」の「9 章 装置管理」に下記のコマンドを追加しました。 ・**temperature-limit** ・「02-WLAN」の「2 章 無線管理の設定」に下記のコマンドを追加しました。 ・**radio-type 2.4g** ・**radio-type 5g** ・「02-WLAN」の「2 章 無線管理の設定」の下記コマンドのデフォルト値を変更しました。 ・**mu-txbf** ・**su-txbf** ・「02-WLAN」の「3 章 WLAN アクセスの設定」の下記コマンドの名称を変更しました。 (変更前) ・**display wlan statistics** (変更後) ・**display wlan statistics (v7.1.13 以前)** ・「02-WLAN」の「3 章 WLAN アクセスの設定」に下記コマンドを追加しました。 ・**display wlan statistics client** ・**display wlan statistics connect-history** ・**display wlan statistics service-template**

		・dot11ax support maximum-he-mcs **・reset wlan statistics service-template・** 「02-WLAN」の「14 章 WLAN RRM」に下記コマンドを追加しました。 **・calibrate-channel channel-set-optimization** **・calibrate-channel channel-set-optimization neighbor-threshold** **・calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent** **・calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent-per-set** **・calibrate-channel 2.4g channel-set-optimization enable** **・calibrate-channel 2.4g channel-set-optimization neighbor-threshold** **・calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent** **・calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent-per-set** ・「02-WLAN」の「22 章 IoT 機能の設定」に下記コマンドを追加しました。 **・display iot transport-profile** **・filter rssi threshold** **・filter rssi-fluctuation threshold** **・filter recent-packet duration** **・filter highest-rssi** ・「05-IP サービス」の「2 章 Gratuitous ARP」に下記コマンドを追加しました。 **・gratuitous-arp mac-change retransmit** ・「08-ACL and QoS」の「1 章 ACL」の下記コマンドの名称を変更しました。 (変更前) **・packet-filter** (変更後) **・packet-filter (Interface view)** ・「08-ACL and QoS」の「1 章 ACL」に下記コマンドを追加しました。 **・packet-filter (service template view)** ・「09-セキュリティ」の「1 章 AAA」に下記コマンドを追加しました。 **・nas-id** ・「11-システム管理」の「11 章 NetMeister」に下記コマンドを追加しました。 **・netmeister alarm enable notice**

		・**netmeister management ip** ・「12-IRF スタック」の「1 章 IRF スタック」に下記コマンドを追加しました。 ・**wlan client-backup hot-backup delay**
1.21	2023/06	・「01-はじめに」の「2 章 RBAC」 下記コマンドの **web-menu** パラメータをサポートしました。 ・**rule** ・「01-はじめに」の「3 章 ログイン」に下記コマンドを追加しました。 ・**display web menu** ・「01-はじめに」の「9 章 装置管理」に下記コマンドを追加しました。 ・**locator blink** ・「01-はじめに」の「11 章 システム管理」に下記コマンドを追加しました。 ・**netmeister update** ・「02-WLAN」の「2 章 無線管理の設定」の下記コマンドの設定範囲を変更しました。 ・**max-power** ・「02-WLAN」の「2 章 無線管理の設定」の下記コマンドのデフォルト値を変更しました。 ・**mu-txbf** ・**su-txbf** ・「02-WLAN」の「3 章 WLAN アクセスの設定」に下記コマンドを追加しました。 ・**display wlan ap region-code** ・「02-WLAN」の「3 章 WLAN アクセスの設定」 下記コマンドの **vlan** パラメータは使用できないため削除しました。 ・**client forwarding-location** ・「02-WLAN」の「3 章 WLAN アクセスの設定」の下記コマンドの名称を変更しました。 (変更前) ・**display wlan region-code ap** (変更後) ・**display wlan region-code ap (v7.1.13 以前)** ・「02-WLAN」の「11 章 チャネルスキャンの設定」の下記コマンドは使用出来ないため削除しました。 ・**scan mode all** ・「02-WLAN」に「19 章 コンフィグレーションプロファイルの設定」の下記コマンドの Syntax に、”**acl number** *acl-number*”の形式を追加し

		ました。 ・**acl** ・「02-WLAN」の「22 章 IoT 機能の設定」に下記コマンドを追加しました。 ・**rfid-tracking aeroscout** ・**rfid-tracking aeroscout aggregate-report interval** ・**rfid-tracking aeroscout engine-address** ・**rfid-tracking aeroscout engine-detection** ・**rfid-tracking aeroscout report-mode** ・**rfid-tracking aeroscout tag-multicast-address** ・**rfid-tracking aeroscout timestamp** ・**rfid-tracking aeroscout vendor-port** ・**rfid-tracking mode** ・**rfid-tracking radio** ・**display wlan rfid-tracking radio** ・**rfid-tracking client rate-limit** ・**rfid-tracking client rate-limit cir** ・**rfid-tracking dilution** ・**rfid-tracking dilution factor** ・**rfid-tracking ignore ap-frame** ・**rfid-tracking ignore beacon** ・**rfid-tracking keepalive** ・**rfid-tracking rate-limit** ・**rfid-tracking rate-limit cir** ・**rfid-tracking rssi** ・**rfid-tracking rssi threshold** ・「08-ACL and QoS」の「1 章 ACL」の下記コマンドの Syntax に、”**acl number** *acl-number*”の形式を追加しました。 ・**acl** ・「02-WLAN」に「21 章 Web リダイレクトの設定」を追加しました。 ・「09-セキュリティ」の「7 章 SSL」のコマンドが Web 認証(ポータル認証)と重複していたため削除しました。 ・誤記訂正
1.22	2024/01	・「01-はじめに」の「3 章 ログイン」に、下記コマンドを追加しました。 ・**telnet server port** ・「02-WLAN」の「1 章 AP 管理」に下記コマンドを追加しました。

		・**wlan save ap-configuration** ・「02-WLAN」の「2 章 無線管理の設定」の下記コマンドのレーダ検出時の説明を修正しました。 ・**channel** ・「02-WLAN」の「4 章 WLAN セキュリティ」の下記コマンドの **enterprise-only-mode** と **enterprise-transition-mode** のパラメータをサポートしました。 ・**wpa3** ・「02-WLAN」の「16 章 WLAN 最適化」に下記コマンドを追加しました。 ・**rrop client fast-keep-alive** ・「09-セキュリティ」の「6 章 SSH」に、下記コマンドを追加しました。 ・**ssh server port** ・「09-セキュリティ」に「7 章 PKI」を追加しました。 ・「09-セキュリティ」の「8 章 SSL」に、1.21 版で削除したコマンドと、下記のコマンドを追加しました。 ・**display ssl client-policy** ・**server-verify enable** ・**ssl client-policy** ・**version** ・「11-システム管理」の「9 章 Information center」の下記コマンドに SSL により暗号化した syslog 送信に必要なパラメータを追加しました。 ・**info-center loghost** ・「11-システム管理」の「11 章 NetMeister」に下記コマンドを追加しました。 ・**netmeister track** ・誤記訂正

1.23	2024/06	・「01-はじめに」の「9 章 装置管理」に下記コマンドを追加しました。 **・display maintain cpu-usage history process** ・「01-はじめに」の「9 章 装置管理」に下記コマンドにパラメータを追加しました。 **・locator blink** ・「02-WLAN」の「1 章 AP 管理」の下記コマンドのパラメータを修正しました。 **・ap-model** **・wlan-ap** ・「02-WLAN」の「2 章 無線管理の設定」に下記コマンドを追加しました。 **・dot11be mandatory maximum-nss** **・dot11be multicast-nss** **・dot11be support maximum-nss** **・mru** **・pre-puncture static** **・wlan out-band 6g-discovery enable** ・radar-channel-switchback disable ・「02-WLAN」の「2 章 無線管理の設定」に下記コマンドのデフォルト値を追記しました。 **・channel band-width** ・「02-WLAN」の「2 章 無線管理の設定」の下記コマンドに QX-W1240 のパラメータ設定範囲を追記しました。 **・max-power** ・「02-WLAN」の「2 章 無線管理の設定」の下記コマンドにパラメータと QX-W1240 のデフォルト値を追記しました。 **・type** ・「02-WLAN」の「3 章 WLAN アクセスの設定」に下記コマンドを追加しました。 **・display wlan client online-duration** ・「02-WLAN」の「7 章 WLAN QoS の設定」の下記コマンドにパラメータを追加しました。 **・wlan client-rate-limit** **・wlan max-bandwidth** ・「02-WLAN」の「14 章 WLAN RRM」の下記コマンドの Global Configuration view の Syntax にパラメータを追加しました。 **・calibrate-bandwidth self-decisive**

		・**calibrate-power coverage enable** ・「02-WLAN」の「14 章 WLAN RRM」の下記コマンドの Syntax を修正しました。 ・**calibrate-channel self-decisive** ・**calibrate-power self-decisive** ・「02-WLAN」の「14 章 WLAN RRM」の下記コマンドにパラメータを追加しました。 ・**wlan calibrate-channel pronto ap all** ・**wlan calibrate-power pronto ap all** ・「02-WLAN」の「14 章 WLAN RRM」に下記コマンドを追加しました。 ・**calibrate-power 6g max** ・**calibrate-power 6g coverage rssi-threshold** ・**calibrate-power 6g coverage weak-signal-client ratio** ・**calibrate-power 6g coverage weak-signal-client threshold** ・**calibrate-power 6g coverage weak-signal-packet ratio** ・**calibrate-power 6g coverage weak-signal-packet threshold** ・「02-WLAN」の「16 章 WLAN 最適化」に下記コマンドを追加しました。 ・**rrop anti-bmc upstream client-rate-limit** ・**rrop anti-bmc upstream client-rate-limit pps** ・「02-WLAN」に「22 章 Hotspot 2.0 の設定」を追加しました。 ・「04-アクセス」の「6 章 LLDP」の下記コマンドの表示結果（Port power classification）の説明を追記しました。 ・**display lldp local-information** ・「11-システム管理」の「4 章 SNMP」に下記コマンドを追加しました。 ・**simulate snmp-trap**
1.24	2024/06	・「02-WLAN」の「1 章 AP 管理」に下記コマンドを追加しました。 ・**power-level default** ・「02-WLAN」の「2 章 無線管理の設定」の下記コマンドのメモ書きを修正しました。 ・**bss-color** ・**dl-ofdma** ・**twt negotiate** ・**ul-ofdma**

		・「02-WLAN」の「4 章 WLAN セキュリティ」の下記コマンドに QX-W1240 に関するメモ書きを追記しました。 **・cipher-suite** **・wep key** **・wep key-id** **・wep mode dynamic** **・wpa3** ・「02-WLAN」の「5 章 WLAN 認証」の下記コマンドに QX-W1240 に関するメモ書きを追記しました。 **・dot1x max-user** **・mac-authentication max-user** ・「02-WLAN」の「7 章 WLAN QoS の設定」の下記コマンドに QX-W1240 に関するメモ書きを追記しました。 **・atf** **・mu-edca client** ・「02-WLAN」の「21 章 コンフィグレーションプロファイルの設定」の下記コマンドに QX-W1240 のデフォルト値を追記しました。 **・authentication-mode** **・set authentication password** **・telnet server enable**
1.25	2024/10	・「02-WLAN」の「1 章 AP 管理」に下記コマンドを追加しました。 **・display wlan ap group-name** ・「02-WLAN」の下記コマンドの **pass-phrase** の文字列で "?" の文字の使用をサポートしました。 **・preshared-key** ・「02-WLAN」の「4 章 WLAN セキュリティ」の下記コマンドの説明文を修正しました。 **・pmf association-comeback** ・「02-WLAN」の「7 章 WLAN QoS の設定」に下記コマンドを追加しました。 **・edca auto** ・「02-WLAN」の「15 章 WLAN IP スヌーピング」に下記コマンドを追加しました。 **・wlan client ip-conflict-detection enable** ・「02-WLAN」の「17 章 WLAN 無線ロードバランス」に下記コマンドを追加しました。 **・radio-load-balance band-navigation association-reject** ・誤記訂正

1.26	2024/11	・「02-WLAN」の「2 章 無線管理の設定」に下記コマンドを追加しました。 **・wlan in-band 6g-discovery** **・wlan multiple-bssid enable** ・「02-WLAN」の「3 章 WLAN アクセスの設定」の下記コマンドのデフォルト値を変更しました。 **・client idle-timeout** ・「02-WLAN」の「16 章 WLAN 最適化」に下記コマンドを追加しました。 **・sacp roam-optimize packet-loss-improve enable** ・「09-セキュリティ」の「12 章 ユーザアイソレーション」の下記コマンドで使用できるパラメータを追加しました。 **・display user-isolation statistics** ・誤記訂正
1.27	2024/11	・「02.WLAN」の「1 章 AP 管理」の下記のコマンドの説明を変更しました。 **・display wlan ap diagnostic-information** ・「09.セキュリティ」の「6 章 SSH」の下記のコマンドの説明を変更しました。 **・ssh user** ・「09.セキュリティ」の「7 章 PKI 設定」の下記のコマンドの説明を変更しました。 **・pki storage** ・「11.セキュリティ」の「7 章 プロセスモニタリングとメンテナンス」の下記のコマンドの説明を変更しました。 **・display exception context** ・「11.セキュリティ」の「9 章 Information cente」の下記のコマンドの説明を変更しました。 **・display logfile summary** **・info-center logfile directory**
1.28	2025/6	・「02.WLAN」の「4 章 WLAN セキュリティ」の下記コマンドに 6GHz 帯無線での WPA3 エンタープライズの 192bit セキュリティなしモード(**enterprise-only-mode**)の利用に関する記述を追記しました。 **・wpa3** ・「02.WLAN」の「8 章 WLAN ローミングの設定」の下記コマンドに v7.2.85a 以降のコマンド書式とコンフィグ引継ぎに関するメモ書きを追記しました。 **・sacp anti-sticky** ・「02.WLAN」の「8 章 WLAN ローミングの設定」に下記コマンドを

		追加しました。 ・**sacp anti-sticky forced-logoff** ・**sacp anti-sticky interval** ・**sacp anti-sticky rssi** ・「02.WLAN」の「14 章 WLAN RRM」に下記コマンドを追加しました。 ・**calibrate-channel track radar-detect enable** ・「02.WLAN」の「16 章 WLAN 最適化」 下記コマンドの **ipv4-and-ipv6-simple enable** パラメータと System-View への設定をサポートしました。 ・**rrop anti-bmc network** ・「02.WLAN」の「16 章 WLAN 最適化」に下記コマンドを追加しました。 ・**rrop arp ap-proxy-gateway enable** ・「02.WLAN」の「16 章 WLAN 最適化」の下記コマンドにローカル転送モードでの利用に関するメモ書きを追記しました。 ・**sacp roam-optimize packet-loss-improve enable** ・「02.WLAN」の「17 章 WLAN 無線ロードバランス」の下記コマンドの **unknown-capability** パラメータの設定範囲を変更しました。 ・**radio-load-balance band-navigation association-reject** ・「05.IP サービス」の「8 章 DHCP クライアント」に下記コマンドを追加しました。 ・**dhcp client user-defined request-list exclude** ・「05.IP サービス」の「11 章 DNS」に下記コマンドを追加しました。 ・**ip host interface** ・「11.システム管理」の「9 章 Information center」に下記のコマンドを追加しました。 ・i**nfo-center keep-alive custom-info** ・i**nfo-center keep-alive enable** ・i**nfo-center keep-alive interval** ・i**nfo-center keep-alive level**
1.29	2025/12	・QX-W1210/QX-W1230 の管理サポートに伴い、メモ書き内の QX-W1240 の型番記載を QX-W1200 シリーズに修正しました。 ・「01-はじめに」の「9 章 装置管理」に下記コマンドを追加しました。 ・**display environment** ・**restore factory-default**

		・**user-role** ・「02.WLAN」の「1 章 AP 管理」の下記コマンドに、QX-W1230 と QX-W1210 のパラメータを追加しました。 ・**ap-model** ・**wlan ap** ・「02.WLAN」の「1 章 AP 管理」の下記コマンドの AP グループに設定可能な最大ルール数の記述を更新しました。 ・**if-match ip** ・「02.WLAN」の「2 章 無線管理の設定」の下記コマンドで 320MHz 帯域幅モードの設定をサポートしました。 ・**channel band-width** ・「02.WLAN」の「2 章 無線管理の設定」の下記コマンドに QX-W1210/QX-W1230 のデフォルト値を追加しました。 ・**max-power** ・**type** ・「02WLAN」の「2 章 無線管理の設定」の下記コマンドの AP group Radio View での設定をサポートしました。 ・**mru** ・**pre-puncture static** ・「02.WLAN」の「5 章 WLAN 認証」の下記コマンドにパラメータを追加しました。 ・**radius-server test-profile** ・「02-WLAN」の「16 章 WLAN 最適化」に下記コマンドを追加しました。 ・**option keep-active** ・**rrop flow-schedule mode** ・「02.WLAN」の「16 章 WLAN 最適化」 下記コマンドのデフォルト値を変更しました。 ・**rrop arp ap-proxy-gateway enable** ・**rrop anti-bmc network** ・「02-WLAN」の「19 章 コンフィグレーションプロファイルの設定」のデフォルト値説明等に書かれている QX-W1240 の型番の記載を QX-W1200 シリーズに修正しました。 ・「02-WLAN」の「22 章 Hotspot 2.0 の設定」の下記コマンドは使用できない為削除しました。 ・**nai-realm config-order** ・「11.システム管理」の「11 章 NetMeister」に下記のコマンドを追加しました。 ・**netmeister event syslog enable** ・誤記訂正

1.30	2026/02	・「02-WLAN」の「1 章 AP 管理」の下記コマンドの設定例を修正しました。 **・display wlan ap** ・「02-WLAN」の「1 章 AP 管理」の下記コマンドのパラメータを修正しました。 **・led-mode** ・「02-WLAN」の「3 章 WLAN アクセスの設定」の下記コマンドの説明を修正しました。 **・region-code** ・「02-WLAN」の「4 章 WLAN セキュリティ」の下記コマンドにメモ欄を追記しました。 **・preshared-key** ・「02-WLAN」の「13 章 WLAN 高可用性の設定」の下記コマンドの説明を修正しました。 **・wlan tunnel-preempt** ・「02-WLAN」の「14 章 WLAN RRM」の下記コマンドの説明を修正しました。 **・tolerance-level** ・「04-アクセス」の「1 章 MAC アドレステーブル」の下記コマンドを削除しました。 **・display mac-address mac-move** **・mac-address notification mac-move** **・mac-address notification mac-move suppression (interface view)** **・mac-address notification mac-move suppression (system view)** ・「11-システム管理」の「11 章 Netmeiste」の下記コマンドの説明を修正しました。 **・netmeister alarm enable notice**
1.31	2026/07	・「01-はじめに」の「7 章 コンフィグレーションファイル管理」の下記コマンドに **by-section** のパラメータを追加しました。 **・display current-configuration** **・display saved-configuration** **・display this** ・「02-WLAN」の「3 章 WLAN アクセスの設定」の下記コマンドに 6GHz 無線に関する注記を追加しました。 **・beacon ssid-hide** ・「02-WLAN」の「3 章 WLAN アクセスの設定」に下記コマンドを追加しました。 **・display wlan client history-record mac-address** ・「02-WLAN」の「6 章 WIPS の設定」に、無線通信と WIPS センサの併用に関する説明を追加しました。

		・「02-WLAN」の「8 章 WLAN ローミングの設定」の以下のコマンドの説明を修正しました。 **・ft enable** ・「02-WLAN」の「8 章 WLAN ローミングの設定」について、以下のコマンドのメモ書きに WPA3 との併用に関する記述を追加しました。 **・ft enable** ・「セクション 02-WLAN」の「16 章 WLAN 最適化」の下記コマンドのメモを修正しました。 **・rrop client fast-keep-alive** ・「09-セキュリティ」の「1 章 AAA の設定」の下記コマンドに ap-ip のパラメータを追加しました。 **・nas-ip (RADIUS scheme view)** ・誤記訂正
1.32	2026/11	・「01-はじめに」の「1 章 CLI」に、下記コマンドを追加しました。 **・repeat** ・「01-はじめに」の「9 章 装置管理」に、下記コマンドを追加しました。 **・display transceiver alarm** **・display transceiver manuinfo** ・「02-WLAN」の「4 章 WLAN セキュリティ」の下記コマンドの **private-psk** パラメータは未サポートであるため削除しました。 **・akm mode** ・「04-アクセス」の「4 章 STP」の下記コマンドのデフォルト値の誤記を修正しました。 **・stp pathcost-standard**

Copyright © NEC Corporation 2018 - 2026

All Rights Reserved

事前に NEC の書面による許可なく、本マニュアルをいかなる形式または方法で複製または配布することを禁止します。

商標

本マニュアルに記載されているその他の商標は、各社が保有します。

注意

- 本装置は *QX-W2230AC アクセスコントローラ コマンドマニュアル*に記載されているコマンドのみ使用することができます。*QX-W2230AC アクセスコントローラコマンドマニュアル*に記載されていないコマンドを使用した場合の動作については保証しません。
- 本マニュアルの内容は、予告なく変更されることがあります。本マニュアルのすべての記述、情報、および推奨事項は、明示的か暗黙的かにかかわらず、いかなる種類の保証の対象になりません。

本マニュアルについて

バージョン

本マニュアルに対応する製品バージョンは Version 7.1.X を含む以降のソフトウェアです。

関連マニュアル

次のマニュアルには、QX-W2230AC アクセスコントローラに関する詳細な説明があります

マニュアル	内容
QX-W2230AC アクセスコントローラ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-W2230AC アクセスコントローラ オペレーションマニュアル	機能の設定について説明しています。
QX-W2230AC アクセスコントローラコマンドマニュアル	機能に関するコマンドについて説明しています。
QX-W2230AC アクセスコントローラ Web コンソール操作マニュアル	Web コンソールからの装置設定、状態確認等についての操作を記述しています。

マニュアルの構成

このコマンドマニュアルは以下のセクションで構成されます。

- **はじめに**

  アクセスコントローラへのアクセス方法、ファイルシステム管理、設定ファイル管理、ソフトウェア管理、装置管理といった、アクセスコントローラの管理の設定について説明します。

- **WLAN**

  WLAN の設定について説明します。

- **インタフェース**

  Ethernet ポートの設定について説明します。

- **アクセス**

  リンクアグリゲーション、VLAN、LLDP といった、レイヤ 2 機能の設定について説明します。

- **IP サービス**

  ARP、IP アドレス（IPv4）、DHCP 関連機能、IP パフォーマンスといった、ネットワークプロトコルの設定について説明します。

- **ルーティングプロトコル**

  各種ルーティングプロトコル（IPv4）の設定について説明します。

- **IP マルチキャスト**

  IGMP スヌーピングの設定について説明します。

- **ACL and QoS**

  QoS、ACL の設定について説明します。

- **セキュリティ**

  AAA、RADIUS、802.1X、MAC アドレス認証、SSH 等の設定について説明します。

- **高可用性**

  Track の設定について説明します。

- **システム管理**

  システム保守、ネットワーク管理の設定といった、アクセスコントローラのシステム管理および保守について説明します。

- **IRF スタック**

  IRF スタックの設定について説明します。

表記規則

本マニュアルでは、次の表記規則を使用しています。

I. コマンド表記規則

表記規則	説明
太字体	コマンドラインを示すキーワードには**太字体**を使用します。
イタリック体	コマンドの引数は*イタリック体*を使用します。
[ ]	大カッコに囲まれた項目(キーワード、引数)はオプションです。
{ x | y | … }	選択する項目は、中カッコに入れて縦線で区切ってあります。1 つを選択します。
[x | y | …]	オプションの選択項目は、大カッコに入れて縦線で区切ってあります。1 つまたは複数を選択します。
{ x | y | … }*	選択する項目は、中カッコに入れて縦線で区切ってあります。少なくとも 1 つ選択できます。
[x | y | …]*	オプションの選択項目は、大カッコに入れて、縦線で区切ってあります。1 つあるいは複数選択することも、何も選択しないこともできます。
&<1-n>	&の前のキーワードと引数を組み合わせます。引数で指定した数までキーワードを繰り返し指定できます。
#	#で始まる行はコメントを示します。

II. GUI 表記規則

表記規則	説明
< >	ボタン名は三角カッコに入っています。例えば、<OK>ボタンをクリックします。
[ ]	ウィンドウ名、メニュー項目、データ表、およびフィールド名は大カッコに入っています。例えば、[New User]ウィンドウが表示されます。
/	複数レベルのメニューはスラッシュで区切ってあります。例えば、[File/Create/Folder]。

III. キーボード操作

表記規則	説明
<KEY>	KEY のキーを押します。例えば、 <Enter>は Enter キーを押します。
<KEY1 + KEY2>	複数のキーを同時に押します。例えば、<Ctrl+Alt+A>は 3 つのキーを同時に押すことを表します。
<KEY1, KEY2>	複数のキーを順番に押します。例えば、 <Alt, A>は 2 つのキーを順に押すことを表します。

IV. マウス操作

表記規則	説明
クリック	マウスのボタンを素早く押します。特に指定がない場合は左ボタンを押します。
ダブルクリック	マウスの左ボタンを素早く 2 回押します。
ドラッグ	マウスの左ボタンを押したまま移動します。

V. 記号

表記規則	説明
⚠ **警告**	表示を無視したり指示に従わない場合、利用者が怪我などをする恐れのある重要な情報を示します。
⚠ **注意**	表示を無視したり指示に従わない場合、データの損失や破損、ハードウェアやソフトウェアの損傷などが発生する恐れのある重要な情報を示します。
⚠ **重要**	注意を払う必要がある情報を示します。
🕮 **メモ**	追加または補足となる情報を示します。
🕮 **ポイント**	参考となる情報を示します。

VI. ネットワークアイコン

表記規則	説明
	ルータ、スイッチ、またはファイアウォールなどの一般的なネットワークデバイスを表しています。
	ルータまたはレイヤ 3 スイッチなどのルーティング対応のデバイスを表しています。
	レイヤ 2、レイヤ 3 スイッチまたはレイヤ 2 転送機能に対応したルータなどの一般的なスイッチデバイスを表しています。

VII. 設定例

本マニュアルの設定例は各機能での代表的な設定例を示します。インタフェース番号、システム名の表記、display コマンドで表示される情報は、ご使用の装置と異なることがあります。

VIII. セキュリティ強化

セキュリティ強化のため、simple で設定されたパスワードも cipher や hash で登録されます。

本マニュアルは以下に示す 12 個のセクションで構成されています。

01 - はじめに

02 - WLAN

03 - インタフェース

04 - アクセス

05 - IP サービス

06 - ルーティングプロトコル

07 - IP マルチキャスト

08 - ACL and QoS

09 - セキュリティ

10 - 高可用性

11 - システム管理

12 - IRF スタック

QX-W2230AC アクセスコントローラ

コマンドマニュアル

1. はじめに

本マニュアルは以下に示す章で構成されています。

01-CLI
02-RBAC
03-ログイン
04-FTP
05-TFTP
06-ファイルシステム管理
07-コンフィグレーションファイル管理
08-ソフトウェアのアップグレード
09-装置管理
10-Tcl の使用
11-Python の使用
12-ライセンス管理

目次

このセクションのページは **1-x-x** です。

1 章 CLI 1-1
1.1 CLI 設定コマンド 1-1
1.1.1 alias 1-1
1.1.2 display | { begin | exclude | include } 1-3
1.1.3 display | by-linenum 1-4
1.1.4 display > 1-5
1.1.5 display >> 1-6
1.1.6 display alias 1-7
1.1.7 display history-command 1-8
1.1.8 display history-command all 1-9
1.1.9 display hotkey 1-10
1.1.10 hotkey 1-12
1.1.11 quit 1-13
1.1.12 repeat 1-13
1.1.13 return 1-15
1.1.14 screen-length disable 1-15
1.1.15 system-view 1-16

1章 CLI

1.1 CLI設定コマンド

1.1.1 alias

Syntax

alias *alias command*

undo alias *alias*

デフォルト

表 1-1 にシステム定義のエイリアスを示します。

表 1-1 システム定義のコマンドエイリアス

エイリアス	コマンド
access-list	acl
end	return
erase	delete
exit	quit
hostname	sysname
logging	info-center
no	undo
show	display
write	save

View

System view

定義済みユーザロール

network-admin

パラメータ

alias: エイリアスを指定します。設定範囲は 1～20 文字です。大文字、小文字を区別します。エイリアスは alias あるいはスペースを使用することができません。

command: コマンドの文字列を指定します。コマンド文字列は構文の要件に一致している必要があります。

説明

alias コマンドはコマンドのエイリアスを設定します。

undo alias コマンドはコマンドのエイリアスを削除します。

コマンドあるいはコマンドのパラメータで開始するエイリアスを設定することができます。設定後はコマンドを実行するためにエイリアスを使用することができます。**undo** で始まるコマンドがある場合についても、エイリアスを使用することができます。

たとえば、**display ip routing-table** コマンドのエイリアス **siprt** を設定すると、**display ip routing-table** コマンドを実行するために、**siprt** コマンドを入力することが可能です。

display ip コマンドのエイリアスに **ship** コマンドを設定した場合、**display ip** で始まるすべてのコマンドを実行するため、**ship** を使用することができます。

- **display ip routing-table** コマンドを実行するため **ship routing-table** コマンドを入力します。
- **display ip interface** コマンドを実行するため **ship interface** コマンドを入力します。

コマンド文字列は最大 9 つのパラメータまで含むことができます。各パラメータはドル記号（$）と 1～9 までのシーケンス番号で開始します。たとえば、**display ip $1 | include $2** を行うためにエイリアス **shinc** を設定できます。**display ip interface | include GigabitEthernet1/0/1** コマンドを実行する場合、**shinc interface GigabitEthernet1/0/1** だけで実行することができます。

例

display ip routing-table コマンドを行うためにエイリアス **shiprt** を設定し、設定を確認します。

<AC> system-view

[AC] alias shiprt display ip routing-table

[AC] shiprt

```
Destinations : 13       Routes : 13
Destination/Mask   Proto   Pre Cost       NextHop        Interface
0.0.0.0/32         Direct  0   0          127.0.0.1      InLoop0
3.3.3.3/32         Static  60  0          192.168.1.62    GE1/0/1
127.0.0.0/8        Direct  0   0          127.0.0.1      InLoop0
127.0.0.0/32       Direct  0   0          127.0.0.1      InLoop0
127.0.0.1/32       Direct  0   0          127.0.0.1      InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1      InLoop0
169.254.0.0/24     Direct  0   0          169.254.0.188   GE1/0/1
```

```
169.254.0.0/32     Direct  0   0          169.254.0.188   GE1/0/1
169.254.0.188/32   Direct  0   0          127.0.0.1       InLoop0
169.254.0.255/32   Direct  0   0          169.254.0.188   GE1/0/1
224.0.0.0/4        Direct  0   0          0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0          0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0          127.0.0.1       InLoop0
```

display $1 | include $2 コマンドを行うためにエイリアス **shinc** を設定します。

<AC> system-view

[AC] alias shinc display ip $1 | include $2

すべてのスタティックルート情報を表示するためにエイリアス **shinc** を使用します。

<AC> system-view

[AC] shinc routing-table Static

```
3.3.3.3/32         Static  60  0          192.168.1.62    Vlan1
```

関連コマンド

display alias

1.1.2 display | { begin | exclude | include }

Syntax

display *command* | { **begin** | **exclude** | **include** } *regular-expression*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

command: **display** コマンドのキーワードと引数を指定します。有効なキーワードと引数を表示する場合、**display ?**と入力します。

begin: 指定した正規表現の文字列を含む以降の行を表示します。

exclude: 指定した正規表現の文字列を含まない行を表示します。

include: 指定した正規表現の文字列を含む行を表示します。

regular-expression: 1～256 字の大文字と小文字を区別した正規表現を指定します。

説明

display | { **begin** | **exclude** | **include** }コマンドは正規表現を使用して **display** コマンドから出力をフィルタします。

正規表現の詳細は、オペレーションマニュアルのセクション 1 *はじめに “CLI”* を参照してください。

例

カレントコンフィグレーションで vlan を含む行を表示します。

<AC> display current-configuration | include vlan

```
vlan 1
vlan 999
 port access vlan 999
```

1.1.3 display | by-linenum

Syntax

display *command* **| by-linenum**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

command: **display** コマンドのキーワードと引数を指定します。有効なキーワードと引数を表示する場合、**display ?**と入力します。

説明

display | by-linenum コマンドは **display** コマンドに行番号をつけて表示します。

行番号を使用することで、わかりやすく表示することができます。

行番号は 5 桁で表示され、コロン（:）あるいはハイフン（-）が続きます。**display | by-linenum** コマンドと **display | begin regular-expression** コマンドを同時に使用した場合、正規表現に一致しないすべての行はハイフン（-）で表示されます。

例

VLAN999 の設定を表示するため、行番号をつけて出力を表示します。

<AC> display vlan 999 | by-linenum

```
 1:  VLAN ID: 999
 2:  VLAN type: Static
 3:  Route interface: Configured
 4:  IPv4 address: 192.168.2.1
 5:  IPv4 subnet mask: 255.255.255.0
 6:  Description: For LAN Access
 7:  Name: VLAN 0999
 8:  Tagged ports:  None
 9:  Untagged ports:
10:    GigabitEthernet1/0/1
```

カレントコンフィグレーションで user-group で始まる行から以降の行を表示します。

<AC> display current-configuration | by-linenum begin user-group

```
114:  user-group system
115-  #
116-  return
```

1.1.4 display >

Syntax

display *command* **>** *filename*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

command: **display** コマンドのキーワードと引数を指定します。有効なキーワードと引数を表示する場合、**display ?**と入力します。

filename: 出力を保存するファイル名を 1～63 文字で指定します。

説明

display >コマンドは **display** コマンドの出力を別のファイルに保存します。

display コマンドは設定、統計情報、装置の状態を表示します。**display >**コマンドはファイルに **display** コマンドの出力を保存します。

指定したファイルが存在しない場合、ファイルを新規に作成し、ファイルに **display** コマンドの出力を保存します。指定したファイルが存在する場合、ファイルに上書きします。

例

vlan.txt というファイルに VLAN 1 の設定を保存します。

<AC> display vlan 1 > vlan.txt

vlan.txt ファイルの内容を確認します。

<AC> more vlan.txt

```
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/2
```

1.1.5 display >>

Syntax

display *command* **>>** *filename*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

command: **display** コマンドのキーワードと引数を指定します。有効なキーワードと引数を表示する場合、**display ?**と入力します。

filename: 出力を保存するファイル名を 1～63 文字で指定します。

説明

display >>コマンドは **display** コマンドの出力をファイルの最後に追記します。

display コマンドは設定、統計情報、装置の状態を表示します。**display >>**コマンドはファイルに **display** コマンドの出力を保存します。

指定したファイルが存在しない場合、ファイルを新規に作成し、ファイルに **display** コマンドの出力を保存します。指定したファイルが存在する場合、ファイルの最後に追記します。

例

vlan.txt というファイルの最後に VLAN 999 を追記します。

<AC> display vlan 999 >> vlan.txt

```
<AC>
```

vlan.txt ファイルの内容を確認します。

<AC> more vlan.txt

```
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:  None
 Untagged ports:
   GigabitEthernet1/0/2

 VLAN ID: 999
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 192.168.2.1
 IPv4 subnet mask: 255.255.255.0
 Description: For LAN Access
 Name: VLAN 0999
 Tagged ports:  None
 Untagged ports:
   GigabitEthernet1/0/2
```

1.1.6 display alias

Syntax

display alias [*alias*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

alias: コマンドエイリアスを指定します。指定しない場合、すべてのコマンドのエイリアスを表示します。

説明

display alias コマンドはコマンドエイリアスを表示します。

例

すべてのコマンドのエイリアスを表示します。

<AC> display alias

```
Index     Alias              Command key
1         access-list         acl
2         end                return
3         erase              delete
4         exit               quit
5         hostname           sysname
6         logging            info-center
7         no                 undo
8         shinc              display $1 | include $2
9         show               display
10        sirt               display ip routing-table
11        write              save
```

コマンドエイリアス shinc を表示します。

<AC> display alias shinc

```
Alias             Command key
shinc             display ip $1 | include $2
```

関連コマンド

alias

1.1.7 display history-command

Syntax

display history-command

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display history-command コマンドは履歴バッファに保存されているすべてのコマンドを表示します。このコマンドは現在の CLI セッションで実行された有効なコマンドです。

システムは現在の CLI セッションで実行された有効なコマンドを自動的に保存します。

履歴バッファに保存されているコマンドを表示し、再度実行することができます。

デフォルトで、最大 10 個まで履歴コマンドを保存できます。履歴バッファのサイズを設定するには、**history-command max-size** コマンドを使用します。

バッファサイズが最大のときに新しいコマンドをバッファする場合、システムはバッファのもっとも古いコマンドを削除します。

現在の CLI セッションの履歴コマンドのすべてのコマンドはログアウトしたときに削除されます。

例

現在の CLI セッションで履歴バッファにあるすべてのコマンドを表示します。

<AC> display history-command

```
system-view
vlan 2
quit
```

関連コマンド

history-command max-size

1.1.8 display history-command all

Syntax

display history-command all

View

すべての view

定義済みユーザロール

network-admin

説明

display history-command all コマンドは履歴バッファに保存されているすべてのコマンドを表示します。このコマンドはすべての CLI セッションで実行された有効なコマンドです。

システムはすべての CLI セッションで実行された有効なコマンドを自動的に保存します。

履歴バッファに保存されているコマンドを表示し、再度実行することができます。

最大 1024 個まで履歴コマンドを保存できます。履歴バッファのサイズが最大になったとき、最初に保存されたコマンドを削除し、新しく実行されたコマンドを保存します。

ユーザがログアウトした場合、すべての CLI セッションの履歴バッファからコマンドを削除します。

例

すべての CLI セッションで履歴バッファにあるすべてのコマンドを表示します。

<AC> display history-command all

```
Date      Time     Terminal   Ip            User
03/16/2017 20:03:33 vty0      192.168.1.26    **
Cmd:dis his all

03/16/2017 20:03:29 vty0      192.168.1.26    **
Cmd:sys
```

表 1-2 コマンド出力

フィールド	説明
Date	コマンドを実行した日付です。
Time	コマンドを実行した時間です。
Terminal	ユーザが使用しているlineです。
Ip	ユーザが使用している端末のIPアドレスです。
User	ユーザが使用するユーザ名です。
Cmd	ユーザによって入力したコマンドです。

関連コマンド

display history-command

1.1.9 display hotkey

Syntax

display hotkey

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display hotkey コマンドはホットキー情報を表示します。

例

ホットキー情報を表示します。

<AC> display hotkey

```
----------------- Hotkeys -----------------
         -Defined function hotkeys-
CTRL_A  Move the cursor to the beginning of the line.
CTRL_B  Move the cursor one character to the left.
CTRL_C  Stop the current command.
CTRL_D  Erase the character at the cursor.
CTRL_E  Move the cursor to the end of the line.
CTRL_F  Move the cursor one character to the right.
CTRL_H  Erase the character to the left of the cursor.
CTRL_K  Abort the connection request.
CTRL_N  Display the next command in the history buffer.
CTRL_P  Display the previous command in the history buffer.
CTRL_R  Redisplay the current line.
CTRL_V  Paste text from the clipboard.
CTRL_W  Delete the word to the left of the cursor.
CTRL_X  Delete all characters from the beginning of the line to the cursor.
CTRL_Y  Delete all characters from the cursor to the end of the line.
CTRL_Z  Return to the User View.
CTRL_]  Kill incoming connection or redirect connection.
ESC_B   Move the cursor back one word.
ESC_D   Delete all characters from the cursor to the end of the word.
ESC_F   Move the cursor forward one word.
ESC_N   Move the cursor down a line.
ESC_P   Move the cursor up a line.
ESC_<   Move the cursor to the beginning of the clipboard.
ESC_>   Move the cursor to the end of the clipboard.
```

関連コマンド

hotkey

1.1.10 hotkey

Syntax

hotkey { CTRL_G | CTRL_L | CTRL_O | CTRL_T | CTRL_U } command

undo hotkey { CTRL_G | CTRL_L | CTRL_O | CTRL_T | CTRL_U }

デフォルト

ctrl_G: **display current-configuration**（カレントコンフィグレーションを表示します。）

ctrl_L: **display ip routing-table**（IPv4 ルーティングテーブル情報を表示します。）

ctrl_O: **undo debugging all**（すべてのデバッグ機能を無効にします。）

ctrl_T: ホットキーにコマンドが割り当てられていません。

ctrl_U: ホットキーにコマンドが割り当てられていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

CTRL_G: ホットキー**Ctrl+G** にコマンドを割り当てます。

CTRL _L: ホットキー**Ctrl+L** にコマンドを割り当てます。

CTRL _O: ホットキー**Ctrl+O** にコマンドを割り当てます。

CTRL _T: ホットキー**Ctrl+T** にコマンドを割り当てます。

CTRL _I: ホットキー**Ctrl+U** にコマンドを割り当てます。

command: ホットキーに割り当てるコマンドを指定します。

説明

hotkey コマンドは設定可能なホットキーにコマンドを割り当てます。

undo hotkey コマンドはデフォルトに戻します。

システムはいくつかのホットキーを定義し、5 つの設定可能なコマンドホットキーを提供します。ホットキーを押下することでホットキーに割り当てられたコマンドを実行します。

システムで定義されたホットキーと設定可能なホットキーを表示するには **display hotkey** コマンドを使用します。

例

ホットキーCTRL+T に **display tcp status** コマンドを割り当てます。

<AC> system-view

[AC] hotkey ctrl_t display tcp statistics

関連コマンド

display hotkey

1.1.11 quit

Syntax

quit

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

quit コマンドは上位の view に戻ります。

user view で **quit** コマンドを実行すると装置から切断されログアウトします。

例

GigabitEthernet 1/0/1 interface view から system view に戻り、次に user view に戻ります。

[AC-GigabitEthernet1/0/1] quit

[AC] quit

<AC>

1.1.12 repeat

Syntax

repeat [*number*] [**count** *times*] [**delay** *seconds*]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

number: 現在の CLI セッションのコマンド履歴バッファで、繰り返し実行したい直近のコマンド数を指定します。値の範囲は 1～256 です。デフォルトは 1 です。

count *times*: コマンドを実行する回数を指定します。値の範囲は 0～4294967295 です。デフォルトは 0 です。このオプションを指定しない場合、エスケープキーを押して停止するまで実行は継続されます。

delay *seconds*: コマンドを再実行する前にシステムが待機する時間(秒)を指定します。値の範囲は 0～4294967295 です。デフォルトは 1 です。

説明

repeat コマンドを使用すると、現在の CLI セッションのコマンド履歴バッファ内のコマンドを繰り返し実行できます。

コマンドを繰り返す場合、まずそのコマンドのビューに入ります。複数のコマンドを繰り返す場合は、最初のコマンドのビューに入ります。

対話型コマンドを繰り返す際、システムはユーザの操作を待機します。

パスワード設定コマンドはすべてスキップされます。

コマンド履歴バッファで繰り返されるコマンド数は、以下の最小値によって決まります。

· repeat コマンドで指定した直近のコマンド数

· history-command max-size コマンドで指定したコマンド履歴バッファのサイズ

· コマンド履歴バッファ内のコマンド数

例

直近に実行した 2 つのコマンド（display cpu-usage と display clock）を 10 秒間隔で 2 回実行します。

<AC> repeat 2 count 2 delay 10

```
<AC> display cpu
Unit CPU usage:
     33% in last 5 seconds
     32% in last 1 minute
     33% in last 5 minutes

<AC> display clock
07:02:18 UTC Thu 06/19/2017
<AC> display cpu-usage
Unit CPU usage:
     33% in last 5 seconds
     32% in last 1 minute
     33% in last 5 minutes

<AC> display clock
```

```
07:02:28 UTC Thu 06/19/2017
```

1.1.13 return

Syntax

return

View

user view を除いたすべての view

定義済みユーザロール

network-admin

network-operator

説明

return コマンドはほかの view から user view に戻ります。

Ctrl+Z ホットキーは **return** コマンドと同一です。

例

GigabitEthernet 1/0/1 interface view から user view に戻ります。

[AC-GigabitEthernet1/0/1] return

<AC>

1.1.14 screen-length disable

Syntax

screen-length disable

undo screen-length disable

デフォルト

user line view の **screen-length** コマンドの設定によってデフォルトは変わります。

screen-length コマンドのデフォルトは以下です。

- 出力画面ごとにスクロールを停止します。
- 画面上で一度に 24 行まで表示します。

View

User view

定義済みユーザロール

network-admin

説明

screen-length disable コマンドは現在のセッションで出力画面のスクロールの停止を無効にします。

undo screen-length disable コマンドは現在のセッションで出力画面のスクロールの停止を有効にします。

出力画面のスクロールの停止を無効にした場合、すべての出力が表示されます。最後の画面が表示されるまで連続して画面がリフレッシュします。

本コマンドは現在の画面のみ適用されます。ログアウトすると設定はデフォルトに戻ります。

例

現在のセッションで出力画面のスクロールの停止を無効にします。

<AC> screen-length disable

関連コマンド

screen-length

1.1.15 system-view

Syntax

system-view

View

User view

定義済みユーザロール

network-admin

network-operator

説明

system-view コマンドは user view から system view に移行します。

例

user view から system view に移行します。

<AC> system-view

```
System View: return to User View with Ctrl+Z.
```

[AC]

目次

このセクションのページは **1-x-x** です。

2 章 RBAC 2-1
2.1 RBAC 設定コマンド 2-1
2.1.1 description 2-1
2.1.2 display role 2-2
2.1.3 display role feature 2-10
2.1.4 display role feature-group 2-13
2.1.5 feature 2-16
2.1.6 interface policy deny 2-17
2.1.7 permit interface 2-19
2.1.8 permit vlan 2-21
2.1.9 role 2-23
2.1.10 role default-role enable 2-24
2.1.11 role feature-group 2-25
2.1.12 rule 2-26
2.1.13 super 2-31
2.1.14 super authentication-mode 2-32
2.1.15 super default role 2-33
2.1.16 super password 2-34
2.1.17 vlan policy deny 2-35

2章 RBAC

2.1 RBAC設定コマンド

2.1.1 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

User role view

定義済みユーザロール

network-admin

パラメータ

text: ユーザロールの説明を設定します。設定範囲は 1～128 です。大文字、小文字を区別します。

説明

description コマンドはユーザロールの説明を設定します。

undo description コマンドはユーザロールの説明を削除します。

例

ユーザロール **role1** の説明を **labVIP** に設定します。

<AC> system-view

[AC] role name role1

[AC-role-role1] description labVIP

関連コマンド

- **display role**
- **role**

2.1.2 display role

Syntax

display role [**name** *role-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *role-name*: ユーザロール名を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。ユーザロール名を指定しない場合、定義済みのユーザロールを含むすべてのユーザロールの情報を表示します。

説明

display role コマンドはユーザロールの情報を表示します。

例

ユーザロール **123** の情報を表示します。

<AC> display role name 123

```
Role: 123
  Description: new role
  VLAN policy: deny
  Permitted VLANs: 1 to 5, 7 to 8
  Interface policy: deny
  Permitted interfaces: Ten-GigabitEthernet1/0/1 to Ten-GigabitEthernet1/0/2,
Vlan-interface1 to Vlan-interface20
  VPN instance policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope        Entity
  ------------------------------------------------------------------
  1       permit RWX   feature-group abc
  2       deny   -W-   feature      ldap
  3       permit       command      system ; radius sc *
  4       permit R--   xml-element   -
  5       permit RW-   oid          1.2.1
  R:Read W:Write X:Execute
```

すべてのユーザロールに関する情報を表示します。

<AC> display role

```
Role: network-admin
  Description: Predefined network admin role has access to all commands on the
device
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope       Entity
  ----------------------------------------------------------------------
  sys-1   permit      command     *
  sys-2   permit RWX   web-menu     -
  sys-3   permit RWX   xml-element   -
  sys-4   deny        command     display security-logfile summary
  sys-5   deny        command     system-view ; info-center
                                security-logfile directory *
  sys-6   deny        command     security-logfile save
  sys-7   permit RW-   oid         1
  R:Read W:Write X:Execute

Role: network-operator
  Description: Predefined network operator role has access to all read commands
on the device
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope       Entity
  ----------------------------------------------------------------------
  sys-1   permit      command     display *
  sys-2   permit      command     xml
  sys-3   permit      command     system-view ; probe ; display *
  sys-4   deny        command     display history-command all
  sys-5   deny        command     display exception *
  sys-6   deny        command     display cpu-usage configuration
                                *
  sys-7   deny        command     display kernel exception *
  sys-8   deny        command     display kernel deadloop *
  sys-9   deny        command     display kernel starvation *
  sys-10  deny        command     display kernel reboot *
  sys-13  permit      command     system-view ; local-user *
  sys-15  permit R--   web-menu     -
  sys-16  permit R--   xml-element   -
  sys-17  deny        command     display security-logfile summary
```

```
  sys-18  deny        command      system-view ; info-center
                                  security-logfile directory *
  sys-19  deny        command      security-logfile save
  sys-20  deny        command      system-view ; local-user-import
                                  *
  sys-21  deny        command      system-view ; local-user-export
                                  *
  sys-22  permit R--   oid          1
  sys-23  deny        command      display smartmc *
  R:Read W:Write X:Execute

Role: level-0
  Description: Predefined level-0 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ---------------------------------------------------------------------
  Rule    Perm   Type  Scope        Entity
  ---------------------------------------------------------------------
  sys-1   permit      command      tracert *
  sys-2   permit      command      telnet *
  sys-3   permit      command      ping *
  sys-4   permit      command      ssh2 *
  sys-5   permit      command      super *
  sys-6   permit      command      mtrace *
  R:Read W:Write X:Execute

Role: level-1
  Description: Predefined level-1 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ---------------------------------------------------------------------
  Rule    Perm   Type  Scope        Entity
  ---------------------------------------------------------------------
  sys-1   permit      command      tracert *
  sys-2   permit      command      telnet *
  sys-3   permit      command      ping *
  sys-4   permit      command      ssh2 *
  sys-5   permit      command      display *
  sys-6   permit      command      super *
  sys-7   deny        command      display history-command all
  sys-8   permit      command      mtrace *
```

```
  R:Read W:Write X:Execute

Role: level-2
  Description: Predefined level-2 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-3
  Description: Predefined level-3 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-4
  Description: Predefined level-4 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-5
  Description: Predefined level-5 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-6
  Description: Predefined level-6 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-7
  Description: Predefined level-7 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-8
  Description: Predefined level-8 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
```

```
Role: level-9
  Description: Predefined level-9 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope       Entity
  ----------------------------------------------------------------------
  sys-1   permit RWX   feature      -
  sys-2   deny   RWX   feature      device
  sys-3   deny   RWX   feature      filesystem
  sys-4   permit       command      display *
  sys-5   deny         command      display history-command all
  R:Read W:Write X:Execute

Role: level-10
  Description: Predefined level-10 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-11
  Description: Predefined level-11 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-12
  Description: Predefined level-12 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-13
  Description: Predefined level-13 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-14
  Description: Predefined level-14 role
  VLAN policy: permit (default)
```

```
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-15
  Description: Predefined level-15 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope       Entity
  ----------------------------------------------------------------------
  sys-1   permit      command     *
  sys-2   permit RWX   web-menu     -
  sys-3   permit RWX   xml-element   -
  sys-4   deny        command     display security-logfile summary
  sys-5   deny        command     system-view ; info-center
                                 security-logfile directory *
  sys-6   deny        command     security-logfile save
  sys-7   permit RW-   oid         1
  sys-8   deny        command     display smartmc *
  sys-9   deny        command     debugging smartmc *
  sys-10  deny        command     undo debugging smartmc *
  sys-11  deny        command     system-view ; smartmc *
  sys-12  deny        command     system-view ; undo smartmc *
  sys-13  deny        command     system-view ; interface * ; smartmc *
  sys-14  deny        command     system-view ; interface * ; undo
                                 smartmc *
  sys-29  deny        command     create batch-file *
  R:Read W:Write X:Execute

Role: security-audit
  Description: Predefined security audit role only has access to commands for
the
security log administrator
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope       Entity
  ----------------------------------------------------------------------
  sys-1   deny        command     *
  sys-2   permit      command     display security-logfile summary
  sys-3   permit      command     system-view ; info-center
```

```
                                security-logfile directory *
  sys-4   permit      command      security-logfile save
  sys-5   permit      command      cd *
  sys-6   permit      command      copy *
  sys-7   permit      command      delete *
  sys-8   permit      command      dir *
  sys-9   permit      command      mkdir *
  sys-10  permit      command      more *
  sys-11  permit      command      move *
  sys-12  permit      command      rmdir *
  sys-13  permit      command      pwd
  sys-14  permit      command      rename *
  sys-15  permit      command      undelete *
  sys-16  permit      command      ftp *
  sys-17  permit      command      sftp *
  R:Read W:Write X:Execute

Role: guest-manager
  Description: Predefined guest manager role can't access to commands
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope        Entity
  ----------------------------------------------------------------------
  sys-1   permit RWX   xml-element   useraccounts/approveguest/
  sys-2   permit RWX   xml-element   useraccounts/exportguestaccount/
  sys-3   permit RWX   xml-element   useraccounts/generateguestaccount/
  sys-4   permit RWX   xml-element   useraccounts/guest/
  sys-5   permit RWX   xml-element   useraccounts/guestconfigure/
  sys-6   permit RWX   xml-element   useraccounts/importguestaccount/
  sys-7   permit RWX   xml-element   useraccounts/exportguesttemplet/
  sys-8   permit RWX   xml-element   rpc/
  sys-9   deny        command      *
  R:Read W:Write X:Execute
```

表 2-1 コマンド出力

フィールド	説明
Role	ユーザロール名です。 定義済みのユーザロール名は以下です。 ● network-admin ● network-operator

フィールド	説明
	● level-*n* （*n*は0～15の整数です） ● security-audit. ● guest-manager.
Description	設定内容を容易に識別できるようにするためのユーザロールの説明です。
VLAN policy	ユーザロールのVLANポリシーです。 ● **deny**–許可されたVLANを除くVLANへのアクセスを拒否します。 ● **permit (default)**–デフォルトVLANポリシーです。すべてのVLANにアクセスするユーザロールを有効にします。
Permitted VLANs	ユーザロールにアクセス可能なVLANです。
Interface policy	ユーザロールのインタフェースポリシーです。 ● **deny**–許可されたインタフェースを除くインタフェースへのアクセスを拒否します。 ● **permit (default)**–デフォルトインタフェースポリシーです。すべてのインタフェースにアクセスするユーザロールを有効にします。
Permitted interfaces	ユーザロールにアクセス可能なインタフェースです。
VPN instance policy	ユーザロールのVPNインスタンスポリシーです。 ● **deny**–許可されたVPNインスタンスを除くVPNインスタンスへのアクセスを拒否します。 ● **permit (default)**–デフォルトVPNインスタンスポリシーです。すべてのVPNインスタンスにアクセスするユーザロールを有効にします。
Permitted VPN instances	ユーザロールにアクセス可能なVPNインスタンスです。
Rule	ユーザロール番号です。 定義済みのユーザロールのルールはsys-*n*で指定されます。ここで*n*は整数です。
Perm	アクセス制御タイプです。 ● **permit**–ユーザロールは、エンティティフィールドの項目にアクセスできます。 ● **deny**–ユーザロールは、エンティティフィールドの項目にアクセスできません。
Type	制御タイプです。 ● **R**–Read-onlyです。

フィールド	説明
	• **W**–Writeです。 • **X**–Executeです。
Scope	ルール制御範囲です。 • **command**–コマンドへのアクセスを制御する、あるいはエンティティフィールドで指定されるコマンドです。 • **feature**–エンティティフィールドに指定され、機能のコマンドへのアクセスを制御します。 • **feature-group**–エンティティフィールドに指定され、機能グループの機能のコマンドへのアクセスを制御します。 • **web-menu**–Webメニューへのアクセスを制御します。このルール制御範囲は、現在のソフトウェアバージョンではサポートされていません。 • **xml-element**— XML要素へのアクセスを制御します。 • **oid**– MIBノードへのアクセスを制御します。
Entity	ユーザグループルールで指定されたコマンド文字列、機能名、機能グループです。 • エンダッシュ（–）はすべての機能を示します。 • アスタリスク（*）は0以上の文字を示します。

関連コマンド

role

2.1.3 display role feature

Syntax

display role feature [**name** *feature-name* | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *feature-name*: 機能のコマンドを表示します。*feature-name* は機能名を指定します。すべての文字は小文字にする必要があります。

verbose: 各機能のコマンドを表示します。

説明

display role feature コマンドはシステムで有効な機能を表示します。

パラメータを指定しない場合、システムで有効な機能のリストのみを表示します。

例

機能のリストを表示します。

<AC> display role feature

```
Feature: device         (Device configuration related commands)
Feature: interface      (Interface related commands)
Feature: syslog         (Syslog related commands)
```

…

各機能のコマンドを表示します。

<AC> display role feature verbose

```
Feature: device         (Device configuration related commands)
  display clock    (R)
  debugging dev    (W)
  display debugging dev    (R)
  display device *    (R)
  display diagnostic-information *    (R)
  display environment *    (R)
  display fan *    (R)
  display power *    (R)
  display current-configuration *    (R)
  display saved-configuration *    (R)
  display default-configuration *    (R)
  display startup    (R)
  display this *    (R)
```

…

aaa 機能のコマンドを表示します。

<AC> display role feature name aaa

```
Feature: aaa            (AAA related commands)
  system-view ; domain *    (W)
  system-view ; header *    (W)
  system-view ; aaa *    (W)
```

```
  display domain *    (R)
  display aaa *    (R)
  system-view ; user-group *    (W)
  system-view ; local-user *    (W)
  display local-user *    (R)
  display user-group *    (R)
  display debugging local-server    (R)
  debugging local-server *    (W)
  super *    (X)
  display password-control *    (R)
  reset password-control *    (W)
  system-view ; password-control *    (W)
...
```

表 2-2 コマンド出力 (**display role feature name** *aaa*)

フィールド	説明
Feature	機能の名前、概要の説明を表示します。
system-view ; domain *	system viewでの**domain**キーワードで始まるすべてのコマンドです。ISP domain viewでのすべてのコマンドです。
system-view ; header *	system viewでの**header**キーワードで始まるすべてのコマンドです。
system-view ; aaa *	system viewでの**aaa**で始まるすべてのコマンドです。
display domain *	user viewでの**display domain**キーワードで始まるすべてのコマンドです。
system-view ; user-group *	system viewでの**user-group**キーワードで始まるすべてのコマンドとuser group viewのすべてのコマンドです。
system-view ; local-user *	system viewでの**local-user**キーワードで始まるすべてのコマンドとlocal user viewのすべてのコマンドです。
display user-group *	user viewでの**display user-group**キーワードで始まるすべてのコマンドです。
display debugging local-server	user viewでの**display debugging local-server**キーワードで始まるすべてのコマンドです。
debugging local-server *	user viewでの**debugging local-server**キーワードで始まるすべてのコマンドです。
super *	user viewでの**super**キーワードで始まるすべてのコマンドです。
display password-control *	user viewでの**display password-control**キーワードで始まるすべてのコマンドです。
reset password-control *	user viewでの**reset password-control**キーワードで始まるすべてのコマンドです。

フィールド	説明
system-view ; password-control *	system viewでの**password-control**キーワードで始まるすべてのコマンドです。
(W)	コマンドタイプがwriteです。writeコマンドはシステムを設定します。
(R)	コマンドタイプがreadです。readコマンドは設定を表示あるいは情報を維持します。
(X)	コマンドタイプがexecuteです。execute コマンドは指定した機能を実行します。

関連コマンド

feature

2.1.4 display role feature-group

Syntax

display role feature-group [**name** *feature-group-name*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *feature-group-name*: 機能グループを指定します。*feature-group-name* は機能グループ名を指定します。設定範囲は 1～31 です。大文字、小文字を区別します。機能グループを指定しない場合、すべての機能グループの情報を表示します。

verbose: 指定された機能グループの各機能のコマンドを表示します。機能グループを指定しない場合、各機能グループの各機能のコマンドを表示します。**verbose** キーワードを指定しない場合、機能グループの機能リストのみを表示します。

説明

display role feature-group コマンドは機能グループの情報を表示します。

機能グループ **L2**、**L3** は機能グループで定義されています。

例

機能グループの機能リストを表示します。

<AC> display role feature-group

```
Feature group: L2
Feature: igmp-snooping   (IGMP-Snooping related commands)
Feature: mld-snooping    (MLD-Snooping related commands)
Feature: lacp           (LACP related commands)
Feature: stp            (STP related commands)
Feature: lldp           (LLDP related commands)
Feature: dldp           (DLDP related commands)
Feature: cfm            (CFM related commands)
Feature: eoam           (EOAM related commands)
Feature: smart-link      (Smart-link related commands)
Feature: monitor-link    (Monitor-link related commands)
Feature: loopbk-detect   (Loopback-detection related commands)
Feature: vlan           (Virtual LAN related commands)
Feature: evb            (EVB related commands)
Feature: mvrp           (MVRP related commands )
Feature: rrpp           (RRPP related commands)
Feature: erps           (ERPS related commands)
Feature: ofp            (OFP related commands)
Feature: port-security   (Port-security related commands)
Feature: l2pt           (L2PT related commands)

Feature group: L3
Feature: route          (Route management related commands)
Feature: staticrt       (Unicast static route related commands)
Feature: ospf           (Open Shortest Path First protocol related commands)
Feature: rip            (Routing Information Protocol related commands)
Feature: isis           (ISIS protocol related commands)
Feature: lisp           (LISP protocol related commands)
Feature: bgp            (Border Gateway Protocol related commands)
Feature: l3vpn          (Layer 3 Virtual Private Network related commands)
Feature: route-policy    (Routing Policy related commands)
Feature: multicast       (Multicast related commands)
Feature: pim            (Protocol Independent Multicast related commands)
Feature: igmp           (Internet Group Management Protocol related commands)
Feature: mld            (Multicast Listener Discovery related commands)
Feature: msdp           (Multicast Source Discovery Protocol related commands)
```

各機能グループのコマンドを表示します。コマンドのワイルドカードと記号についての詳細は、表 2-2 を参照してください。

<AC> display role feature-group verbose

```
Feature group: L2
Feature: igmp-snooping   (IGMP-Snooping related commands)
```

```
  system-view ; igmp-snooping *    (W)
  system-view ; multicast-vlan *    (W)
  system-view ; vlan * ; igmp-snooping *    (W)
  system-view ; vlan * ; pim-snooping *    (W)
  system-view ; vsi * ; igmp-snooping *    (W)
  system-view ; vsi * ; pim-snooping *    (W)
  system-view ; interface * ; igmp-snooping *    (W)
  system-view ; interface * ; port multicast-vlan *    (W)
  display igmp-snooping *    (R)
  display pim-snooping *    (R)
  display multicast-vlan *    (R)
  display l2-multicast *    (R)
  system-view ; probe ; display system internal l2-multicast *    (R)
  system-view ; probe ; display system internal multicast-vlan *    (R)
  reset igmp-snooping *    (W)
  reset pim-snooping *    (W)
  reset multicast-vlan *    (W)
  reset l2-multicast *    (W)
  debugging igmp-snooping *    (W)
  display debugging igmp-snooping *    (R)
  system-view ; probe ; debugging system internal igmp-snooping *    (W)
Feature: mld-snooping    (MLD-Snooping related commands)
  system-view ; mld-snooping *    (W)
  system-view ; ipv6 multicast-vlan *    (W)
  system-view ; mld-snooping    (W)
  system-view ; mld-snooping *    (W)
  system-view ; ipv6 multicast-vlan *    (W)
  system-view ; vlan * ; mld-snooping *    (W)
  system-view ; vlan * ; ipv6 pim-snooping *    (W)
  system-view ; vsi * ; mld-snooping *    (W)
  system-view ; vsi * ; ipv6 pim-snooping *    (W)
  system-view ; interface * ; mld-snooping *    (W)
  system-view ; interface * ; ipv6 port multicast-vlan *    (W)
  display mld-snooping *    (R)
  display ipv6 pim-snooping *    (R)
  display ipv6 multicast-vlan *    (R)
  display ipv6 l2-multicast *    (R)
  system-view ; probe ; display system internal ipv6 l2-multicast *    (R)
  system-view ; probe ; display system internal ipv6 multicast-vlan *    (R)
  reset mld-snooping *    (W)
  reset ipv6 pim-snooping *    (W)
  reset ipv6 multicast-vlan *    (W)
  reset ipv6 l2-multicast *    (W)
```

```
  debugging mld-snooping *    (W)
  display debugging mld-snooping *    (R)
  system-view ; probe ; debugging system internal mld-snooping *    (W)
...
```

機能グループ **L3** の機能リストを表示します。

<AC> display role feature-group name L3

```
Feature group: L3
Feature: route          (Route management related commands)
Feature: staticrt       (Unicast static route related commands)
Feature: ospf           (Open Shortest Path First protocol related commands)
Feature: rip            (Routing Information Protocol related commands)
Feature: isis           (ISIS protocol related commands)
Feature: lisp           (LISP protocol related commands)
Feature: bgp            (Border Gateway Protocol related commands)
Feature: l3vpn          (Layer 3 Virtual Private Network related commands)
Feature: route-policy    (Routing Policy related commands)
Feature: multicast      (Multicast related commands)
Feature: pim            (Protocol Independent Multicast related commands)
Feature: igmp           (Internet Group Management Protocol related commands)
Feature: mld            (Multicast Listener Discovery related commands)
Feature: msdp           (Multicast Source Discovery Protocol related commands)
```

関連コマンド

- **feature**
- **role feature-group**

2.1.5 feature

Syntax

feature *feature-name*

undo feature *feature-name*

デフォルト

設定なし

View

Feature group view

定義済みユーザロール

network-admin

パラメータ

feature-name: 機能名を指定します。機能名は小文字で入力する必要があります。

説明

feature コマンドは機能グループに機能を追加します。

undo feature コマンドは機能グループから機能を削除します。

機能グループに複数の機能を追加する場合、**feature** コマンドを繰り返してください。

例

セキュリティグループ **security-features** にセキュリティ機能 AAA、ACL を追加します。

<AC> system-view

[AC] role feature-group name security-features

[AC-featuregrp-security-features] feature aaa

[AC-featuregrp-security-features] feature acl

関連コマンド

- **display role feature**
- **display role feature-group**
- **role feature-group**

2.1.6 interface policy deny

Syntax

interface policy deny

undo interface policy deny

デフォルト

User role はすべてのインタフェースにアクセスできます。

View

User role view

定義済みユーザロール

network-admin

説明

interface policy deny コマンドはインタフェースへのアクセスを拒否し、ユーザロールの interface policy view に移行します。

undo interface policy deny コマンドはユーザロールインタフェースポリシーをデフォルトに戻します。

指定したインタフェースのみユーザロールのインタフェースへのアクセスを制限するために、以下の作業を行います。

1) interface policy deny コマンドでユーザロールインタフェースポリシービューに移行します。
2) permit interface コマンドでアクセス可能なインタフェースを指定します。

🕮 **メモ：**

interface policy deny コマンドは、**permit interface** コマンドが設定されていない場合、すべてのインタフェースへのユーザロールのアクセスを拒否します。

インタフェースを設定するため、ユーザロールのインタフェースポリシーで許可されているインタフェースが使用されているであることを確認してください。アクセス可能なインタフェースで以下の操作を実行することができます。

- インタフェースの作成、削除、設定を行います。
- interface view へ移行します。
- **feature** コマンドでインタフェースを指定します。

作成および削除は、論理インタフェースでのみ有効です。

ユーザロールのインタフェースポリシーの変更は、変更後にユーザロールにログインしたユーザのみ適用されます。

例

ユーザロール **role1** でインタフェースへのアクセスを拒否します。

<AC> system-view

[AC] role name role1

[AC-role-role1] interface policy deny

[AC-role-role1-ifpolicy] quit

ユーザロール **role1** で Ten-GigabitEthernet 1/0/1～Ten-GigabitEthernet 1/0/4 を除くインタフェースへのアクセスを拒否します。

<AC> system-view

[AC] role name role1

[AC-role-role1] interface policy deny

[AC-role-role1-ifpolicy] permit interface Ten-GigabitEthernet 1/0/1 to Ten-GigabitEthernet 1/0/4

関連コマンド

- **display role**

- **permit interface**
- **role**

2.1.7 permit interface

Syntax

permit interface *interface-list*

undo permit interface [*interface-list*]

デフォルト

ユーザロールの interface policy view で許可されているインタフェースはありません。

View

User role interface policy view

定義済みユーザロール

network-admin

パラメータ

interface *interface-list*: 最大 10 個のインタフェース項目をスペースで区切り、リストを指定することができます。各インタフェースは *interface-type interface-number* あるいは *interface-type interface-number* **to** *interface-type interface-number* の形式で指定します。インタフェースの範囲を指定する場合、終了インタフェースは以下の要件に一致する必要があります。

- 開始インタフェースと同一のタイプにしてください。
- 開始インタフェースよりもインタフェース番号を大きい値にしてください。

説明

permit interface コマンドはユーザロールにアクセス可能なインタフェースのリストを設定します。

undo permit interface コマンドは指定したインタフェースのアクセスを無効にします。

interface policy deny コマンドを設定した後、インタフェースにアクセスするユーザロールを許可するため、ポリシーの許可されたインタフェースリストにインタフェースを追加する必要があります。ユーザロールで許可されたインタフェースリストのインタフェースで以下の操作を実行することができます。

- インタフェースの作成、削除、設定を行います。
- interface view へ移行します。
- **feature** コマンドでインタフェースを指定します。

作成および削除は、論理インタフェースでのみ有効です。

ユーザロールのインタフェースポリシーに許可されたインタフェースを追加するため、**permit interface** コマンドを複数繰り返すことができます。

インタフェースを指定しない場合、**undo permit interface** コマンドは許可されたインタフェースのリスト全体を削除します。

ユーザロールのインタフェースポリシーの変更は、変更後にユーザロールにログインしたユーザのみ適用されます。

例

1) ユーザロール **role1** を設定します。

interface view、VLAN view で有効なすべてのコマンドを実行するため、ユーザロール **role1** を許可します。

<AC> system-view

[AC] role name role1

[AC-role-role1] rule 1 permit command system-view ; interface *

[AC-role-role1] rule 2 permit command system-view ; vlan *

Ten-GigabitEthernet 1/0/1、Ten-GigabitEthernet 1/0/3～Ten-GigabitEthernet 1/0/5 へアクセスするため、ユーザロールを許可します。

[AC-role-role1] interface policy deny

[AC-role-role1-ifpolicy] permit interface Ten-GigabitEthernet 1/0/1 Ten-GigabitEthernet 1/0/3 to Ten-GigabitEthernet 1/0/5

[AC-role-role1-ifpolicy] quit

[AC-role-role1] quit

2) ユーザロール **role1** で Ten-GigabitEthernet 1/0/1、Ten-GigabitEthernet 1/0/3～ Ten-GigabitEthernet 1/0/5 を除いたインタフェースで動作するユーザロールが使用できないことを確認します。

Ten-GigabitEthernet 1/0/1 interface view に移行できることを確認します。

[AC] interface Ten-GigabitEthernet 1/0/1

[AC-Ten-GigabitEthernet1/0/1] quit

Ten-GigabitEthernet 1/0/5 に VLAN 10 の割り当てができることを確認します。この例では、ユーザロールのデフォルト VLAN ポリシーが使用されているため、ユーザロールはすべての VLAN にアクセスできます。

[AC] vlan 10

[AC-vlan10] port Ten-GigabitEthernet 1/0/5

[AC-vlan10] quit

Ten-GigabitEthernet 1/0/2 の interface view に移行できないことを確認します。

[AC] interface Ten-GigabitEthernet 1/0/2

```
Permission denied.
```

関連コマンド

- **display role**
- **interface policy deny**
- **role**

2.1.8 permit vlan

Syntax

permit vlan *vlan-id-list*

undo permit vlan [*vlan-id-list*]

デフォルト

ユーザロールの VLAN policy view で許可されている VLAN の設定はありません。

View

User role VLAN policy view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: VLAN を指定します。半角スペースで区切ることで 10 の VLAN を指定することができます。

各 VLAN は VLAN ID で VLAN を指定あるいは *vlan-id1* **to** *vlan-id2* の形式で指定します。VLAN ID の設定範囲は 1～4094 です。VLAN の範囲を指定する場合、*vlan-id2* は *vlan-id1* よりも大きい値にしてください。

説明

permit vlan コマンドはユーザロールにアクセスできる VLAN のリストを設定します。

undo permit vlan コマンドは指定した VLAN にアクセスするため、ユーザロールの許可を削除します。

vlan policy deny コマンドを設定したのち、VLAN にアクセスするユーザロールを許可するために、ポリシーの許可された VLAN リストに VLAN を追加する必要があります。ユーザロールで、許可された VLAN リストの VLAN で以下の操作を実行することができます。

- VLAN の作成、削除、設定を行います。
- VLAN view へ移行します。
- **feature** コマンドで VLAN を指定します。

ユーザロールの VLAN ポリシーに許可された VLAN を追加するため、**permit vlan** コマンドを複数繰り返すことができます。

VLAN を指定しない場合、**undo permit vlan** コマンドは許可された VLAN のリスト全体を削除します。

ユーザロールの VLAN ポリシーの変更は、変更後にユーザロールにログインしたユーザのみ適用されます。

デフォルトでは、すべてのアクセスポートは VLAN 1 に属します。

port access vlan コマンドを使用してアクセスポートを他のすべての VLAN に割り当てるには、VLAN 1 と新しい VLAN の両方にアクセスできるユーザロールがあることを確認します。

例

1) ユーザロール **role1** を設定します。

interface view、VLAN view で有効なすべてのコマンドを実行するため、ユーザロール **role1** を許可します。

<AC> system-view

[AC] role name role1

[AC-role-role1] rule 1 permit command system-view ; interface *

[AC-role-role1] rule 2 permit command system-view ; vlan *

VLAN 1、VLAN 2、VLAN 4、VLAN 50～VLAN 100 にアクセスするユーザロール **role1** を許可します。

[AC-role-role1] vlan policy deny

[AC-role-role1-vlanpolicy] permit vlan 1 2 4 50 to 100

[AC-role-role1-vlanpolicy] quit

[AC-role-role1] quit

2) VLAN 1、VLAN 2、VLAN 4、VLAN 50～VLAN 100 を除いた VLAN で動作するユーザロール **role1** が使用できないことを確認します。

VLAN 100 を作成し、VLAN view に移行できることを確認します。

[AC] vlan 100

[AC-vlan100] quit

アクセスポートとして VLAN 100 に Ten-GigabitEthernet 1/0/1 を追加できることを確認します。

[AC] interface Ten-GigabitEthernet 1/0/1

[AC-Ten-GigabitEthernet1/0/1] port access vlan 100

[AC-Ten-GigabitEthernet1/0/1] quit

VLAN 101 を作成し、VLAN view に移行できないことを確認します。

[AC] vlan 101

```
Permission denied.
```

関連コマンド

- **display role**
- **role**
- **vlan policy deny**

2.1.9 role

Syntax

role name *role-name*

undo role name *role-name*

デフォルト

以下の定義済みユーザロールがあります。

- network-admin
- network-operator
- level-*n* （*n* は 0～15 の整数です）

View

System view

定義済みユーザロール

network-admin

パラメータ

name *role-name*: ユーザ名を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。

説明

role コマンドはユーザロールを作成し、user role view に移行します。ユーザロールが作成されている場合、直接 user role view に移行します。

undo role コマンドはユーザロールを削除します。

定義済みのユーザロールに加えて 64 のユーザロールを作成することができます。

定義済みのユーザロールを削除することはできません。あるいは定義済みの network-admin、network-operator、level-15 に割り当てられた許可を変更することはできません。

非 AAA 認証ユーザにセキュリティ検査のロールを割り当てることはできません。

Level-0～level-14 のユーザロールのアクセス許可は、ユーザロールのルールとリソースのアクセスポリシーを使用して変更できます。

ただし、これらのユーザロールの定義済みアクセス権を変更することはできません。

これらのユーザロールのアクセス権を **display history-command all** コマンドに変更することはできません。

例

ユーザロール **role1** を作成し、user role view に移行します。

<AC> system-view

[AC] role name role1

[AC-role-role1]

関連コマンド

- **display role**
- **interface policy deny**
- **rule**
- **vlan policy deny**

2.1.10 role default-role enable

Syntax

role default-role enable [*role-name*]

undo role default-role enable

デフォルト

デフォルトユーザロール機能は無効です。ユーザロールがない AAA ユーザは装置にログインすることができません。

View

System view

定義済みユーザロール

network-admin

パラメータ

role-name: ユーザロール名を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。ユーザロールはシステムになければなりません。ユーザロールの指定がない場合、デフォルトユーザロールとしてコマンドは network-operator を指定します。

説明

role default-role enable コマンドはリモート AAA ユーザのデフォルトユーザロールを有効にします。

undo role default-role enable コマンドはデフォルトに戻します。

AAA サーバがユーザにすべてのユーザロールを許可しない場合、デフォルトユーザロール機能は AAA 認証ユーザにデフォルトユーザロールを割り当てます。これらのユーザは、デフォルトユーザロールでシステムへのアクセスが許可されます。

ローカル認証では、**authorization-attribute user role** コマンドを使用して、ユーザロールをローカルユーザに割り当てない場合、このコマンドが必要です。

AAA ユーザにユーザロールが割り当てられている場合、ユーザロールでログインします。

例

デフォルトユーザロール機能を有効にします。

<AC> system-view

[AC] role default-role enable

関連コマンド

role

2.1.11 role feature-group

Syntax

role feature-group name *feature-group-name*

undo role feature-group name *feature-group-name*

デフォルト

ユーザロールグループ **L2**、**L3** が作成されています。

View

System view

定義済みユーザロール

network-admin

パラメータ

name *feature-group-name*: 機能グループ名を指定します。設定範囲は 1～31 です。大文字、小文字を区別します。

説明

role feature-group コマンドはユーザロール機能グループを作成し、ユーザロールの group view に移行します。

undo role feature-group コマンドはユーザロール機能グループを削除します。

L2 機能グループはすべてのレイヤ 2 機能コマンドを含みます。**L3** 機能グループはすべてのレイヤ 3 機能コマンドを含みます。この定義済みの機能グループはユーザが設定できません。

定義済みの機能グループ **L2**、**L3** に加えて、64 のユーザ機能グループを作成することができます。

例

機能グループ **security-features** を作成し、その view に移行します。

<AC> system-view

[AC] role feature-group name security-features

[AC-featuregrp-security-features]

関連コマンド

- **display role feature**
- **display role feature-group**
- **feature**

2.1.12 rule

🕮 **メモ**:

web-menu のパラメータはソフトウェアバージョン 7.2.67 を含む以降のソフトウェアからサポートしています。

Syntax

rule *number* { **deny** | **permit** } { **command** *command-string* | { **execute** | **read** | **write** } * { **feature** [*feature-name*] | **feature-group** *feature-group-name* | **web-menu** [*web-string*] } }

undo rule { *number* | **all** }

デフォルト

ユーザが定義したユーザロールにルールがなく、すべてのコマンドおよび Web メニューへのアクセスができません。

View

User role view

定義済みユーザロール

network-admin

パラメータ

number: ルール番号を指定します。設定範囲は 1～256 です。

deny: 指定されたコマンドへのアクセスを拒否します。

permit: 指定されたコマンドへのアクセスを許可します。

command *command-string*: コマンドを指定します。*command-string* の設定範囲は 1～128 です。大文字、小文字を区別します。以下の記号を含むことができます。

- ワイルドカードアスタリスク(*)
- 半角スペースとタブキーの区切り記号
- 印刷可能な文字列

execute: 実行コマンドを指定します。**execute** コマンドは指定した機能あるいはプログラムを実行します。たとえば **ping** コマンドです。

read: 読み込みコマンドを指定します。**read** コマンドは設定を表示あるいは情報を維持します。たとえば、**display、dir、more、pwd** コマンドです。

write: 書き込みコマンドを指定します。**write** コマンドはシステムを設定します。たとえば、**ssh server enable** コマンドです。

feature [*feature-name*]: 1 つ以上の機能を指定します。*feature-name* は機能名を指定します。機能名を指定しない場合、システムのすべての機能を指定します。機能を指定するとき、機能名は **display role feature** コマンドで表示される名前と同一にしてください。

feature-group *feature-group-name*: ユーザ定義あるいは定義済みの機能グループを指定します。*feature-group-name* は機能グループ名を示します。設定範囲は 1～31 です。大文字、小文字を区別します。機能グループが作成されていない場合、ルールはグループが作成されたのち適用されます。作成された機能グループを表示する場合、**display role feature-group** コマンドを使用します。

web-menu [*web-string*]: Web メニューを指定します。*web-string* 引数は、Web メニューの ID パスを表し、大文字と小文字を区別しない 1 文字から 255 文字の文字列です。ID 項目の区切りには、スラッシュ (/) を使用します。
(例: m_system/m_tools/m_debug/m_diagnostic) 。
web-string を指定しない場合、ルールはすべての Web メニューに適用されます。Web メニューの ID パスを確認するには、**display web menu** コマンドを使用します。

all: すべてのユーザロールのルールを削除します。

説明

rule コマンドは制御するコマンドのユーザロールのルールを作成あるいは変更します。

undo rule コマンドはユーザロールのルールを削除します。

細分化された異なるアクセス制御を行うため、以下のルールのタイプを定義することができます。

- **Command rule**－正規表現に一致するコマンドあるいはコマンドリストへのアクセス制御を行います。
- **Feature rule**－コマンドタイプによって機能のコマンドにアクセス制御を行います。

- **Feature group rule**－コマンドタイプによって機能グループのコマンドにアクセス制御を行います。
- **Web-Menu rule** － メニュータイプによって Web メニューへのアクセスを制御します。
- **XML element rule**－要素タイプ別に XML 要素へのアクセスを制御します。
- **OID rule**－ノードタイプによって、指定された MIB ノードとその子ノードへのアクセスを制御します。

ユーザロールは、ユーザロールルールで指定されている許可されたリソースのセットにアクセスできます。

ユーザロールルールには、定義済み（sys-n で識別）およびユーザ定義のユーザロールルールが含まれます。

ユーザロールには最大 256 のユーザ定義ルールを設定できます。

ユーザ定義ユーザロールルールの総数は 1024 以下です。

ユーザロールに対するルールの変更、追加、または削除は、変更後にそのユーザロールでログインしたユーザにのみ有効になります。

ファイルシステムコマンドへのアクセスは、ファイルシステムコマンドルールとファイルシステム機能ルールの両方によって制御されます。

ファイルシステムへの出力リダイレクトを伴うコマンドは、コマンドタイプ write がファイルシステム機能に割り当てられている場合にのみ許可されます。

以下のガイドラインは、OID 以外のルールに適用されます。

- 同一タイプのユーザ定義のルールが混在した場合、高い ID のルールが適用されます。たとえば、もしユーザロールに以下のコマンドを使用したルールが含まれる場合、ユーザロールが **tracert** コマンドを使用することができますが、**ping** コマンドは使用できません。
  - **rule** *1* **permit command** *ping*
  - **rule** *2* **permit command** *tracert*
  - **rule** *3* **deny command** *ping*
- 定義済みのユーザロールのルールとユーザ定義のユーザロールが混在した場合、ユーザ定義したユーザロールが適用されます。

コマンド文字列を指定するとき、表 2-3 のガイドラインに従ってください。

表 2-3 コマンド文字列設定ルール

ルール	ガイドライン
区切り機能はセミコロン（;）です。	コマンドあるいはコマンドリストにアクセスする前に、各viewのコマンドを区切るためにセミコロンを使用してください。しかし**display**コマンドや**dir**コマンドなどuser viewやすべてのviewで有効なコマンドを区切るためにセミコロンを使用しないでください。 セミコロンで区切られたセグメントは、最小限、印刷可能な1文字がある必要があります。

ルール	ガイドライン
	viewにあるが、サブviewにないコマンドを指定する場合、最後のセグメントの最後の印刷可能な文字にセミコロンを使用してください。viewとviewのサブviewにあるコマンドを指定する場合、最後のセグメントの最後の印刷可能な文字にセミコロンを使用しないでください。 たとえば、interface viewに移行する前にsystem viewに移行してください。すべてのinterface viewの**ip**キーワードで開始するすべてのコマンドを指定するため、**system ; interface * ; ip * ;**を使用してください。 **system ; radius scheme * ;**コマンドはsystem viewの**radius scheme**キーワードで始まるすべてのコマンドを示します。**system ; radius scheme ***コマンドはsystem viewの**radius scheme**キーワードで始まるすべてのコマンドとRADIUS scheme viewのすべてのコマンドを示します。
アスタリスクがワイルドカードです。	アスタリスクは0あるいは複数の文字を示します。 最後のセグメントでない場合、セグメントの最後のみアスタリスクを使用することができます。 最後のセグメントである場合、セグメントのいずれの位置でもアスタリスクを使用することができます。アスタリスクから始まる場合、アスタリスクの後ろに印刷可能な文字を指定することができません。 たとえば、**system ; ***コマンドはsystem viewとsystem viewのサブviewで有効なすべてのコマンドを示します。**debugging * event**コマンドはuser viewで有効なすべてのイベントをデバッグするコマンドを示します。
キーワードの省略ができます。	キーワードの最初の数文字を入力することでキーワードを指定することができます。ルールに一致する文字列から始まるすべてのコマンドです。 たとえば、**rule 1 deny command dis arp source ***コマンドは**display arp source-mac interface**コマンドと**display arp source-suppression.**コマンドのアクセスを拒否します。
コマンドへのアクセスを制御するため、コマンドがあるviewの直後にコマンドを指定する必要があります。	コマンドへのアクセスを制御するため、コマンドが割り当てられたviewの直後にコマンドを指定する必要があります。 すべてのサブviewのコマンドを制御するルールはコマンドに適用されません。 たとえば、**rule 1 deny command system ; interface * ; ***コマンドはinterface viewに割り当てられたコマンドへのアクセスを無効にします。しかしこのコマンドはsystem viewよりもinterface viewで割り当てられるため、interface viewの**acl advanced**コマンドを実行することができます。

ルール	ガイドライン
	このコマンドへのアクセスを無効にする場合、**rule 1 deny command system ; acl *;**コマンドを使用します。
ユーザロールのコマンドルールの**display**コマンドを指定するとき、垂直バー（|）、大なり記号（>）、2 重大なり記号（>>）を含みません。	システムはコマンドラインの一部として記号に従うリダイレクト記号とパラメータを含みません。 ユーザロールのコマンドルールで、コマンドラインの一部にリダイレクト記号とパラメータが存在します。その結果、これらの記号を含むルールは一致するコマンドはありません。 たとえば、**rule 1 permit command display debugging > log**コマンドは、**display debugging**コマンドではなく、**display debugging > log**コマンドに一致するコマンドはありません。

例

display acl コマンドを実行するユーザロール **role1** を許可します。

<AC> system-view

[AC] role name role1

[AC-role-role1] rule 1 permit command display acl

display キーワードで開始するすべてのコマンドを実行するユーザロール **role1** を許可します。

[AC-role-role1] rule 2 permit command display *

system view の **radius scheme aaa** コマンドを実行するユーザロール **role1** を許可し、RADIUS scheme view に割り当てられたすべてのコマンドを使用します。

[AC-role-role1] rule 3 permit command system ; radius scheme aaa

すべての機能の read あるいは write コマンドへアクセスするユーザロール **role1** を拒否します。

[AC-role-role1] rule 4 deny read write feature

aaa 機能のすべての read コマンドへアクセスするユーザロール **role1** を拒否します。

[AC-role-role1] rule 5 deny read feature aaa

機能グループ **security-features** の read、write、execute コマンドへアクセスするユーザロール **role1** を許可します。

[AC-role-role1] rule 6 permit read write execute feature-group security-features

関連コマンド

- **display role**
- **display role feature**
- **display role feature-group**
- **display web menu**

- **role**

2.1.13 super

Syntax

super [*role-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

role-name: ユーザロールを指定します。設定範囲は 1～63 です。大文字、小文字を区別します。システムにユーザロールが存在する必要があります。ユーザロールを指定しない場合、デフォルトターゲットのユーザロールを取得します。

説明

super コマンドは装置に再接続することなく、別のユーザロールを取得します。

このコマンドは現在のログインでのみ適用されるため、取得されたユーザロールは一時的なユーザロールです。次回ユーザアカウントでログインすると、元のユーザロールの設定が適用されます。

装置に再接続することなく、ユーザが別のユーザロールを取得するため、ユーザロールの認証を設定する必要があります。

- ローカルパスワードがローカルパスワード認証（**local**）で設定されていない場合、AUX ユーザはいずれかの文字列を入力するか、なにも入力しないことでユーザロールの許可を取得できます。
- ローカルパスワードが local-then-remote 認証（**local scheme**）で設定されていない場合、以下のルールが適用されます。
  - VTY ユーザはリモート認証を実行します。
  - AUX ユーザはいずれかの文字列を入力するか、なにも入力しないことでユーザロールの許可を取得できます。

例

ユーザロール network-operator を取得します。

<AC> super network-operator

```
Password:
User privilege role is network-operator, and only those commands that
authorized to the role can be used.
```

関連コマンド

- **authentication super** (コマンドマニュアルのセクション 9 *セキュリティ*)
- **super authentication-mode**
- **super password**

2.1.14 super authentication-mode

Syntax

super authentication-mode { **local** | **scheme** } *

undo super authentication-mode

デフォルト

local

View

System view

定義済みユーザロール

network-admin

パラメータ

local: ローカルパスワード認証を有効にします。

scheme: リモート AAA 認証を有効にします。

説明

super authentication-mode コマンドは一時的なユーザロールの許可を取得するため認証モードを設定します。

undo super authentication-mode コマンドはデフォルトに戻します。

ローカルパスワードでは、パスワードを設定するため、**super password** コマンドを使用します。

リモート AAA 認証では、RADIUS サーバのユーザ名とパスワードを設定します。

local と **scheme** キーワードの両方を指定した場合、最初に指定されたキーワードが適用されます。

- **scheme local**– remote-then-local 認証モードを有効にします。装置は一時的なユーザロールを取得するため、最初に AAA 認証を実行します。リモート RADIUS サーバが応答しないあるいは装置の AAA の設定が無効である場合、ローカル認証が実行されます。
- **local scheme**– local-then-remote 認証モードを有効にします。装置は最初にローカルパスワード認証を実行します。ユーザロールのパスワードが設定されていない場

合、装置はリモート認証を実行します。VTY ユーザ、AUX ユーザは、文字列を入力するか、何も入力しないで別のユーザロールを取得できます。

AAA の詳細は、オペレーションマニュアルのセクション 8 *セキュリティ “AAA”* を参照してください。

例

一時的なユーザロールの許可を取得するため、local-only 認証を有効にします。

<AC> system-view

[AC] super authentication-mode local

一時的なユーザロールの許可を取得するため、remote-then-local 認証を有効にします。

<AC> system-view

[AC] super authentication-mode scheme local

関連コマンド

- **authentication super** (コマンドマニュアルのセクション 9 *セキュリティ*)
- **super password**

2.1.15 super default role

Syntax

super default role *role-name*

undo super default role

デフォルト

network-admin

View

System view

定義済みユーザロール

network-admin

パラメータ

role-name: デフォルトターゲットユーザロールの名前を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。システムにユーザロールが存在する必要があり、セキュリティ監査になることはできません。

説明

super default role コマンドは一時的なユーザロールの許可を取得するためデフォルトターゲットのユーザロールを指定します。

undo super default role コマンドはデフォルトに戻します。

コマンドのユーザロールを指定しないとき、デフォルトターゲットのユーザロールが **super** コマンドあるいは **super password** コマンドに割り当てられます。

例

一時的なユーザロールの許可を取得するため、デフォルトターゲットのユーザロールを **network-operator** に指定します。

<AC> system-view

[AC] super default role network-operator

関連コマンド

- **super**
- **super password**

2.1.16 super password

Syntax

super password [**role** *role-name*] [{ **hash** | **simple** } *string*]

undo super password [**role** *role-name*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

role *role-name*: ユーザロールを指定します。設定範囲は 1～63 です。大文字、小文字を区別します。システムにユーザロールが存在する必要があり、セキュリティ監査にはなれません。ユーザロールを指定しない場合、**super default role** コマンドを使用して設定される、デフォルトターゲットのユーザロールのパスワードを設定します。

hash: ハッシュテキストのパスワードを設定します。

simple: プレーンテキストのパスワードを設定します。セキュリティのため、ハッシュテキストで保存され、暗号化されます。

string: パスワードを指定します。大文字、小文字を区別します。

- **simple** キーワードが指定される場合、パスワードの設定範囲は 1～63 文字です。
- **hash** キーワードが指定される場合、パスワードの設定範囲は 1～110 文字です。

説明

super password コマンドはユーザロールのパスワードを設定します。

undo super password コマンドはデフォルトに戻します。

パラメータを指定しない場合、インタラクティブモードでプレーンテキストパスワードを指定します。

一時的なユーザロールの許可のローカルパスワード認証を設定する場合、パスワードを設定します。

異なるユーザロールに異なるパスワードを指定することを推奨します。

例

ユーザロール network-operator のプレーンテキストのパスワード **123456TESTplat&!** を設定します。

<AC> system-view

[AC] super password role network-operator simple 123456TESTplat&!

ユーザロール network-operator のパスワード **123456TESTplat&!**をインタラクティブモードで設定します。

<AC> system-view

[AC] super password role network-operator

```
Password:
Confirm :
Updating user information. Please wait... ...
```

関連コマンド

- **super authentication-mode**
- **super default role**

2.1.17 vlan policy deny

Syntax

vlan policy deny

undo vlan policy deny

デフォルト

VLAN へのユーザロールのアクセス可能にします。

View

User role view

定義済みユーザロール

network-admin

説明

vlan policy deny コマンドは VLAN へのユーザロールのアクセスを拒否し、ユーザロールの VLAN policy view に移行します。

undo vlan policy deny コマンドはユーザロールの VLAN policy view へのアクセスをデフォルトに戻します。

指定した VLAN のみユーザロールの VLAN へのアクセスを制限するために、以下の作業を行います。

1) vlan policy deny コマンドでユーザロールの VLAN policy へ移行します。
2) permit vlan コマンドでアクセス可能な VLAN を指定します。

🕮 **メモ**:

vlan policy deny コマンドは、**permit vlan** コマンドが設定されていない場合、すべての VLAN へのユーザロールのアクセスを拒否します。

VLAN を設定するため、ユーザロールの VLAN ポリシーで許可されている VLAN が使用されていることを確認してください。アクセス可能な VLAN で以下の操作を実行することができます。

- VLAN の作成、削除、設定を行います。
- VLAN view へ移行します。
- **feature** コマンドで VLAN を指定します。

ユーザロールの VLAN ポリシーの変更は、変更後にユーザロールにログインしたユーザのみ適用されます。

例

VLAN へのユーザロール **role1** のアクセスを拒否します。

<AC> system-view

[AC] role name role1

[AC-role-role1] vlan policy deny

[AC-role-role1-vlanpolicy] quit

VLAN50～VLAN100 を除く VLAN へのユーザロール **role1** のアクセスを拒否します。

<AC> system-view

[AC] role name role1

[AC-role-role1] vlan policy deny

[AC-role-role1-vlanpolicy] permit vlan 50 to 100

関連コマンド

- **display role**
- **permit vlan**
- **role**

目次

このセクションのページは **1-x-x** です。

3 章 ログイン 3-1
3.1 ログイン設定コマンド 3-1
3.1.1 authentication-mode 3-1
3.1.2 auto-execute command 3-3
3.1.3 databits 3-4
3.1.4 display ip http 3-5
3.1.5 display ip https 3-6
3.1.6 display line 3-7
3.1.7 display telnet client 3-9
3.1.8 display user-interface 3-10
3.1.9 display users 3-11
3.1.10 display web menu 3-13
3.1.11 display web users 3-19
3.1.12 escape-key 3-19
3.1.13 free line 3-22
3.1.14 free user-interface 3-23
3.1.15 free web users 3-24
3.1.16 history-command max-size 3-25
3.1.17 idle-timeout 3-26
3.1.18 ip http acl 3-27
3.1.19 ip http enable 3-28
3.1.20 ip http port 3-29
3.1.21 ip https acl 3-30
3.1.22 ip https enable 3-31
3.1.23 ip https port 3-32
3.1.24 line 3-32
3.1.25 line class 3-34
3.1.26 lock 3-35
3.1.27 parity 3-36
3.1.28 protocol inbound 3-37
3.1.29 screen-length 3-38
3.1.30 send 3-39
3.1.31 set authentication password 3-40
3.1.32 shell 3-42
3.1.33 speed 3-43
3.1.34 stopbits 3-44

3.1.35 telnet 3-45
3.1.36 telnet client source 3-46
3.1.37 telnet server acl 3-47
3.1.38 telnet server dscp 3-48
3.1.39 telnet server enable 3-49
3.1.40 telnet server port 3-50
3.1.41 terminal type 3-51
3.1.42 user-interface 3-52
3.1.43 user-interface class 3-53
3.1.44 user-role 3-54
3.1.45 web idle-timeout 3-55

3章 ログイン

3.1 ログイン設定コマンド

いくつかのログインコマンドは user line view と user line class view の両方で有効です。

- user line view の設定は、user line にのみ適用されます。user line class view はクラスのすべての user line に適用されます。
- user line view と user line class view のどちらかの view でデフォルトでない設定がある場合、デフォルトでない設定は、もう一方のデフォルト設定よりも優先されます。user line view のデフォルトでない設定は user line class view のデフォルトでない設定よりも優先されます。

3.1.1 authentication-mode

Syntax

authentication-mode { **none** | **password** | **scheme** }

undo authentication-mode

デフォルト

VTY line の認証モードは password です。

console lines の認証モードは none です。

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

none: 認証を無効にします。

password: ローカルパスワード認証を行います。

scheme: AAA 認証を行います。AAA の詳細はオペレーションマニュアルのセクション 9 *セキュリティ　“AAA”* を参照してください。

説明

authentication-mode コマンドは user line の認証モードを設定します。

undo authentication-mode コマンドはデフォルトに戻します。

network-admin またはレベル 15 ユーザの役割を割り当てられたユーザだけがこのコマンドを実行することができます。他のユーザがこのコマンドを実行する権利を与えられても、このコマンドを実行することができません。

認証モードが **none** である場合、すべてのユーザは認証なしでログインすることができます。装置のセキュリティを改善するため、認証モードを **password** あるいは **scheme** にしてください。

VTY line view で、**authentication-mode** コマンドは **protocol inbound** コマンドと関連します。VTY line view で 2 つのコマンドのうち、1 つコマンドのみデフォルトでない認証モードである場合、もう一方のコマンドは VTY line class view の設定に関わらず、デフォルトの認証モードを使用します。

認証モードを変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

例

user line VTY 0 で認証モードを none にします。

<AC> system-view

[AC] line vty 0

[AC-line-vty0] authentication-mode none

user line VTY 0 で認証モードを password に設定し、パスワードを 321 に設定します。

<AC> system-view

[AC] line vty 0

[AC-line-vty0] authentication-mode password

[AC-line-vty0] set authentication password simple 321

user line VTY 0 で認証モードを scheme に設定します。ローカルユーザ 123 を設定し、パスワードを 321 に設定します。Telnet サービスを割り当て、ユーザのユーザロールを network-admin に割り当てます。

<AC> system-view

[AC] line vty 0

[AC-line-vty0] authentication-mode scheme

[AC-line-vty0] quit

[AC] local-user 123

[AC-luser-manage-123] password simple 321

[AC-luser-manage-123] service-type telnet

[AC-luser-manage-123] authorization-attribute user-role network-admin

関連コマンド

set authentication password

3.1.2 auto-execute command

注意:

user line にこのコマンドを実行すると、user line による CLI アクセスができなくなる可能性があります。このコマンドを設定する前に、異なる user line によって CLI にアクセスできることを確認してください。

Syntax

auto-execute command *command*

undo auto-execute command

デフォルト

ログインユーザのために、自動的に実行されるコマンドは指定されていません。

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

command: 自動で実行されるコマンドを指定します。

説明

ログインユーザが自動的に実行するコマンドを指定するために、**auto-execute command** を使用します。デフォルトを復元するには、**undo auto-execute command** を使用してください。

auto-execute コマンドは、console line view と console line class view ではサポートされません。

このコマンドは user line view と user line class view の両方において実行可能です。どちらの view における非デフォルト設定も他の view におけるデフォルト設定に優先します。user line view における非デフォルト設定は user line class view における非デフォルト設定に優先します。

auto-execute コマンドを使用して変更された設定は、現在のセッションには適用されません。

ユーザが現在の user line にログインしたとき、装置は指定されたコマンドを自動で実行します。指定したコマンドが別の作業を引き起こす場合、装置は作業が完了するまでユーザの接続を切断しません。コマンドが他の作業を引き起こさない場合、装置はコマンド実行後にユーザの接続を切断します。

auto-execute command telnet *X.X.X.X* コマンドを設定すると、装置は Telnet ユーザを X.X.X.X のホストにリダイレクトさせます。ユーザが X.X.X.X との Telnet 接続を削除した場合、装置との接続は切断されます。

例

ユーザが VTY line 0 にログインした後、自動的に Telnet192.168.1.41 を実行するように設定します。

<AC> system-view

[AC] line vty 0

[AC-line-vty0] auto-execute command telnet 192.168.1.41

```
This action will lead to configuration failure through line-vty0. Are you sure?
[Y/N]:y
[AC-line-vty0]
```

設定を確認するため、192.168.1.40 に Telnet します。

装置は自動的に 192.168.1.41 に Telnet し、以下の出力が表示されます。

C:¥> telnet 192.168.1.40

```
<AC>
Trying 192.168.1.41 ...
Press CTRL+K to abort
Connected to 192.168.1.41 ...
<AC.41>
```

この動作は、Telnet で 192.168.1.41 に直接ログインすることと同一です。192.168.1.41 への Telnet 接続を終了するとき、同時に 192.168.1.40 への Telnet 接続も終了されます。

3.1.3 databits

Syntax

databits { **5** | **6** | **7** | **8** }

undo databits

デフォルト

8

View

User line view

定義済みユーザロール

network-admin

パラメータ

5: データビット数 5 を指定します。モデム dial-in にのみ適用可能なキーワードです。

6: データビット数 6 を指定します。モデム dial-in にのみ適用可能なキーワードです。

7: データビット数 7 を指定します。

8: データビット数 8 を指定します。

説明

databits コマンドは各文字のデータビット数を指定します。

undo databits コマンドはデフォルトに戻します。

このコマンドは VTY line view でサポートしていません。

この設定は端末のデータビットと同一にしてください。

例

CONSOLE 0 のデータビットを 7 に設定します。

<AC> system-view

[AC] line console 0

[AC-line-console0] databits 5

3.1.4 display ip http

Syntax

display ip http

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ip http コマンドは HTTP サービスの設定とステータス情報を表示します。

例

HTTP サービスの設定とステータス情報を表示します。

<AC> display ip http

```
HTTP port: 80
Basic ACL: 2222
HTTP status: Enabled
```

表 3-1 コマンド出力

フィールド	説明
HTTP port	HTTPサービスのポート番号です。
Basic ACL	HTTPアクセスを制御するために使用されるACLです。HTTPサービスにACLが割り当てられていない場合、0と表示されます。
HTTP status	HTTPサービスが有効かどうかを示します。

関連コマンド

- **ip http acl**
- **ip http enable**
- **ip http port**

3.1.5 display ip https

Syntax

display ip https

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ip https コマンドは HTTPS サービスの設定とステータス情報を表示します。

例

HTTPS サービスの設定とステータス情報を表示します。

<AC> display ip https

```
HTTPS port: 443
SSL server policy: test
```

```
Certificate access control policy: Not configured
Basic ACL: 2222
HTTPS status: Enabled
```

表 3-2 コマンド出力

フィールド	説明
HTTPS port	HTTPSサービスのポート番号です。
SSL server policy	HTTPSサービスに割り当てられたSSLサービスポリシーです。HTTPSサービスにSSLサービスポリシーが割り当てられていない場合、**Not configured**と表示されます。
Certificate access-control-policy	クライアントアクセス権の制御に使用される証明書属性ベースのアクセスコントロールポリシーです。HTTPSサービスにアクセスコントロールポリシーが割り当てられていない場合、**Not configured**と表示されます。
Basic ACL	HTTPSアクセスを制御するために使用されるACLです。HTTPSサービスにACLが割り当てられていない場合、**0**と表示されます。
HTTPS status	HTTPSサービスが有効かどうかを示します。

関連コマンド

- **ip https acl**
- **ip https certificate access-control-policy**
- **ip https enable**
- **ip https port**
- **ip https ssl-server-policy**

3.1.6 display line

Syntax

display line [*number1* | { **console** | **vty** } *number2*] [**summary**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

number1: user line の絶対番号を指定します。（0～32）

console *number2*: console line の相対番号 0 を指定します。

vty *number2*: VTY line の相対番号を指定します（0～31）。

summary: user line についての概要情報を表示します。このキーワードを指定しない場合、詳細な情報が表示されます。

説明

display line コマンドは user line の情報を表示します。

例

user line の情報を表示します。

<AC> display line 0

```
Idx  Type     Tx/Rx      Modem Auth  Int       Location
0    CON 0    9600       -       N   -          1/0


+    : Line is active.
F    : Line is active and in async mode.
Idx  : Absolute index of line.
Type : Type and relative index of line.
Auth : Login authentication mode.
Int  : Physical port of the line.
A    : Authentication use AAA.
N    : No authentication is required.
P    : Password authentication.
```

表 3-3 コマンド出力

フィールド	説明
Modem	モデムのモードがin/outを示します。デフォルトでは設定されていません。ハイフン(－)が表示されます。
Int	lineの物理ポートです。lineに物理ポートがない、あるいはコンソールlineの場合、ハイフン(－)が表示されます。
Location	lineの物理的な位置を表示します。スロット番号/CPU番号の形式です。

すべての user line の概要情報を表示します。

<AC> display line summary

```
Line type : [CON]
        0:XXXX
Line type : [VTY]
```

```
  4:UUUU UXXX XXXX XXXX
 20:XXXX XXXX XXXX XXXX
 5 lines used.     (U)
31 lines not used.  (X)
```

表 3-4 コマンド出力

フィールド	説明
number:status	*number*はuser line classの最初のuser lineの通し番号を示します。0からの番号です。*status*はuser line classのuser lineが使用されているかどうかを示します。Xは未使用でUは使用されています。 例えば、"2:UXXX X"が表示された場合、user line classには絶対番号2～6を使用する5つのuser lineが存在します。user line2は使用中で、その他のuser lineは未使用です。

3.1.7 display telnet client

Syntax

display telnet client

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display telnet client コマンドは、Telnet クライアント用のパケットの送信元の設定を表示します。

例

Telnet クライアント用のパケットの送信元の設定を表示します。

<AC> display telnet client

```
The source IP address is 1.1.1.1.
```

関連コマンド

telnet client source

3.1.8 display user-interface

Syntax

display user-interface [*number1* | { **console** | **vty** } *number2*] [**summary**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

number1: user line の絶対番号です。

以下のマトリクスは *number1* 引数の値の範囲を示します（0～32）。

console *number2*: console line の相対番号 0 を指定します。**vty** *number2*: VTY line の相対番号を指定します（0～31）。

summary: user line の概要を表示します。指定しない場合、詳細な情報を表示します。

説明

display user-interface コマンドは user line の情報を表示します。

このコマンドは古いソフトウェアバージョンで使用していたユーザのためにサポートされているコマンドです。古いソフトウェアバージョンで動作するコマンドです。**display line** コマンドと同一機能です。通常は **display line** コマンドを使用してください。

例

user line の情報を表示します。

<AC> display user-interface 0

```
  Idx  Type    Tx/Rx     Modem Auth  Int       Location
  0    CON 0   9600      -    N     -         0/0
  +    : Line is active.
  F    : Line is active and in async mode.
  Idx  : Absolute index of line.
  Type : Type and relative index of line.
  Auth : Login authentication mode.
  Int  : Physical port of the line.
  A    : Authentication use AAA.
  N    : No authentication is required.
  P    : Password authentication.
```

表 3-5 コマンド出力

フィールド	説明
Modem	モデムのモードがin/outを示します。デフォルトでは設定されていません。ハイフン(－)が表示されます。
Int	lineの物理ポートです。lineに物理ポートがない、あるいはコンソールlineの場合、ハイフン(－)が表示されます。
Location	lineの物理的な位置を表示します。スロット番号/CPU番号の形式です。

すべての user line の概要情報を表示します。

<AC> display user-interface summary

```
Line type : [CON]
        0:XXXX
Line type : [VTY]
        4:UUUU UXXX XXXX XXXX
       20:XXXX XXXX XXXX XXXX
 5 lines used.     (U)
31 lines not used.  (X)
```

表 3-6 コマンド出力

フィールド	説明
number:status	*number*はuser line classの最初のuser lineの通し番号を示します。0からの番号です。*status*はuser line classのuser lineが使用されているかどうかを示します。**X** は未使用でUは使用されています。 例えば、"2:UXXX X"が表示された場合、user line classには絶対番号2～6を使用する5つのuser lineが存在します。user line2は使用中で、その他のuser lineは未使用です。

3.1.9 display users

Syntax

display users [**all**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: 装置でサポートされるすべての user line を表示します。

説明

display users コマンドは、オンライン CLI ユーザの情報を表示します。

例

オンライン CLI ユーザの情報を表示します。

<AC> display users

```
  Idx  Line     Idle      Time             Pid     Type
  10   VTY 0    00:10:49   Jun 11 11:27:32   320     TEL
+ 11   VTY 1    00:00:00   Jun 11 11:39:40   334     TEL

Following are more details.
VTY 0   :
       Location: 192.168.1.12
VTY 1   :
       Location: 192.168.1.26
 +    : Current operation user.
 F    : Current operation user works in async mode.
```

出力は、2 つのユーザが装置にログインしたことを示します。一方は user line VTY 0 を使用し、もう一方（使用者自身）は VTY 1 を使用します。使用者の IP アドレスは 192.168.1.26 です。

表 3-7 コマンド出力

フィールド	説明
Idx	user lineの通し番号です。
Line	user lineのタイプとタイプごとの番号です。
Idle	ユーザがログインしてからの経過時間です。hh:mm:ssで表示します。
Time	ユーザのログイン時間です。
Pid	ユーザセッションのプロセスIDです。
Type	ユーザタイプです。 • **TEL**—Telnetユーザです。 • **SSH**—SSHユーザです。
+	カレントユーザが使用しているuser lineを示します。

フィールド	説明
Location	カレントユーザのIPアドレスです。

3.1.10 display web menu

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.67 を含む以降のソフトウェアからサポートしています。

Syntax

display web menu

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display web menu コマンドは Web コンソールのナビゲーションツリー情報を表示します。

例

Web コンソールのナビゲーションツリー情報を表示します。

<AC>display web menu

```
.
|--m_system: ID = m_system
|    |--m_dashboard: ID = m_dashboard
|    |--Network Configuration: ID = m_controller
|    |    |--Mobility Domain: ID = m_mobilitydomain
|    |    |    `--Roaming: ID = m_roamoutstation
|    |    |--Network Interfaces: ID = m_networkinterfaces
|    |    |    |--m_interface: ID = m_interface
|    |    |    `--m_lagg: ID = m_lagg
|    |    |--VLAN: ID = m_vlan
|    |    |    |--m_vlan: ID = m_vlan
|    |    |    |--m_mac: ID = m_mac
|    |    |    `--m_stp: ID = m_stp
```

```
|   |   |--Network Routing: ID = m_networkrouting
|   |   |   |--m_routingtable: ID = m_routingtable
|   |   |   `--m_staticrouting: ID = m_staticrouting
|   |   |--Network Services: ID = m_networkservices
|   |   |   |--IP Services: ID = m_ipservices
|   |   |   |   |--m_ip: ID = m_ip
|   |   |   |   `--m_ipv6: ID = m_ipv6
|   |   |   |--DHCP/DNS: ID = m_dhcpdns
|   |   |   |   |--m_dhcp: ID = m_dhcp
|   |   |   |   |--m_dhcpsnooping: ID = m_dhcpsnooping
|   |   |   |   |--IPv4 DNS: ID = m_dns
|   |   |   |   `--IPv6 DNS: ID = m_ipv6dns
|   |   |   |--Multicast: ID = m_multicast
|   |   |   |   |--m_igmpsnooping: ID = m_igmpsnooping
|   |   |   |   `--m_mldsnooping: ID = m_mldsnooping
|   |   |   |--ARP: ID = m_arp
|   |   |   |   `--m_arp: ID = m_arp
|   |   |   |--ND: ID = m_nd
|   |   |   |   `--m_nd: ID = m_nd
|   |   |   `--m_nat: ID = m_nat
|   |   |--Management Protocols: ID = m_managementprotocols
|   |   |   |--m_http: ID = m_http
|   |   |   |--m_ftp: ID = m_ftp
|   |   |   |--m_telnet: ID = m_telnet
|   |   |   |--m_ssh: ID = m_ssh
|   |   |   |--m_ntp: ID = m_ntp
|   |   |   |--m_lldp: ID = m_lldp
|   |   |   `--m_logsettings: ID = m_logsettings
|   |   `--NetMeister Settings: ID = m_netmeister
|   |       `--NetMeister Settings: ID = m_netmeister
|   |--Network Security: ID = m_networksecurity
|   |   |--Packet Filter: ID = m_packetfilter
|   |   |   `--m_packetfilter: ID = m_packetfilter
|   |   |--Traffic Policy: ID = m_trafficpolicy
|   |   |   |--m_mqc: ID = m_mqc
|   |   |   `--m_priority: ID = m_priority
|   |   |--Access Control: ID = m_accesscontrol
|   |   |   `--m_8021x: ID = m_8021x
|   |   |--Authentication: ID = m_authentication
|   |   |   |--m_ispdomain: ID = m_ispdomain
|   |   |   `--m_radius: ID = m_radius
|   |   `--User Management: ID = m_usermanagement
|   |       `--m_localuser: ID = m_localuser
```

```
|    |--System: ID = m_system
|    |    |--Event Logs: ID = m_syslogtop
|    |    |    `--Event Logs: ID = m_syslog
|    |    |--Resource: ID = m_resource
|    |    |    |--IPv4 ACL: ID = m_ipv4acl
|    |    |    |--IPv6 ACL: ID = m_ipv6acl
|    |    |    |--m_macacl: ID = m_macacl
|    |    |    |--m_timerange: ID = m_timerange
|    |    |    `--User Profile: ID = m_userprofile
|    |    |--File Systems: ID = m_filesys
|    |    |    `--File System Management: ID = m_filesystem
|    |    |--License Management: ID = m_license
|    |    |    |--License configuration: ID = m_liccfg
|    |    |    |--Obtain DID: ID = m_licdid
|    |    |    |--Licenses and features: ID = m_licbrief
|    |    |    `--Compress: ID = m_liccompress
|    |    |--Administrators: ID = m_administrator
|    |    |    `--m_admin: ID = m_admin
|    |    `--Management: ID = m_management
|    |         |--m_devicesettings: ID = m_devicesettings
|    |         |--m_config: ID = m_config
|    |         |--m_upgrade: ID = m_upgrade
|    |         |--m_reboot: ID = m_reboot
|    |         `--m_about: ID = m_about
|    `--Tools: ID = m_tools
|         |--Debug: ID = m_debug
|         |    `--m_diagnostic: ID = m_diagnostic
|         |--Ping: ID = m_ping
|         |    |--IPv4 Ping: ID = m_ping4
|         |    `--IPv6 Ping: ID = m_ping6
|         `--Tracert: ID = m_tracert
|              |--IPv4 Tracert: ID = m_tracert4
|              `--IPv6 Tracert: ID = m_tracert6
|--m_global: ID = m_global
|    |--m_dashboard: ID = m_dashboard
|    |--Quick Start: ID = m_quickaction
|    |    |--Add AP: ID = m_addaptop
|    |    |    `--Add AP: ID = m_addap
|    |    |--Add Services: ID = m_addssidtop
|    |    |    `--Add Services: ID = m_addssid
|    |    `--Add User: ID = m_addusertop
|    |         `--Add User: ID = m_adduser
|    |--Monitoring: ID = m_monitoring
```

```
|   |   |--Wireless Networks: ID = m_monwirelessnetworks
|   |   |   `--Wireless Services: ID = m_monssid
|   |   |--Access Points: ID = m_monaccesspoints
|   |   |   |--APs: ID = m_monaps
|   |   |   `--AP Groups: ID = m_monapgroups
|   |   |--Clients: ID = m_monclients
|   |   |   `--Clients: ID = m_monclients
|   |   |--Wireless Security: ID = m_wipssecurity
|   |   |   `--WIPS: ID = m_wipsdashboard
|   |   |--RF Monitoring: ID = m_rfmonitoring
|   |   |   |--RRM: ID = m_monrfoptimization
|   |   |   `--Spectrum Analysis: ID = m_monitoringspectrumanalysis
|   |   |--Client Proximity Sensor: ID = m_monprobes
|   |   |   `--Client Proximity Sensor: ID = m_monprobe
|   |   `--Application Monitoring: ID = m_appmonitoring
|   |       |--Bonjour: ID = m_monbonjour
|   |       `--Multicast Optimization: ID = m_monitoringmulticast
|   |--Wireless Configuration: ID = m_wsconfig
|   |   |--Wireless Networks: ID = m_wirelessnetworks
|   |   |   |--Wireless Networks: ID = m_servicetemplate
|   |   |   `--Hotspot2.0: ID = m_hotspot
|   |   |--AP Management: ID = m_apmanage
|   |   |   |--AP: ID = m_accesspoints
|   |   |   |--AP Groups: ID = m_apgroups
|   |   |   |--AP Global Settings: ID = m_apsettings
|   |   |   |--AP Provisioning: ID = m_approvision
|   |   |   `--AP Group Provisioning: ID = m_apgroupprovision
|   |   |--Wireless QoS: ID = m_wlanqos
|   |   |   |--Client Rate Limit: ID = m_clientratelimit
|   |   |   |--Bandwidth Guarantee: ID = m_bandwidthguarantee
|   |   |   `--Wi-Fi Multimedia: ID = m_wifimultimedia
|   |   |--Wireless Security: ID = m_wirelesssecurity
|   |   |   |--WIPS: ID = m_wips
|   |   |   |   |--WIPS Enable: ID = m_wipsenable
|   |   |   |   |--VSD: ID = m_vsd
|   |   |   |   |--Classification: ID = m_classfy
|   |   |   |   |--Detection: ID = m_detect
|   |   |   |   |--Signature: ID = m_signature
|   |   |   |   |--Countermeasure: ID = m_counter
|   |   |   |   |--Classification rule: ID = m_classrule
|   |   |   |   |--Signature rule: ID = m_signarule
|   |   |   |   `--Ignore MAC: ID = m_ignoremac
|   |   |   `--Allowlist and denylist: ID = m_wuac
```

```
|   |   |       |--Allowlist: ID = m_white
|   |   |       |--Static denylist: ID = m_staticblack
|   |   |       `--Dynamic denylist: ID = m_dynamicblack
|   |   |--Radio Management: ID = m_radiomanage
|   |   |   |--Radio Configuration: ID = m_radio
|   |   |   |--RRM: ID = m_rfoptimization
|   |   |   |--Spectrum Analysis: ID = m_spectrumanalysis
|   |   |   |--Load Balancing: ID = m_loadbalancing
|   |   |   `--Band Navigation: ID = m_bandnavigation
|   |   |--Client Proximity Sensor: ID = m_probecfg
|   |   |   `--Client Proximity Sensor: ID = m_probe
|   |   `--Applications: ID = m_applications
|   |       |--Mesh Services: ID = m_meshservices
|   |       |--Multicast Optimization: ID = m_multicastvideooptimization
|   |       |--Location Aware: ID = m_locationaware
|   |       `--Bonjour: ID = m_bonjour
|   |--Network Security: ID = m_networksecurity
|   |   |--Packet Filter: ID = m_packetfilter
|   |   |   `--m_packetfilter: ID = m_packetfilter
|   |   |--Traffic Policy: ID = m_trafficpolicy
|   |   |   |--m_mqc: ID = m_mqc
|   |   |   `--m_priority: ID = m_priority
|   |   |--Access Control: ID = m_accesscontrol
|   |   |   `--m_8021x: ID = m_8021x
|   |   |--Authentication: ID = m_authentication
|   |   |   |--m_ispdomain: ID = m_ispdomain
|   |   |   `--m_radius: ID = m_radius
|   |   |--BYOD: ID = m_byod
|   |   |   |--BYOD Rules: ID = m_byod
|   |   |   `--BYOD Authorization: ID = m_byodauth
|   |   |--User Management: ID = m_usermanage
|   |   |   `--m_localuser: ID = m_localuser
|   |   |--Guest Management: ID = m_guestmanage
|   |   |   |--Guest List: ID = m_guestlist
|   |   |   |--Import Guests: ID = m_importguest
|   |   |   |--Generate Guest Accounts: ID = m_generateguest
|   |   |   |--Approve Guest: ID = m_approveguest
|   |   |   `--Guest Configuration: ID = m_guestsyscfg
|   |   `--m_access: ID = m_access
|   |       |--MAC Authentication: ID = m_maca
|   |       |--Port Security: ID = m_portsec
|   |       `--m_portal: ID = m_portal
|   |--System: ID = m_system
```

```
|   |   `--Resource: ID = m_resource
|   |       |--IPv4 ACL: ID = m_ipv4acl
|   |       |--IPv6 ACL: ID = m_ipv6acl
|   |       |--m_macacl: ID = m_macacl
|   |       |--m_timerange: ID = m_timerange
|   |       |--VLAN Groups: ID = m_vlangroup
|   |       `--User Profile: ID = m_userprofile
|   |--Tools: ID = m_tools
|   |   |--Wireless Capture: ID = m_wirelesscapture
|   |   |   `--Wireless Packet Capture: ID = m_wirelesscapture
|   |   |--RF Ping: ID = m_rfping
|   |   |   `--RF Ping: ID = m_rfping
|   |   `--Debug: ID = m_debug
|   |       |--m_diagnostic: ID = m_diagnostic
|   |       `--AP Diagnostic Log: ID = m_apdiagnostic
|   `--Reporting: ID = m_reporting
|       |--Client Statistics: ID = m_clientreports
|       |   |--Access Category Frames: ID = m_acframe
|       |   |--Access Category Bytes: ID = m_acbyte
|       |   |--Total Frames: ID = m_totalframe
|       |   `--Total Bytes: ID = m_totalbyte
|       |--AP Statistics: ID = m_apreports
|       |   `--APs: ID = m_apreports
|       `--Wireless Service Statistics: ID = m_wsreport
|           `--Wireless Services: ID = m_wsreport
|--m_apnode: ID = m_apnode
|   `--Wireless Configuration: ID = m_wsconfig
|       |--AP Management: ID = m_apmanage
|       |   |--AP Details: ID = m_apdetail
|       |   |--Edit AP: ID = m_apconfig
|       |   `--AP Provision: ID = m_approvision
|       |--Applications: ID = m_applications
|       |   `--Location Aware: ID = m_locationaware
|       `--Radio Management: ID = m_radiomanage
|           `--Radio Configuration: ID = m_radio
`--m_apgroup: ID = m_apgroup
    `--Wireless Configuration: ID = m_wsconfig
        `--AP Management: ID = m_apmanage
            |--Access Points: ID = m_accesspoints
            |--AP Group Details: ID = m_apgdetail
            |--Edit AP Group: ID = m_apgsetting
            |--AP Provision: ID = m_approvision
            `--AP Group Provision: ID = m_apgroupprovision
```

3.1.11 display web users

Syntax

display web users

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display web users コマンドはオンライン Web ユーザを表示します。

例

オンライン Web ユーザを表示します。

<AC> display web users

```
UserID         Name           Type   Language JobCount LoginTime LastOperation
AB2039483271293 Administrator   HTTP   Chinese    3    12:00:23  14:10:05
F09382BA2014AC8 user           HTTPS  English    1    13:05:00  14:11:00
```

表 3-8 コマンド出力

フィールド	説明
UserID	オンラインWebユーザを一意に識別するために使用されるIDです。
JobCount	ユーザによって接続が確立された数です。

3.1.12 escape-key

Syntax

escape-key { *key-string* | **default** }

undo escape-key

デフォルト

Ctrl+C

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

key-string: ショートカットキーを指定します。d と D を除いた文字列あるいは ASCII コードで指定します。文字列は大文字、小文字を区別します。ASCII コードの設定範囲は 0～127 です。たとえば、**escape-key** 1 コマンドを設定した場合、ショートカットキーは **Ctrl+A** です。**escape-key a** コマンドを設定した場合、ショートカットキーは **a** です。**d** または **D** の文字列を指定するならば、ショートカットキーは **Ctrl+C** です。ショートカットキーとして **d** または **D** を使うためには、この ASCII コード値を指定しなければなりません。**Ctrl** キーを使用する ASCII コードの詳細は表 3-9 を参照してください。

表 3-9 Ctrl キーを使用する ASCII コード

フィールド	説明
Ctrl+A	1
Ctrl+B	2
Ctrl+C	3
Ctrl+D	4
Ctrl+E	5
Ctrl+F	6
Ctrl+G	7
Ctrl+H	8
Ctrl+I	9
Ctrl+J	10
Ctrl+K	11
Ctrl+L	12
Ctrl+M	13
Ctrl+N	14

フィールド	説明
Ctrl+O	15
Ctrl+P	16
Ctrl+Q	17
Ctrl+R	18
Ctrl+S	19
Ctrl+T	20
Ctrl+U	21
Ctrl+V	22
Ctrl+W	23
Ctrl+X	24
Ctrl+Y	25
Ctrl+Z	26

default: エスケープキーを Ctrl+C に戻します。

説明

escape-key コマンドはエスケープキーを設定します。

undo escape-key コマンドはエスケープキーを無効にします。

実行したコマンドを中断する場合、エスケープキーを押下します。たとえば、ping コマンド、tracert コマンドを中断する場合に使用します。デフォルトで Ctrl+C が指定されているかどうかはコマンドの実装によって異なります。詳細はコマンドのガイドラインに従ってください。

エスケープキーとしてキーシーケンスを使用します。エスケープシーケンスとして 1 文字を指定する場合、実行したコマンドを中断するとき、キーを押下します。コマンドが実行されない場合、共通文字列として入力されます。

もし、装置からリモート装置へ telnet 接続する場合、キーを押すことにより、文字はリモート装置の共通文字列として入力されます。

以下の条件が満たされている場合に、キーはリモート装置上で、escape キーの働きをします。

- ローカル装置を管理する場合、キーを押すと同一の文字列で入力されます。
- 別の装置に Telnet しリモート装置を管理する場合、キーを押しても動作しません。

undo escape-key コマンドは現在のエスケープキーを無効にします。

コマンドは user line view と user line class view で有効です。user line view と user line class view のどちらかの view でデフォルトでない設定がある場合、デフォルトでない設定は、もう一方のデフォルト設定よりも優先されます。user line view のデフォルトでない設定は user line class view のデフォルトでない設定よりも優先されます。

user line view で設定した場合、現在のセッションにすぐに適用します。user line class view で設定を変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

現在のエスケープキーを表示する場合、**display current-configuration | include escape-key** コマンドを使用します。

例

console line 0 でエスケープキーとして a を設定します。

<AC> system-view

[AC] line console 0

[AC-line-console0] escape-key a

設定を確認します。

1) IP アドレス 192.168.1.49 に ping を実行します。-c パラメータを使用して ICMP エコーリクエストパケットの数を 20 に設定します。

<AC> ping -c 20 192.168.1.49

```
PING 192.168.1.49: 56  data bytes, press a to break
  Reply from 192.168.1.49: bytes=56 Sequence=1 ttl=255 time=3 ms
  Reply from 192.168.1.49: bytes=56 Sequence=2 ttl=255 time=3 ms
```

2) a を押下します。

システムはコマンドを中断し、user view に戻ります。

```
--- 192.168.1.49 ping statistics ---
  2 packet(s) transmitted
  2 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 3/3/3 ms
<AC>
```

3.1.13 free line

Syntax

free line { *number1* | { **console** | **vty** } *number2* }

View

User view

定義済みユーザロール

network-admin

パラメータ

number1: user line の絶対番号です（0～32）。

console *number2*: console line の相対番号を指定します。

vty *number2*: VTY line の相対番号を指定します（0～31）。

説明

free line コマンドは user line を切断します。

カレントユーザを切断することはできません。

例

オンラインユーザを表示します。

<AC> display users

```
  Idx  Line     Idle      Time             Pid     Type
  10   VTY 0    00:10:49   Jun 11 11:27:32   320     TEL
+ 11   VTY 1    00:00:00   Jun 11 11:39:40   334     TEL

Following are more details.
VTY 0   :
       Location: 192.168.1.12
VTY 1   :
       Location: 192.168.1.26
 +    : Current operation user.
 F    : Current operation user works in async mode.
```

user line VTY 1 を切断します。

<AC> free line vty 1

```
Are you sure to free line vty1? [Y/N]:y
 [OK]
```

3.1.14 free user-interface

Syntax

free user-interface { *number1* | { **console** | **vty** } *number2* }

View

User view

定義済みユーザロール

network-admin

パラメータ

number1: user line の絶対番号です（0～32）。

console *number2*: console line の相対番号を指定します。

vty *number2*: VTY line の相対番号を指定します（0～31）。

説明

free user-interface コマンドは user line を切断します。

カレントユーザを切断することはできません。

このコマンドは古いソフトウェアバージョンで使用していたユーザのためにサポートされているコマンドです。古いソフトウェアバージョンで動作するコマンドです。**free line** コマンドと同一機能です。通常は **free line** コマンドを使用してください。

例

オンラインユーザを表示します。

<AC> display users

```
  Idx  LINE     Idle      Time            Pid     Type
  10   VTY 0    00:10:49   Jun 11 11:27:32   320     TEL
+ 11   VTY 1    00:00:00   Jun 11 11:39:40   334     TEL
Following are more details.
VTY 0   :
       Location: 192.168.1.12
VTY 1   :
       Location: 192.168.1.26
 +    : Current operation user.
 F    : Current operation user works in async mode.
```

VTY 1 を切断します。

<AC> free user-interface vty 1

```
Are you sure to free line vty1? [Y/N]:y
 [OK]
```

3.1.15 free web users

Syntax

free web users { **all** | **user-id** *user-id* | **user-name** *user-name* }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべての Web ユーザを指定します。

user-id: Web ユーザの ID を指定します。15 桁の 16 進数表示です。ユーザを識別するため、各 Web ユーザに一意の ID を割り当てます。

user-name: Web ユーザのユーザ名を指定します。設定範囲は 1～255 文字です。大文字、小文字を区別します。

説明

free web users コマンドはオンライン Web ユーザをログオフします。

例

すべてのオンライン Web ユーザをログオフします。

<AC> free web users all

関連コマンド

display web users

3.1.16 history-command max-size

Syntax

history-command max-size *size-value*

undo history-command max-size

デフォルト

10

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

size-value: 履歴コマンドをバッファに保存できる最大数を指定します。設定範囲は 0～256 です。

説明

history-command max-size コマンドは user line のコマンドの履歴をバッファに保存する最大数を設定します。

undo history-command max-size コマンドはデフォルトに戻します。

各 user line は、実行された有効なコマンドを別のバッファに保存します。バッファサイズはバッファにいくつの履歴コマンドを保存できるかを決定します。

カレント user line で保存された履歴コマンドを表示する場合、矢印キーの↑あるいは↓を押下するか、**display history-command** コマンドを実行します。詳細はオペレーションマニュアルのセクション 1 *はじめに　“CLI”* を参照してください。

CLI セッションを終了すると、履歴コマンドのバッファはクリアされます。

user line view での設定は現在のセッションにすぐさま適用されます。user line class view での設定は、設定が行われた後、ログインセッションで適用されます。

例

user line Console 0 のコマンドの履歴をバッファに記録する最大数を 20 に設定します。

<AC> system-view

[AC] line console 0

[AC-line-console0] history-command max-size 20

3.1.17 idle-timeout

Syntax

idle-timeout *minutes* [*seconds*]

undo idle-timeout

デフォルト

10 分

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

minutes: タイムアウト時間の分を指定します。設定範囲は 0～35791 です。デフォルトは 10 分です。

seconds: タイムアウト時間の秒を指定します。設定範囲は 0～59 です。デフォルトは 0 秒です。

説明

idle-timeout コマンドは CLI セッションがタイムアウトする時間を設定します。

undo idle-timeout コマンドはデフォルトに戻します。

ユーザ操作が実行されずにタイムアウト時間が経過すると、ユーザ接続を切断します。

タイムアウト時間を 0 にすると、**idle-timeout** コマンドを無効にし、セッションがタイムアウトしません。

user line view での設定は現在のセッションにすぐさま適用されます。user line class view での設定は、設定が行われた後、ログインセッションで適用されます。

例

user line Console 0 の CLI セッションのタイムアウト時間を 1 分 30 秒に設定します。

<AC> system-view

[AC] line console 0

[AC-line-console0] idle-timeout 1 30

3.1.18 ip http acl

Syntax

ip http acl { *acl-number* | **name** *acl-name* }

undo ip http acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

acl-number: ACL の番号を指定します。設定範囲は 2000～2999 です。

name *acl-name*: ACL の名前を指定します。大文字と小文字を区別しません。1～63 文字です。英文字ではじめてください。混乱を防ぐため all には設定できません。指定された ACL は、ACL が存在しベーシック ACL の場合に適用されます。

説明

ip http acl コマンドは HTTP サービスに ACL を適用します。

undo ip http acl コマンドはデフォルトに戻します。

ip http acl コマンドを複数回実行する場合、最新の設定が適用されます。

適用された ACL に許可されたクライアントのみ、HTTP で装置にアクセスできます。

例

10.10.0.0/16 のユーザのみが HTTP を通して装置にアクセスできるように HTTP サービスに ACL2001 を割り当てます。

<AC> system-view

[AC] acl basic 2001

[AC-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255

[AC-acl-ipv4-basic-2001] quit

[AC] ip http acl 2001

関連コマンド

acl（コマンドマニュアルのセクション 8 *ACL and QoS* ）

3.1.19 ip http enable

Syntax

ip http enable

undo ip http enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ip http enable コマンドは HTTP サービスを有効にします。

undo ip http enable コマンドは HTTP サービスを無効にします。

ユーザが HTTP を通して装置にアクセスする場合、HTTP サービスを有効にする必要があります。

例

HTTP サービスを有効にします。

<AC> system-view

[AC] ip http enable

関連コマンド

ip https enable

3.1.20 ip http port

Syntax

ip http port *port-number*

undo ip http port

デフォルト

80

View

System view

定義済みユーザロール

network-admin

パラメータ

port-number: HTTP サービスのポート番号を指定します。設定範囲は 1～65535 です。

説明

ip http port コマンドは HTTP サービスのポート番号を指定します。

undo ip http port コマンドはデフォルトに戻します。

HTTP サービスが有効であるとき、HTTP サービスのポート番号を変更した場合、HTTP サービスを再度有効にし、すべての HTTP 接続を切断します。再度ログインする場合、ユーザは Web ブラウザのアドレスバーで新しい URL を入力する必要があります。

例

HTTP サービスのポート番号を 80 に指定します。

<AC> system-view

[AC] ip http port 80

3.1.21 ip https acl

Syntax

ip https acl { *acl-number* | **name** *acl-name* }

undo ip https acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

acl-number: ACL の番号を指定します。設定範囲は 2000～2999 です。

name *acl-name*: ACL の名前を指定します。*acl-name* 引数は大文字と小文字を区別しない 1～63 文字で指定します。英文字ではじめます。混乱を防ぐため、all には設定できません。指定された ACL は、ACL が存在しベーシック ACL のときのみ適用されます。

説明

ip https acl コマンドは HTTPS サービスに ACL を割り当てます。

undo ip https acl コマンドは ACL の割り当てを削除します。

Web ログインリクエストには、ユーザ名とパスワードが含まれます。セキュリティの観点から、装置は Web ログインリクエストの転送には常に HTTPS を使用します。

HTTPS サービスに適用された ACL は HTTPS と HTTP ログインの両方を制御します。装置にアクセスするため、HTTP クライアントは以下の ACL によって許可する必要があります。

- HTTP サービスに適用する ACL
- HTTPS サービスに適用する ACL

ip https acl コマンドを複数実行した場合、最後に行った設定が適用されます。

例

10.10.0.0/16 のユーザのみが HTTP あるいは HTTPS を通して装置にアクセスできるように ACL2001 を割り当てます。

<AC> system-view

[AC] acl basic 2001

[AC-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255

[AC-acl-ipv4-basic-2001] quit

[AC] ip https acl 2001

関連コマンド

acl（コマンドマニュアルのセクション 8 *ACL and QoS* ）

3.1.22 ip https enable

Syntax

ip https enable

undo ip https enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ip https enable コマンドは HTTPS サービスを有効にします。

undo ip https enable コマンドは HTTPS サービスを無効にします。

ユーザが HTTPS を通して装置にアクセスする場合、HTTPS サービスを有効にする必要があります。

HTTPS サービスを有効にすると、SSH ハンドシェークのネゴシエーションプロセスが開始します。

- 装置がローカル証明書を持っている場合、SSH ハンドシェークのネゴシエーションは成功し、HTTPS サービスを開始します。
- 装置がローカル証明書を持っていない場合、証明書アプリケーションプロセスが開始します。証明書アプリケーションプロセスは長い時間がかかるため、SSH ハンドシェークは失敗し、HTTPS サービスが開始されない可能性があります。この問題を解決するため、HTTPS サービスが有効になるまで **ip https enable** コマンドを再度実行します。

例

HTTPS サービスを有効にします。

<AC> system-view

[AC] ip https enable

3.1.23 ip https port

Syntax

ip https port *port-number*

undo ip https port

デフォルト

443

View

System view

定義済みユーザロール

network-admin

パラメータ

port-number: HTTPS サービスのポート番号を指定します。設定範囲は 1～65535 です。

説明

ip https port コマンドは HTTPS サービスのポート番号を指定します。

undo ip https port コマンドはデフォルトに戻します。

HTTPS サービスが有効であるとき、HTTPS サービスのポート番号を変更した場合、HTTPS サービスを再度有効にし、すべての HTTPS 接続を切断します。再度ログインする場合、ユーザは Web ブラウザのアドレスバーで新しい URL を入力する必要があります。

例

HTTPS サービスのポート番号を 8080 に指定します。

<AC> system-view

[AC] ip https port 8080

3.1.24 line

Syntax

line { *first-number1* [*last-number1*] | { **console** | **vty** } *first-number2* [*last-number2*] }

View

System view

定義済みユーザロール

network-admin

パラメータ

first-number1: 最初の user line の通し番号を指定します。

last-number1: 最後の user line の通し番号を指定します（0～32）。*first-number1* よりも小さくすることはできません。

console *first-number2*: first console line の相対番号を指定します。

vty *first-number2*: first VTY line の相対番号を指定します（0～31）。

vty *last-number2*: last VTY user line の相対番号を指定します（0～31）。*first-number2* よりも小さくすることはできません。

説明

line コマンドは 1 つ以上の user line view に移行します。

シングル user line に設定を行うために、このコマンドを使用して user line view に移行します。

同じ設定を複数の user line に行うために、このコマンドを使用して複数の user line view に移行します。

例

user line Console 0 の view に移行します。

<AC> system-view

[AC] line console 0

[AC-line-console0]

user lines VTY 0～VTY 4 の view に移行します。

<AC> system-view

[AC] line vty 0 4

[AC-line-vty0-4]

関連コマンド

line class

3.1.25 line class

Syntax

line class { **console** | **vty** }

View

System view

定義済みユーザロール

network-admin

パラメータ

console: console line class view を指定します。

vty: VTY line class view を指定します。

説明

line class コマンドは user line class view に移行します。

line class のすべての user line で設定を同一にするために、user line class view に移行します。

user line class view では以下のコマンドを実行することができます。

- **auto-execute command**
- **authentication-mode**
- **history-command max-size**
- **idle-timeout**
- **protocol inbound**
- **screen-length**
- **set authentication password**
- **shell**
- **terminal type**
- **user-role**

いくつかのログインコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定は user line で適用されます。user line class view の設定は class のすべての user line で適用されます。
- user line view と user line class view のどちらかの view でデフォルトでない設定がある場合、デフォルトでない設定は、もう一方のデフォルト設定よりも優先されます。user line view のデフォルトでない設定は user line class view のデフォルトでない設定よりも優先されます。
- user line view の設定はすぐに適用され、オンラインユーザに影響します。user line class view の設定は設定が完了したのちにログインしたユーザのみ適用されます。user line class view の設定はオンラインユーザに影響しません。

例

VTY line class view でユーザ接続タイムアウト時間を 15 分に設定します。

<AC> system-view

[AC] line class vty

[AC-line-class-vty] idle-timeout 15

関連コマンド

line

3.1.26 lock

Syntax

lock

デフォルト

設定なし

View

User view

定義済みユーザロール

network-admin

説明

lock コマンドは現在の user line をロックします。

許可されていないユーザが user line で操作を使用しないように防止します。

lock コマンドを実行した後、ロックされていない user line のパスワードを入力し、再度パスワードを入力します。

user line を解除する場合、Enter キーを押下し、正しいパスワードを入力します。

例

現在の user line をロックします。その後ロックを解除します。

<AC> lock

```
Please input password<1 to 16> to lock current line:
Password:
Again:

                locked !
// The user line is locked. To unlock it, press Enter and enter the password:
```

```
Password:
<AC>
```

3.1.27 parity

Syntax

parity { **even** | **mark** | **none** | **odd** | **space** }

undo parity

デフォルト

none

View

User line view

定義済みユーザロール

network-admin

パラメータ

even: 偶数パリティチェックを実行します。

mark: 記号パリティチェックを実行します。

none: パリティチェックを実行しません。

odd: 奇数パリティチェックを実行します。

space: 空白のパリティチェックを実行します。

説明

parity コマンドはパリティチェックモードを指定します。

undo parity コマンドはデフォルトに戻します。

このコマンドは VTY line view でサポートしていません。

この設定は端末のパリティチェックと同一にしてください。

例

user line Console 0 で偶数パリティチェックを実行するように設定します。

<AC> system-view

[AC] line console 0

[AC-line-console0] parity odd

3.1.28 protocol inbound

Syntax

protocol inbound { **all** | **ssh** | **telnet** }

undo protocol inbound

デフォルト

all

View

VTY line view

VTY line class view

定義済みユーザロール

network-admin

パラメータ

all: SSH、Telnet のプロトコルをサポートします。

ssh: SSH のプロトコルをサポートします。

telnet: Telnet のプロトコルをサポートします。

説明

protocol inbound コマンドはサポートするプロトコルを設定します。

undo protocol inbound コマンドはデフォルトに戻します。

network-admin あるいはレベル 15 のユーザロールが割り当てられたユーザのみコマンドを実行することができます。実行権限があったとしてもほかのユーザはコマンドを実行できません。

user line view で設定を変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

SSH をサポートするため user line を設定する前に、user line の認証モードを scheme に設定してください。詳細な情報は **authentication-mode** コマンドを参照してください。

VTY line view で、**protocol inbound** コマンドは **authentication-mode** コマンドと関連します。VTY line view で 2 つのコマンドのうち、1 つコマンドのみデフォルトでない認証モードである場合、もう一方のコマンドは VTY line class view の設定に関わらず、デフォルトの認証モードを使用します。

例

user line VTY 0～4 で SSH のみを有効にするように設定します。

<AC> system-view

[AC] line vty 0 4

[AC-line-vty0-4] authentication-mode scheme

[AC-line-vty0-4] protocol inbound ssh

SSH を有効にし、VTY line class view で認証モードを scheme に設定します。user line VTY 0～VTY 4 ですべてのプロトコルを有効にし、user line で認証を無効にします。

<AC> system-view

[AC] line class vty

[AC-line-class-vty] authentication-mode scheme

[AC-line-class-vty] protocol inbound ssh

[AC-line-class-vty] line vty 0 4

[AC-line-vty0-4] authentication-mode none

設定を確認します。

1)　装置に Telnet します。

<Client> telnet 192.168.1.241

```
Trying 192.168.1.241 ...
Press CTRL+K to abort
Connected to 192.168.1.241 ...

<Server>
```

認証なしでログインしました。

2)　オンライン CLI ユーザの情報を表示します。

<Server> display users

```
  Idx  Line     Idle      Time            Pid     Type
+ 50   VTY 0    00:00:00   Jan 17 15:29:27   189     TEL

Following are more details.
VTY 0   :
       Location: 192.168.1.186
 +    : Current operation user.
 F    : Current operation user works in async mode.
```

出力は、ユーザは VTY 0 を使用していることを示します。user line view の設定は適用されています。

3.1.29 screen-length

Syntax

screen-length *screen-length*

undo screen-length

デフォルト

24 行

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

screen-length: 画面上で一度に表示される行の最大数を指定します。設定範囲は 0～512 です。0 に設定した場合、出力画面のスクロールは停止しません。

説明

screen-length コマンドは画面上で一度に表示される行の最大数を設定します。

undo screen-length コマンドはデフォルトに戻します。

出力画面に表示される実際の行数は端末のモニタの仕様によって制限されます。

たとえば、画面上で一度に表示される行の最大数を 40 に設定した場合、装置はすぐに端末に 40 行を送信します。もし端末のモニタの仕様が 24 である場合、出力画面には最後の 24 行のみが表示されます。前の 16 行を表示する場合、PgUp キーを押下します。

停止したのち、出力を継続する場合、スペースキーを押下します。出力画面のスクロールの停止機能はデフォルトで有効です。

設定を変更した場合、すぐに現在のセッションに適用します。user line class view での設定は、設定が行われた後、ログインセッションで適用されます。

例

user line Console 0 で一度に表示される行の最大数を 30 行に設定します。

<AC> system-view

[AC] line console 0

[AC-line- console 0] screen-length 30

関連コマンド

screen-length disable

3.1.30 send

Syntax

send { **all** | *number1* | { **console** | **vty** } *number2* }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべての user line を指定します。

number1: user line の通し番号を指定します（0～32）。

console *number2*: console line の相対番号を指定します。

vty *number2*: VTY line の相対番号を指定します（0～31）。

説明

send コマンドはオンラインログインユーザにメッセージを送信します。

メッセージを終了する場合、Enter キーを押下します。メッセージをキャンセルし、user view に戻る場合、Ctrl+C キーを押下します。

ほかのオンラインユーザに影響を及ぼす操作を実行する前に、オンラインユーザに通知するために使用することができます。たとえば装置を再起動する場合などに使用します。

例

VTY 1 の user に通知するため、メッセージを送信します。

<AC> send vty 1

```
Input message, end with Enter; abort with CTRL+C:
Your attention, please. I will reboot the system in 3 minutes.
Send message? [Y/N]:y
```

メッセージは以下の例のようにユーザの設定端末の画面に表示されます。

```
[AC]


***
***
***Message from vty0 to vty1
***
Your attention, please. I will reboot the system in 3 minutes.
```

3.1.31 set authentication password

Syntax

set authentication password { **hash** | **simple** } *password*

undo set authentication password

デフォルト

設定なし

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

hash: 暗号テキストのパスワードを設定します。

simple: プレーンテキストのパスワードを設定します。

password: 大文字、小文字が区別されたパスワードを指定します。**simple** が指定された場合、設定範囲は 1～16 文字です。**hash** が指定された場合、設定範囲は 1～110 文字です。

説明

set authentication password コマンドはパスワード認証のパスワードを設定します。

undo set authentication password コマンドはパスワードを削除します。

network-admin あるいはレベル 15 のユーザロールが割り当てられたユーザのみコマンドを実行することができます。実行権限があったとしてもほかのユーザはコマンドを実行できません。

セキュリティのため、保存されたパスワードは設定に関わらず常に暗号テキストで表示されます。

network-admin あるいはレベル 15 のユーザロールが割り当てられたユーザのみコマンドを実行することができます。実行権限があったとしてもほかのユーザはコマンドを実行できません。

このコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定がデフォルトでないとき、user line view の設定が適用されます。
- user line view の設定がデフォルトで user line class view の設定がデフォルトでないとき、user line class view の設定が適用されます。

パスワードを変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

例

user line Console 0 でパスワード認証のパスワード hello を設定します。

<AC> system-view

[AC] line console 0

[AC-line-console0] authentication-mode password

[AC-line-console0] set authentication password simple hello

関連コマンド

authentication-mode

3.1.32 shell

Syntax

shell

undo shell

デフォルト

有効

View

User line view

User line class view

定義済みユーザロール

network-admin

説明

shell コマンドは user line の端末サービスを有効にします。

undo shell コマンドは user line の端末サービスを無効にします。

console line view あるいは console line class view でコマンドは **undo shell** サポートしていません。

現在使用している user line の端末サービスを無効にすることはできません。

装置が Telnet あるいは SSH サーバとして動作するとき、**undo shell** コマンドを設定することはできません。

user line class view で **undo shell** コマンドが設定された場合、class の user line の view で **shell** コマンドを設定することはできません。

端末サービスが有効であるとき、user line は装置へのログインに使用されます。装置がリダイレクトサーバとして稼働している場合、user line はリダイレクトサービスに使用されます。user line は 1 回につき、1 つの処理のみ行うことができます。

例

user line からユーザが装置にログインできないようにするため、VTY line 0～VTY line 4 の端末サービスを無効にします。

<AC> system-view

[AC] line vty 0 4

[AC-line-vty0-4] undo shell

```
Disable ui-vty0-4 , are you sure? [Y/N]:y
[AC-line-vty0-4]
```

3.1.33 speed

Syntax

speed *speed-value*

undo speed

デフォルト

9600 bps

View

User line view

定義済みユーザロール

network-admin

パラメータ

speed-value: 通信速度を bps で指定します。サポートされる通信速度は設定環境によって異なります。非同期シリアルインタフェースの通信速度を以下に示します。

- 300 bps
- 600 bps
- 1200 bps
- 2400 bps
- 4800 bps
- 9600 bps
- 19200 bps
- 38400 bps
- 57600 bps
- 115200 bps

説明

speed コマンドは user line の通信速度（ボーレートと呼ばれます）を設定します。

undo speed コマンドはデフォルトに戻します。

このコマンドは VTY line view でサポートしていません。

端末と装置で設定を同一にしてください。

例

user line Console 0 で通信速度を 19200 bps に設定します。

<AC> system-view

[AC] line console 0

[AC-line-console0] speed 19200

3.1.34 stopbits

Syntax

stopbits { **1** | **1.5** | **2** }

undo stopbits

デフォルト

1

View

User line view

定義済みユーザロール

network-admin

パラメータ

1: ストップビットを 1 に設定します。

1.5: ストップビットを 1.5 に設定します。装置はストップビット 1.5 をサポートしていません。1.5 が設定された場合、ストップビットは 2 が使用されます。

2: ストップビットを 2 に設定します。

説明

stopbits コマンドは文字列のストップビットを設定します。

undo stopbits コマンドはデフォルトに戻します。

このコマンドは VTY line view でサポートしていません。

端末と装置で設定を同一にしてください。

例

user line Console 0 のストップビットを 1 に設定します。

<AC> system-view

[AC] line console 0

[AC-line-console0] stopbits 1

3.1.35 telnet

Syntax

telnet *remote-host* [*service-port*] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] [**dscp** *dscp-value*]

View

User view

定義済みユーザロール

network-admin

パラメータ

remote-host: リモートホストの IPv4 アドレスあるいはホスト名を指定します。ホスト名は大文字、小文字が区別されません。設定範囲は 1～253 文字です。ホスト名の変数は英字、数字、ハイフン(－)、アンダーライン(__)、ドット(.)が含まれます。

service-port: リモートホストの Telnet サービスの TCP ホスト番号を指定します。設定範囲は 0～65535 です。デフォルトは 23 です。

source: Telnet パケットを送信する送信元 IPv4 アドレスあるいは送信元インタフェースを指定します。指定しない場合、ルートの出力インタフェースのプライマリ IPv4 アドレスを使用します。

interface *interface-type interface-number*: 送信元インタフェースを指定します。インタフェースのプライマリ IPv4 アドレスは Telnet パケットを送信する送信元 IPv4 アドレスとして使用されます。

ip *ip-address*: Telnet パケットを送信する送信元 IPv4 アドレスを指定します。

dscp *dscp-value*: パケットの優先度を指定するため、Telnet パケットの DSCP 値を指定します。設定範囲は 0～63 です。デフォルトは 48 です。

説明

telnet コマンドは IPv4 ネットワークのホストに Telnet します。

現在の Telnet 接続を終了するには、Ctrl+K キーを押下するか **quit** コマンドを実行します。

このコマンドで指定された送信元 IPv4 アドレスあるいは送信元インタフェースは現在の Telnet 接続にのみ適用されます。

例

Telnet パケットを送信する送信元 IP アドレス 1.1.1.1 を使用し、ホスト 1.1.1.2 に Telnet します。

<Sysname> telnet 1.1.1.2 source ip 1.1.1.1

関連コマンド

telnet client source

3.1.36 telnet client source

Syntax

telnet client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo telnet client source

デフォルト

Telnet パケットを送信するために指定された送信元 IPv4 アドレスあるいは送信元インタフェースはありません。送信元 IPv4 アドレスは出力インタフェースのプライマリ IPv4 アドレスです。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 送信元インタフェースを指定します。インタフェースのプライマリ IPv4 アドレスは Telnet パケットを送信する送信元 IPv4 アドレスとして使用されます。

ip *ip-address*: 送信元 IPv4 アドレスを指定します。

説明

telnet client source コマンドは、装置が Telnet クライアントとして動作するとき、Telnet パケットを送信する送信元 IPv4 アドレスあるいは送信元インタフェースを指定します。

undo telnet client source コマンドは設定を削除します。

このコマンドで指定された送信元 IPv4 アドレスあるいは送信元インタフェースはすべての Telnet 接続に適用されます。ユーザが **telnet** コマンドを実行して送信元 IPv4 アドレスあるいは送信元インタフェースを指定した場合、ユーザが設定した送信元 IPv4 アドレスあるいは送信元インタフェースが適用されます。

例

装置が Telnet クライアントとして動作するとき、Telnet パケットを送信する送信元 IPv4 アドレスを 1.1.1.1 に設定します。

<AC> system-view

[AC] telnet client source ip 1.1.1.1

関連コマンド

display telnet client configuration

3.1.37 telnet server acl

Syntax

telnet server acl [**mac**] *acl-number*

undo telnet server acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mac: L2 ACL を指定します。標準 ACL、拡張 ACL を指定する場合、**mac** パラメータを指定しないでください。

acl-number: 以下の番号の ACL を指定します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。**mac** パラメータが必要です。

説明

telnet server acl コマンドは Telnet ログインにフィルタリングを行います。

undo telnet server acl コマンドはデフォルトに戻します。

このコマンドは既存の Telnet 接続には適用されません。

ACL が作成されていなくても、このコマンドで ACL を指定することができますが、ACL が作成されたのち、フィルタリングが適用されます。

コマンドを複数実行した場合、最後に行った設定が適用されます。

ACL の詳細はオペレーションマニュアルのセクション 8 *ACL and QoS　"ACL"* を参照してください。

例

IP アドレス 1.1.1.1 のユーザのみ装置に Telnet を行うことができるようにフィルタリングを行います。

<AC> system-view

[AC] acl basic 2001

[AC-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0

[AC-acl-ipv4-basic-2001] quit

[AC] telnet server acl 2001

3.1.38 telnet server dscp

Syntax

telnet server dscp *dscp-value*

undo telnet server dscp

デフォルト

48

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: DSCP 値を指定します。設定範囲は 0～63 です。

説明

telnet server dscp コマンドは Telnet サーバで Telnet パケットを送信する IPv4 の DSCP 値を設定します。

undo telnet server dscp コマンドはデフォルトに戻します。

DSCP 値は IPv4 パケットの ToS フィールドで送信されます。パケットを転送する優先度を示します。

例

Telnet サーバで Telnet パケットを送信する IPv4 の DSCP 値を 30 に設定します。

<AC> system-view

[AC] telnet server dscp 30

3.1.39 telnet server enable

Syntax

telnet server enable

undo telnet server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

telnet server enable コマンドは Telnet サーバ機能を有効にします。

undo telnet server enable コマンドは Telnet サーバ機能を無効にします。

管理者は Telnet サーバ機能が有効であるときのみ装置に Telnet を行うことができます。

例

Telnet サーバ機能を有効にします。

<AC> system-view

[AC] telnet server enable

3.1.40 telnet server port

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.73 を含む以降のソフトウェアからサポートしています。

Syntax

telnet server port port-number

undo telnet server port

デフォルト

IPv4 Telnet サービスのポート番号は、23 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

port-number: ポート番号を指定します。

設定可能範囲は、23 または 1025 ～ 65535 です。

説明

telnet server port を使用して、IPv4 Telnet サービスのポート番号を指定します。

undo telnet server port を使用して、デフォルトを戻します。

このコマンドは、IPv4 Telnet サーバへの既存のすべての Telnet 接続を終了します。

Telnet サービスを使用するには、ユーザは Telnet 接続を再確立する必要があります。

例

IPv4 Telnet サービスのポート番号を 1025 に設定します。

<AC> system-view

[AC] telnet server port 1025

3.1.41 terminal type

Syntax

terminal type { **ansi** | **vt100** }

undo terminal type

デフォルト

ANSI

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

ansi: 端末の表示タイプを ANSI に指定します。

vt100: 端末の表示タイプを VT100 に指定します。

説明

terminal type コマンドは端末の表示タイプを指定します。

undo terminal type コマンドはデフォルトに戻します。

装置は端末の表示タイプ ANSI と VT100 をサポートします。NEC は装置と端末の両方で表示タイプを VT100 に設定することを推奨します。

装置あるいは端末のどちらかが ANSI を使用している場合、コマンドラインが 80 文字を越えたときにカーソル位置のエラーなどの表示に関する問題が発生する可能性があります。

このコマンドは user line view および user line class view の両方でサポートしています。user line view と user line class view のどちらかの view でデフォルトでない設定がある場合、デフォルトでない設定は、もう一方のデフォルト設定よりも優先されます。user line view のデフォルトでない設定は user line class view のデフォルトでない設定よりも優先されます。

端末の表示タイプを変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

例

端末の表示タイプを VT100 に設定します。

<AC> system-view

[AC] line vty 0

[AC-line-vty0] terminal type vt100

3.1.42 user-interface

Syntax

user-interface { *first-number1* [*last-number1*] | { **console** | **vty** } *first-number2* [*last-number2*] }

View

System view

定義済みユーザロール

network-admin

パラメータ

first-number1: 最初の user line の通し番号を指定します。

last-number1: 最後の user line の通し番号を指定します。*first-number1* よりも小さくすることはできません。

console *first-number2*: console line の相対番号を指定します。

console *last-number2*: console line の相対番号を指定します。*first-number2* よりも小さくすることはできません。

vty *first-number2*: first VTY line の相対番号を指定します（0～31）。

vty *last-number2*: last VTY line の相対番号を指定します（0～31）。

説明

user-interface コマンドは 1 つ以上の user line view に移行します。

1 つの user line を設定する場合、**user-interface** コマンドを使用して user line view に移行します。

複数の user line で同一の設定を行う場合、**user-interface** コマンドを使用して複数の user line view に移行します。

このコマンドは古いソフトウェアバージョンで使用していたユーザのためにサポートされているコマンドです。古いソフトウェアバージョンで動作するコマンドです。**line** コマンドと同一機能です。通常は **line** コマンドを使用してください。

例

user line Console 0 の view に移行します。

<AC> system-view

[AC] user-interface console 0

[AC-line-console0]

VTY 0～VTY 4 の view に移行します。

<AC> system-view

[AC] user-interface vty 0 4

[AC-line-vty0-4]

関連コマンド

user-interface class

3.1.43 user-interface class

Syntax

user-interface class { **console** | **vty** }

View

System view

定義済みユーザロール

network-admin

パラメータ

console: console line class view を指定します。

vty: VTY line class view を指定します。

説明

user-interface class コマンドは user line class view に移行します。

このコマンドは古いソフトウェアバージョンで使用していたユーザのためにサポートされているコマンドです。古いソフトウェアバージョンで動作するコマンドです。**line class** コマンドと同一機能です。通常は **line class** コマンドを使用してください。

line class のすべての user line で設定を同一にするために、user line class view に移行します。

user line class view では以下のコマンドを実行することができます。

- **auto-execute command**
- **authentication-mode**
- **history-command max-size**
- **idle-timeout**
- **protocol inbound**
- **screen-length**
- **set authentication password**

- **shell**
- **terminal type**
- **user-role**

いくつかのログインコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定は user line で適用されます。user line class view の設定は class のすべての user line で適用されます。
- user line view と user line class view のどちらかの view でデフォルトでない設定がある場合、デフォルトでない設定は、もう一方のデフォルト設定よりも優先されます。user line view のデフォルトでない設定は user line class view のデフォルトでない設定よりも優先されます。
- user line view の設定はすぐに適用され、オンラインユーザに影響します。user line class view の設定は設定が完了したのちにログインしたユーザのみ適用されます。user line class view の設定はオンラインユーザに影響しません。

例

VTY line class view でユーザ接続タイムアウト時間を 15 分に設定します。

<AC> system-view

[AC] user-interface class vty

[AC-line-class-vty] idle-timeout 15

関連コマンド

user-interface

3.1.44 user-role

Syntax

user-role *role-name*

undo user-role [*role-name*]

デフォルト

コンソールユーザのユーザロールは network-admin です。

ほかの user line のユーザロールは network-operator です。

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

role-name: ユーザロール名を指定します。大文字、小文字を区別します。範囲は 1～63 です。ユーザロールはユーザ定義あるいは定義済みのユーザロールがあります。定義済みは network-admin、network-operator、level-0～level-15 があります。**undo user-role** コマンドで *role-name* を指定しない場合、デフォルトのユーザロールに戻します。

説明

user-role コマンドは user line でログインしたユーザがユーザロールを取得できるように user line にユーザロールを割り当てます。

undo user-role コマンドはユーザロールを削除あるいはデフォルトに戻します。

network-admin あるいはレベル 15 のユーザロールが割り当てられたユーザのみコマンドを実行することができます。実行権限があったとしてもほかのユーザはコマンドを実行できません。

このコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定がデフォルトでないとき、user line view の設定が適用されます。
- user line view の設定がデフォルトで user line class view の設定がデフォルトでないとき、user line class view の設定が適用されます。

設定を変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

user line に 64 のユーザロールを割り当てることができます。user line からログインしたユーザはすべてのユーザロールを取得します。

例

user line Console 0 にユーザロール network-admin を割り当てます。

<AC> system-view

[AC] line console 0

[AC-line-console0] user-role network-admin

3.1.45 web idle-timeout

Syntax

web idle-timeout *idle-time*

undo web idle-timeout

デフォルト

10 分

View

System view

定義済みユーザロール

network-admin

パラメータ

idle-time: タイムアウトタイマを指定します。設定範囲は 1～999 分です。

説明

web idle-timeout コマンドは Web ユーザの接続のタイムアウトタイマを設定します。

undo web idle-timeout コマンドはデフォルトに戻します。

許可されていないアクセスを防ぐため、アイドルタイムアウト時間内にマウスあるいはキーボードの動作がない場合、システムは自動でユーザの接続を切断します。

このコマンドは現在の Web 接続に即座に適用されます。

例

Web ユーザの接続のタイムアウトタイマを 100 分に設定します。

<AC> system-view

[AC] web idle-timeout 100

目次

このセクションのページは **1-x-x** です。

4 章 FTP 4-1
4.1 FTP サーバ設定コマンド 4-1
4.1.1 display ftp-server 4-1
4.1.2 display ftp-user 4-2
4.1.3 free ftp user 4-3
4.1.4 free ftp user-ip 4-3
4.1.5 ftp server acl 4-4
4.1.6 ftp server dscp 4-5
4.1.7 ftp server enable 4-6
4.1.8 ftp timeout 4-6
4.2 FTP クライアント設定コマンド 4-7
4.2.1 ascii 4-7
4.2.2 binary 4-8
4.2.3 bye 4-9
4.2.4 cd 4-10
4.2.5 cdup 4-11
4.2.6 close 4-12
4.2.7 debug 4-12
4.2.8 delete 4-13
4.2.9 dir 4-14
4.2.10 disconnect 4-15
4.2.11 display ftp client source 4-16
4.2.12 ftp 4-17
4.2.13 ftp client source 4-18
4.2.14 get 4-19
4.2.15 help 4-20
4.2.16 lcd 4-21
4.2.17 ls 4-22
4.2.18 mkdir 4-23
4.2.19 newer 4-24
4.2.20 open 4-25
4.2.21 passive 4-26
4.2.22 put 4-27
4.2.23 pwd 4-28
4.2.24 quit 4-28
4.2.25 rhelp 4-29

4.2.26 rmdir 4-31
4.2.27 user 4-32
4.2.28 verbose 4-33
4.2.29 ? 4-34

4章 FTP

4.1 FTPサーバ設定コマンド

4.1.1 display ftp-server

Syntax

display ftp-server

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ftp-server コマンドは FTP サーバの設定と情報を表示します。

例

FTP サーバの設定と情報を表示します。

<AC> display ftp-server

```
FTP server is running.
User count:                     1
Idle-timeout timer (in minutes):  30
```

表 4-1 コマンド出力

フィールド	説明
User count	現在ログインしているユーザ数です。
Idle-timeout timer (in minutes)	FTPサーバとクライアント間で一定期間、パケットの交換がない場合、FTP接続が切断されます。

関連コマンド

- **ftp server enable**
- **ftp timeout**

4.1.2 display ftp-user

Syntax

display ftp-user

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ftp-user コマンドは FTP ログインユーザに関する詳細情報を表示します。

例

FTP ログインユーザに関する詳細情報を表示します。

<AC> display ftp-user

```
UserName     HostIP           Port     HomeDir
root        192.168.20.184     46539    cfa0:
```

文字数が超過している場合、フィールドの値は次の行に表示されます。改行される場合のフィールドの値の制限を示します。

- **UserName**—10 文字
- **HostIP**—15 文字
- **HomeDir**—37 文字

<AC> display ftp-user

```
UserName     HostIP           Port     HomeDir
user2        2000:2000:2000:    1499     cfa0:/user2
           2000:2000:2000:
           2000:2000
administra   100.100.100.100    10001    cfa0:/123456789/123456789/123456789/
tor                                  123456789/123456789/123456789/1234567
                                    89/123456789
```

表 4-2 コマンド出力

フィールド	説明
UserName	ユーザ名です。
HostIP	ユーザのIPアドレスです。

フィールド	説明
Port	ユーザのポート番号です。
HomeDir	ユーザの許可ディレクトリです。

4.1.3 free ftp user

Syntax

free ftp user *username*

View

User view

定義済みユーザロール

network-admin

パラメータ

username: ユーザ名を指定します。FTP ユーザの情報を表示する場合、**display ftp-user** コマンドを使用します。

説明

free ftp user コマンドは指定したアカウントにより確立された FTP 接続を手動で切断します。

例

ユーザ ftpuser により確立された FTP 接続を手動で切断します。

<AC> free ftp user ftpuser

```
Are you sure to free FTP connection? [Y/N]:y
<AC>
```

4.1.4 free ftp user-ip

Syntax

free ftp user-ip *ipv4-address* [**port** *port*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: FTP 接続の送信元 IP アドレスです。FTP 接続の送信元 IP アドレスを表示する場合、**display ftp-user** コマンドを使用します。

port *port*: FTP 接続の送信元ポート番号を指定します。FTP 接続の送信元ポート番号を表示する場合、**display ftp-user** コマンドを使用します。

説明

free ftp user-ip コマンドは指定した IPv4 アドレスにより確立された FTP 接続を手動で切断します。

例

IPv4 アドレス 192.168.20.184 により確立された FTP 接続を手動で切断します。

<AC> free ftp user-ip 192.168.20.184

```
Are you sure to free FTP connection? [Y/N]:y
<AC>
```

4.1.5 ftp server acl

Syntax

ftp server acl *acl-number*

undo ftp server acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

acl-number: IPv4 ACL 番号を指定します。設定範囲は 2000～3999 です。

説明

ftp server acl コマンドは FTP サーバへの FTP クライアントのアクセスを制御します。

undo ftp server acl コマンドはデフォルトに戻します。

ACL により、FTP サーバは特定の FTP クライアントからの FTP リクエストのみを許可することができます。

この設定は FTP 接続が確立されたときのみ適用されます。既存の FTP 接続は影響がありません。

複数回コマンドを実行した場合、最後に指定した設定が適用されます。

例

FTP サーバへのアクセスが FTP クライアント 1.1.1.1 のみであるように ACL 2001 を指定します。

<AC> system-view

[AC] acl basic 2001

[AC-acl-ipv4-basic-2001] rule 0 permit source 1.1.1.1 0

[AC-acl-ipv4-basic-2001] rule 1 deny source any

[AC-acl-ipv4-basic-2001] quit

[AC] ftp server acl 2001

4.1.6 ftp server dscp

Syntax

ftp server dscp *dscp-value*

undo ftp server dscp

デフォルト

0

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: DSCP 値を指定します。設定範囲は 0～63 です。

説明

ftp server dscp コマンドは FTP クライアントに送信する IPv4 パケットの DSCP 値を指定します。

undo ftp server dscp コマンドはデフォルトに戻します。

DSCP 値は、IP パケットの ToS フィールドによって送信されます。パケットを転送する優先度を示します。

例

FTP サーバの送信 IPv4 パケットの DSCP 値を 30 に設定します。

<AC> system-view

[AC] ftp server dscp 30

4.1.7 ftp server enable

Syntax

ftp server enable

undo ftp server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ftp server enable コマンドは FTP サーバを有効にします。

undo ftp server enable コマンドは FTP サーバを無効にします。

例

FTP サーバを有効にします。

<AC> system-view

[AC] ftp server enable

4.1.8 ftp timeout

Syntax

ftp timeout *minute*

undo ftp timeout

デフォルト

30 分

View

System view

定義済みユーザロール

network-admin

パラメータ

minute: アイドルタイムアウトの時間です。設定範囲は 1～35791 分です。

説明

ftp timeout コマンドは FTP 接続のアイドルタイムアウトを設定します。

undo ftp timeout コマンドはデフォルトに戻します。

FTP 接続のアイドルタイムアウト内にパケットの送信が行われていない場合、FTP サーバはリソースを確保するために接続を切断します。

例

アイドルタイムアウトを 36 分に設定します。

<AC> system-view

[AC] ftp timeout 36

4.2 FTPクライアント設定コマンド

FTP クライアント設定コマンドを実行する前、FTP サーバでのユーザの許可設定が適用されていることを確認してください。許可設定は、作業ディレクトリ下のファイルの参照、ファイルの読み込み、ダウンロード、アップロード、ファイルのリネーム、ファイルの削除、ディレクトリの作成があります。

この章の FTP クライアントのコマンドは、装置によってサポートされていますが、正常に動作するかどうかは FTP サーバに依存します。

このセクションの例の出力例は FTP サーバの種類によって異なる場合があります。

4.2.1 ascii

Syntax

ascii

デフォルト

バイナリモード

View

FTP client view

定義済みユーザロール

network-admin

説明

ascii コマンドはファイルの転送モードを ASCII モードに設定します。

- **バイナリモード**－非テキストファイル（プログラムファイルや絵）を転送します。
- **ASCII モード**－テキストファイルを転送します。

FTP サーバにログイン後のみコマンドを設定することができます。

装置が FTP サーバとして動作するとき、転送モードは FTP クライアントによって決定します。装置が FTP クライアントとして動作するとき、転送モードを設定することができます。

例

転送モードを ASCII モードに設定します。

ftp> ascii

```
200 TYPE is now ASCII
```

関連コマンド

binary

4.2.2 binary

Syntax

binary

デフォルト

バイナリモード

View

FTP client view

定義済みユーザロール

network-admin

説明

binary コマンドはファイルの転送モードをバイナリモードに設定します。このモードはフローモードと呼ばれます。

ascii コマンドはファイルの転送モードを ASCII モードに設定します。

- **バイナリモード**ー非テキストファイル（プログラムファイルや画像ファイル）を転送します。
- **ASCII モード**ーテキストファイルを転送します。

FTP サーバにログイン後のみコマンドを設定することができます。

装置が FTP サーバとして動作するとき、転送モードは FTP クライアントによって決定します。装置が FTP クライアントとして動作するとき、転送モードを設定することができます。

例

転送モードをバイナリモードに設定します。

ftp> binary

```
200 TYPE is now 8-bit binary
```

関連コマンド

asci

4.2.3 bye

Syntax

bye

View

FTP client view

定義済みユーザロール

network-admin

説明

bye コマンドは FTP サーバの接続を終了し、user view に戻ります。

装置とリモート FTP サーバ間で接続が確立していない場合、user view に戻ります。

例

FTP サーバの接続を終了し、user view に戻ります。

ftp> bye

```
221-Goodbye. You uploaded 2 and downloaded 2 kbytes.
```

```
221 Logout.
<AC>
```

関連コマンド

quit

4.2.4 cd

Syntax

cd { *directory* | **..** | */* }

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

directory: [*drive*:][*/*]*path* の形式のターゲットディレクトリ名を指定します。ここでは記憶媒体の名前を示します。通常はフラッシュあるいは CF です。ターゲットディレクトリが存在しない場合、**cd** コマンドは現在の作業ディレクトリを変更しません。ドライブ情報がない場合、現在のディレクトリのフォルダあるいはサブフォルダを示します。*drive* と *path* の引数についての詳細はオペレーションマニュアルのセクション 1 *はじめに* *“FTP”* を参照してください。

..: 上位のディレクトリに戻ります。**cd ..**コマンドは **cdup** コマンドを実行するのと同一です。現在の作業ディレクトリが FTP ルートディレクトリである場合、**cd ..**はルートディレクトリに戻ります。

/: FTP ルートディレクトリに戻ります。

説明

cd コマンドは FTP サーバの現在の作業ディレクトリを別のディレクトリに変更します。

FTP サーバにログインした後のみ実行できます。

アクセスできるディレクトリは FTP サーバによって許可されている必要があります。

例

作業ディレクトリを現在のディレクトリのサブディレクトリ logfile に変更します。

```
ftp> cd logfile
250 OK. Current directory is /logfile
```

作業ディレクトリを FTP ルートディレクトリのサブディレクトリフォルダに変更します。

ftp> cd /folder

```
250 OK. Current directory is /folder
```

作業ディレクトリを現在のディレクトリの上位ディレクトリに変更します。

ftp> cd ..

```
250 OK. Current directory is /
```

作業ディレクトリを FTP ルートディレクトリに変更します。

ftp> cd /

```
250 OK. Current directory is /
```

関連コマンド

- **cdup**
- **pwd**

4.2.5 cdup

Syntax

cdup

View

FTP client view

定義済みユーザロール

network-admin

説明

cdup コマンドは FTP サーバの上位ディレクトリに移行します。

FTP サーバにログインした後のみ実行できます。

現在のディレクトリが FTP ルートディレクトリである場合、このコマンドは作業ディレクトリを変更しません。

例

作業ディレクトリを上位ディレクトリに移行します。

ftp> pwd

```
257 "/ftp/subdir" is your current location
```

ftp> cdup

```
250 OK. Current directory is /ftp
```

ftp> pwd

```
257 "/ftp" is your current location
```

関連コマンド

- **cd**
- **pwd**

4.2.6 close

Syntax

close

View

FTP client view

定義済みユーザロール

network-admin

説明

close コマンドは FTP client view から移動することなく、FTP サーバの接続を終了します。

FTP サーバにログインした後のみ実行できます。

例

FTP client view から移動することなく、FTP サーバの接続を終了します。

ftp> close

```
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
ftp>
```

関連コマンド

disconnect

4.2.7 debug

Syntax

debug

デフォルト

無効

View

FTP client view

定義済みユーザロール

network-admin

説明

debug コマンドは FTP クライアントのデバッグを無効あるいは有効に設定します。

FTP クライアントのデバッグが有効であるとき、このコマンドを使用して FTP クライアントのデバッグを無効にします。

FTP クライアントのデバッグが無効であるとき、このコマンドを使用して FTP クライアントのデバッグを有効にします。

例

FTP クライアントのデバッグを有効にし、その後、無効にします。

ftp> debug

```
Debugging on (debug=1).
```

ftp> debug

```
Debugging off (debug=0).
```

4.2.8 delete

Syntax

delete *remotefile*

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile: FTP サーバのファイル名を指定します。

説明

delete コマンドは FTP サーバのファイルを完全に削除します。

FTP サーバにログインした後のみ実行できます。

この動作を実行するため、FTP サーバの削除権限が必要です。

例

ファイル b.txt を削除します。

ftp> delete b.txt

```
250 Deleted b.txt
```

4.2.9 dir

Syntax

dir [*remotefile* [*localfile*]]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile: FTP サーバのファイルあるいはディレクトリを指定します。

localfile: 表示された情報が保存されるローカルファイルの名前を指定します。

説明

dir コマンドは FTP サーバ上の、現在のディレクトリにあるファイルおよびサブディレクトリに関する詳細情報を表示します。

dir *remotefile* コマンドは FTP サーバのファイルあるいはディレクトリに関する詳細情報を表示します。

dir *remotefile localfile* コマンドはリモート FTP サーバ上の指定したファイルまたはディレクトリに関する詳細情報を表示し、表示された情報を引数 *localfile* で指定したローカルファイルに保存します。

FTP サーバにログインした後のみ実行できます。

FTP client view において、**dir** コマンドは **ls** コマンドと同一です。

例

FTP サーバの現在のディレクトリのファイル、サブディレクトリの詳細情報を表示します。

ftp> dir

```
Directory of cfa0:
   0 drw-         - Nov 22 2017 14:44:17   apimage
   1 -rw-     260607 Nov 22 2017 14:44:14   defaultfile.zip
   2 -rw-     47217 Nov 15 2017 20:12:30   diag_QX-W2230AC_20171115-201144.tar
```

```
.gz
   3 drw-          - Nov 15 2017 19:15:19   diagfile
   4 -rw-        198 Nov 22 2017 14:43:25   ifindex.dat
   5 -rw-          0 Nov 15 2017 20:07:12   lauth.dat
   6 drw-          - Nov 15 2017 19:40:06   logfile
   7 drw-          - Nov 15 2017 19:15:44   pki
   8 -rw-   24859648 Dec 15 2011 09:00:00   qx-w2230ac-boot-v710.bin
   9 -rw-   62296064 Dec 15 2011 09:00:00   qx-w2230ac-system-v710.bin
  10 drw-          - Nov 15 2017 19:15:19   seclog
  11 -rw-       2208 Nov 22 2017 14:43:26   startup.cfg
  12 -rw-      42916 Nov 22 2017 14:43:26   startup.mdb

1048576 KB total (943984 KB free)
```

ファイルの詳細情報を a.txt から s.txt に保存します。

ftp> dir a.txt s.txt

output to local-file: s.txt ? [Y/N]y

```
150 Connecting to port 50203
226-Glob: a.txt
```

s.txt の内容を表示します。

ftp> bye

```
221-Goodbye. You uploaded 0 and downloaded 2 kbytes.
221 Logout
```

<AC> more s.txt

```
-rwxr-xr-x    1 0        0             1481 Jul  7 12:34 a.txt
```

関連コマンド

ls

4.2.10 disconnect

Syntax

disconnect

View

FTP client view

定義済みユーザロール

network-admin

説明

disconnect コマンドは FTP client view から移動することなく、FTP サーバへの接続を終了します。

FTP サーバにログインした後のみ実行できます。

例

FTP client view から移動することなく、FTP サーバへの接続を終了します。

ftp> disconnect

```
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
ftp>
```

関連コマンド

close

4.2.11 display ftp client source

Syntax

display ftp client source

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ftp client source コマンドは FTP クライアントの設定の送信元アドレスを表示します。

例

FTP クライアントの設定の送信元アドレスを表示します。

<AC> display ftp client source

```
The source IP address of the FTP client is 1.1.1.1.
The source IPv6 address of the FTP client is 2001::1.
```

4.2.12 ftp

Syntax

ftp [*ftp-server* [*service-port*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }]] *

View

User view

定義済みユーザロール

network-admin

パラメータ

ftp-server: FTP サーバの IPv4 アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1〜253 です。大文字、小文字を区別しません。ホスト名で使用できる文字列は文字、数字、ハイフン（-）、アンダーライン（-）、ドット（.）です。

service-port: FTP サーバの TCP ポート番号を指定します。設定範囲は 0〜65535 です。デフォルトは 21 です。

dscp *dscp-value*: 送信 FTP パケットで使用される IPv4 パケットの DSCP 値です。パケットの優先度を示します。設定範囲は 0〜63 です。デフォルトは 0 です。

source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }: FTP 接続を確立するために使用する送信元アドレスを指定します。

- **interface** *interface-type interface-number*: インタフェースのタイプと番号を指定します。インタフェースのプライマリ IPv4 アドレスは FTP パケットを送信する送信元アドレスとして使用されます。送信元インタフェースにプライマリ IPv4 アドレスが設定されていない場合、接続は確立できません。
- **ip** *source-ip-address*: IPv4 アドレスを指定します。すでに装置で設定されている必要があります。

説明

ftp コマンドは FTP サーバにログインし、FTP client view に移行します。

このコマンドは IPv4 ネットワークでのみ有効です。

パラメータが指定されない場合、FTP サーバにログインしないで FTP client view に移行します。

パラメータが指定されている場合、FTP にログインするためのユーザ名とパスワードを入力する画面が表示されます。

例

FTP サーバ 192.168.0.211 にログインします。

<AC> ftp 192.168.0.211

```
Press CTRL+C to abort.
```

```
Connected to 192.168.0.211 (192.168.0.211).
220 3Com 3CDaemon FTP Server Version 2.0
User (192.168.0.211:(none)): abc
331 User name ok, need password
Password:
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

4.2.13 ftp client source

Syntax

ftp client source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }

undo ftp client source

デフォルト

FTP パケットを送信する送信元 IPv4 アドレスは設定されていません。装置は送信元 IP アドレスとしてルートの送信インタフェースのプライマリ IPv4 アドレスを使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: FTP 接続を確立する送信元インタフェースを指定します。送信元インタフェースのプライマリ IPv4 アドレスは FTP サーバに送信するパケットの送信元 IP アドレスとして使用されます。転送が成功するために、インタフェースが UP し、プライマリ IPv4 アドレスが設定されていることを確認してください。

ip *source-ip-address*: FTP パケットを送信する送信元 IP アドレスを指定します。UP 状態のインタフェースの IPv4 アドレスが設定されていることを確認してください。そうでなければ転送が失敗します。

説明

ftp client source コマンドは FTP パケットを送信する送信元 IPv4 アドレスを指定します。

undo ftp client source コマンドはデフォルトに戻します。

このコマンドを複数実行した場合、最後に実行したコマンドが適用されます。

ftp コマンドで送信元アドレスが指定されている場合、**ftp client source** コマンドで指定された送信元アドレスよりも優先されます。

ftp client source コマンドで指定された送信元アドレスはすべての FTP 接続に適用されます。**ftp** コマンドで指定された送信元アドレスは現在の FTP 接続に適用されます。

例

FTP パケットを送信する送信元 IPv4 アドレスとして 192.168.20.222 を指定します。

<AC> system-view

[AC] ftp client source ip 192.168.20.222

関連コマンド

ftp

4.2.14 get

Syntax

get *remotefile* [*localfile*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile: ダウンロードするファイル名を指定します。

localfile: ダウンロードされたファイルの名前を指定します。指定しない場合、ダウンロードするファイル名を使用します。

説明

get コマンドは FTP サーバからファイルをダウンロードし、ファイルに保存します。

FTP サーバにログインしたのち、このコマンドを行うことができます。

ftp コマンドによって作業ディレクトリにダウンロードされたファイルを保存するため、以下のどちらかの作業を行います。

- *localfile* パラメータを指定しない場合、元のファイル名を使用します。
- *localfile* パラメータを指定する場合、ファイル名にパス情報を入力しないでください。たとえば a.cfg です。

ダウンロードされたファイルをほかのディレクトリに保存する場合、*localfile* パラメータはターゲットディレクトリと cfa0:/subdirectory/a.cfg のようなファイル名を追加する必要があります。

例

ファイル **a.txt** をダウンロードし、**b.txt** として **ftp** コマンドの作業ディレクトリに保存します。

ftp> get a.txt b.txt

```
local: b.txt remote: a.txt
150 Connecting to port 47457
226 File successfully transferred
1569 bytes received in 0.00527 seconds (290.6 kbyte/s)
```

a.txt ファイルをデバイス上のフラッシュメモリのルートディレクトリにダウンロードし、ファイルを **c.txt** として保存します。

ftp> get a.txt cfa0:/c.txt

```
local: cfa0:/c.txt remote: a.txt
150 Connecting to port 47460
226 File successfully transferred
1569 bytes received in 0.0564 seconds (27.2 kbyte/s)
```

関連コマンド

put

4.2.15 help

Syntax

help [*command-name*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

command-name: FTP クライアントでサポートされるコマンドを指定します。

説明

help コマンドは FTP クライアントでサポートされるすべてのコマンドを表示します。

help *command-name* コマンドはコマンドのヘルプ情報を表示します。

FTP client view において **help** コマンドは**?**コマンドと同一です。

例

FTP クライアントでサポートされるすべてのコマンドを表示します。

ftp> help

```
Commands may be abbreviated.  Commands are:

append          delete          ls              quit            rmdir
ascii           debug           mkdir           reget           status
binary          dir             newer           rstatus         system
bye             disconnect      open            rhelp           user
cd              get             passive         rename          verbose
cdup            help            put             reset           ?
close           lcd             pwd             restart
```

dir コマンドのヘルプ情報を表示します。

ftp> help dir

```
dir             list contents of remote directory
```

関連コマンド

?

4.2.16 lcd

Syntax

lcd [*directory* | */*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

directory: FTP クライアントのローカルディレクトリを指定します。/cfa0:/logfile のように記憶媒体の名前の前にスラッシュ（/）が必要です。

/: FTP クライアントのルートディレクトリを指定します。

説明

lcd コマンドは FTP クライアントのローカル作業ディレクトリを表示します。

lcd *directory* コマンドは FTP クライアントのローカル作業ディレクトリを指定したディレクトリに変更します。

lcd /コマンドは FTP クライアントのローカル作業ディレクトリをローカルルートディレクトリに変更します。

例

ローカル作業ディレクトリを表示します。

ftp> lcd

```
Local directory now /cfa0:
```

ローカル作業ディレクトリを cfa0:/logfile に変更します。

ftp> lcd /cfa0:/logfile

```
Local directory now /cfa0:/logfile
```

4.2.17 ls

Syntax

ls [*remotefile* [*localfile*]]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile: FTP サーバのファイルあるいはディレクトリを指定します。

localfile: 表示された情報が保存されるローカルファイルの名前を指定します。

説明

ls コマンドは FTP サーバ上の、現在のディレクトリにあるファイルおよびサブディレクトリに関する詳細情報を表示します。

ls *remotefile* コマンドは FTP サーバのファイルあるいはディレクトリに関する詳細情報を表示します。

ls *remotefile localfile* コマンドはリモート FTP サーバ上の指定したファイルまたはディレクトリに関する詳細情報を表示し、表示された情報を引数 *localfile* で指定したローカルファイルに保存します。

FTP サーバにログインした後のみ実行できます。

FTP client view において、**ls** コマンドは **dir** コマンドと同一です。

例

FTP サーバの現在のディレクトリのファイル、サブディレクトリの詳細情報を表示します。

ftp> ls

```
150 Connecting to port 50201
-rwxr-xr-x   1 0        0             1481 Jul  7 15:36 a.txt
drwxr-xr-x   2 0        0             8192 Jul  2 14:33 diagfile
drwxr-xr-x   3 0        0             8192 Jul  7 15:21 ftp
drwxr-xr-x   2 0        0             8192 Jul  5 09:15 logfile
drwxr-xr-x   2 0        0             8192 Jul  2 14:33 seclog
-rwxr-xr-x   1 0        0         40808448 Jul  2 14:33 simware-cmw710-sys
tem-a1801.bin
-rwxr-xr-x   1 0        0             3050 Jul  7 12:26 startup.cfg
-rwxr-xr-x   1 0        0            54674 Jul  4 09:24 startup.mdb
-rwxr-xr-x   1 0        0             1481 Jul  7 12:34 x.cfg
226 9 matches total
```

ファイル a.txt の詳細情報を s.txt に保存します。

ftp> ls a.txt s.txt

```
output to local-file: s.txt ? [Y/N]y
150 Connecting to port 50203
226-Glob: s.txt
```

ファイル s.txt の内容を表示します。

ftp> bye

```
221-Goodbye. You uploaded 0 and downloaded 2 kbytes.
221 Logout.
```

<AC> more s.txt

```
-rwxr-xr-x   1 0        0             1481 Jul  7 12:34 a.txt
```

関連コマンド

dir

4.2.18 mkdir

Syntax

mkdir *directory*

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

directory: 作成するディレクトリの名前を指定します。

説明

mkdir コマンドは FTP サーバの現在のディレクトリにサブディレクトリを作成します。

FTP サーバにログインした後のみ実行できます。

この動作を実行するため、FTP サーバの権限が必要です。

例

リモート FTP サーバの現在のディレクトリにサブディレクトリ newdir を作成します。

ftp> mkdir newdir

```
257 "newdir" : The directory was successfully created
```

4.2.19 newer

Syntax

newer *remotefile* [*localfile*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile: FTP サーバのリモートファイルの名前を指定します。

localfile: アップデートされたローカルファイルの名前を指定します。

説明

newer コマンドは FTP サーバのリモートファイルをローカルファイルにアップデートします。

FTP サーバにログインした後のみ実行できます。

ローカルファイルが存在しない場合、FTP サーバからファイルをダウンロードし、ローカルに保存します。

FTP サーバのリモートファイルがローカルファイルよりも古い場合、ローカルファイルをアップデートしません。

例

FTP サーバのファイル a.txt をローカルファイルにアップデートします。

ftp> newer a.txt

```
local: a.txt remote: a.txt
150 Connecting to port 63513
226 File successfully transferred
1573 bytes received in 0.0293 seconds (52.3 kbyte/s)
```

4.2.20 open

Syntax

open *server-address* [*service-port*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

server-address: FTP サーバの IP アドレスまたはホスト名を指定します。

service-port: FTP サーバの TCP ポート番号を指定します。設定範囲は 0～65535 です。デフォルトは 21 です。

説明

open コマンドは FTP client view で FTP サーバにログインします。

このコマンドを実行した後、システムはユーザ名とパスワードを入力する画面が表示されます。

ある FTP サーバにログインした後、別のサーバに **open** コマンドを使用してログインする前に、サーバから切断する必要があります。

例

FTP client view で FTP サーバ 192.168.40.7 にログインします。

<AC> ftp

```
ftp> open 192.168.40.7
Press CTRL+C to abort.
Connected to 192.168.40.7 (192.168.40.7).
220 FTP service ready.
User (192.168.40.7:(none)): root
331 Password required for root.
```

```
Password:
230 User logged in.
Remote system type is NEC.
ftp>
```

4.2.21 passive

Syntax

passive

デフォルト

passive

View

FTP client view

定義済みユーザロール

network-admin

説明

passive コマンドは FTP 伝送モードを passive に設定します。

ftp は以下のいずれかのモードを実行することができます。

- **Active モード**—FTP サーバが TCP 接続を開始します。
- **Passive モード**—FTP クライアントが TCP 接続を開始します。

このコマンドはモードの切り替えを行うため、複数回実行することができます。

このコマンドは主にプライベートネットワークユーザとパブリックネットワークユーザ間の FTP セッションの確立を制御する Firewall と一緒に使用されます。

例

FTP 伝送モードを passive に設定します。

ftp> passive

```
Passive mode on.
```

ftp> passive

```
Passive mode off.
```

4.2.22 put

Syntax

put *localfile* [*remotefile*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

localfile: アップロードするファイル名を指定します。

remotefile: FTP サーバでアップロードされたファイルを保存するファイル名を指定します。

説明

put コマンドはリモート FTP クライアントから FTP サーバにファイルをアップロードします。

FTP サーバにログインした後のみ実行できます。

ftp コマンドによって作業ディレクトリにアップロードするため、*localfile* パラメータで a.cfg のようなファイル名を指定する必要があります。

アップロードされたファイルをほかのディレクトリに保存する場合、*localfile* パラメータはターゲットディレクトリと cfa0:/subdirectory/a.cfg のようにファイル名を追加する必要があります。

例

ftp コマンドで作業ディレクトリにファイル **a.txt** をアップロードします。FTP サーバに **b.txt** として保存します。

ftp> put a.txt b.txt

```
local: a.txt remote: b.txt
150 Connecting to port 47461
226 File successfully transferred
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
```

メンバー装置上のフラッシュメモリの **test** ディレクトリからファイル **a.txt** をアップロードします。FTP サーバに **b.txt** として保存します。

ftp> put cfa0:/test/a.txt b.txt

```
local: cfa0:/test/a.txt remote: b.txt
150 Connecting to port 47461
226 File successfully transferred
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
```

関連コマンド

get

4.2.23 pwd

Syntax

pwd

View

FTP client view

定義済みユーザロール

network-admin

説明

pwd コマンドは FTP サーバの現在アクセスしているディレクトリを表示します。

FTP サーバにログインした後のみ実行できます。

例

リモート FTP サーバの現在アクセスしているディレクトリを表示します。

ftp> cd subdir

```
250 OK. Current directory is /subdir
```

ftp> pwd

```
257 "/subdir" is your current location
```

4.2.24 quit

Syntax

quit

View

FTP client view

定義済みユーザロール

network-admin

説明

quit コマンドは FTP サーバの接続を終了し、user view に戻ります。

例

FTP サーバの接続を終了し、user view に戻ります。

ftp> quit

```
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
<AC>
```

関連コマンド

bye

4.2.25 rhelp

Syntax

rhelp [*protocol-command*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

protocol-command: FTP 関連コマンドを指定します。

説明

rhelp コマンドは FTP サーバがサポートしている FTP 関連コマンドを表示します。

rhelp *protocol-command* コマンドは FTP サーバがサポートしている FTP 関連コマンドのヘルプ情報を表示します。

FTP サーバにログインした後のみ実行できます。

例

FTP サーバがサポートしている FTP 関連コマンドを表示します。

ftp> rhelp

```
214-The following FTP commands are recognized
 USER PASS NOOP QUIT SYST TYPE
 HELP CWD  XCWD PWD  CDUP XCUP
 XPWD LIST NLST MLSD PORT EPRT
 PASV EPSV REST RETR STOR APPE
 DELE MKD  XMKD RMD  XRMD ABOR
 SIZE RNFR RNTO
```

```
214 UNIX Type: L8
```

表 4-3 コマンド出力

フィールド	説明
USER	ユーザ名を表示します。
PASS	パスワードを表示します。
NOOP	Null動作です。
SYST	システムパラメータを表示します。
TYPE	要求タイプを表示します。
CWD	現在のディレクトリを変更します。
XCWD	CWDコマンドの拡張コマンドです。
PWD	現在のディレクトリを表示します。
CDUP	上位ディレクトリに移動します。
XCUP	CDUPコマンドの拡張コマンドです。
XPWD	PWDコマンドの拡張コマンドです。
LIST	ファイルリストを表示します。
NLST	ファイルの説明を概要表示します。
MLSD	ファイル内容を表示します。
PORT	アクティブモード（IPv4）です。
EPRT	アクティブモード（IPv6）です。
PASV	パッシブモード（IPv4）です。
EPSV	パッシブモード（IPv6）です。
REST	再起動します。
RETR	ファイルをダウンロードします。
STOR	ファイルをアップロードします。
APPE	アップロードを追記します。

フィールド	説明
DELE	ファイルを削除します。
MKD	フォルダを作成します。
XMKD	MKDコマンドの拡張コマンドです。
RMD	フォルダを削除します。
XRMD	RMDコマンドの拡張コマンドです。
ABOR	転送を中断します。
SIZE	転送ファイルのサイズを表示します。
RNFR	元の名前を表示します。
RNTO	新しい名前を表示します。

4.2.26 rmdir

Syntax

rmdir *directory*

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

directory: リモート FTP サーバのディレクトリ名を指定します。

説明

rmdir コマンドは FTP サーバのディレクトリを完全に削除します。

FTP サーバにログインした後のみ実行できます。

この動作を実行するため、FTP サーバの削除権限が必要です。

ディレクトリを削除する前に、ディレクトリにあるすべてのファイルとサブディレクトリを削除する必要があります。ファイルを削除する方法については、**delete** コマンドを参照してください。

コマンドを実行すると、指定したディレクトリのごみ箱にあるファイルは削除しません。

例

空のディレクトリ subdir1 を削除します。

ftp> rmdir subdir1

```
250 The directory was successfully removed
```

関連コマンド

delete

4.2.27 user

Syntax

user *username* [*password*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

username: ターゲットユーザアカウントのユーザ名を指定します。

password: ターゲットユーザアカウントのパスワードを指定します。

説明

user コマンドは現在の FTP 接続で FTP 認証を初期化します。

FTP サーバにアクセスしようとして認証に失敗した場合、FTP サーバへの接続が終了する前に再度アクセスすることができます。

FTP サーバにログイン後、新しいアカウントに FTP 認証を開始することができます。

新しいアカウントに変更することで、FTP 接続を再確立することなく、異なる権限を取得することができます。

ターゲットユーザアカウントのユーザ名とパスワードは設定されている必要があります。そうでなければ、ユーザアカウントの変更は失敗し、FTP 接続が切断されます。

例

FTP にログインしたのち、ユーザ名 ftp、パスワード 123456 を使用し、FTP サーバにログインします。（出力は FTP サーバによって変わる可能性があります）

- 方法 1:

ftp> user ftp 123456

```
331 Password required for ftp.
```

```
230 User logged in.
```

- 方法 2:

ftp> user ftp

```
331 Password required for ftp.
Password:
230 User logged in.
```

4.2.28 verbose

Syntax

verbose

デフォルト

装置は FTP 動作の詳細情報を表示します。

View

FTP client view

定義済みユーザロール

network-admin

説明

verbose コマンドは FTP 動作の詳細情報の表示機能を有効、あるいは無効にします。

このコマンドは現在のセッションのみ適用されます。再度ログインしたとき、デフォルトの設定に戻ります。

例

FTP 動作の詳細情報の表示機能を無効にします。

ftp> verbose

```
Verbose mode off.
```

get コマンドを実行します。

ftp> get a.cfg 1.cfg

FTP 動作の詳細情報の表示機能を有効にします。

ftp> verbose

```
Verbose mode on.
```

get コマンドを実行します。

ftp> get a.cfg 2.cfg

```
227 Entering Passive Mode (192,168,1,58,68,14)
```

```
150-Accepted data connection
150 The computer is your friend. Trust the computer
226 File successfully transferred
3796 bytes received in 0.00762 seconds (486.5 kbyte/s)
```

4.2.29 ?

Syntax

? [*command-name*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

command-name: FTP クライアントでサポートされるコマンドを指定します。

説明

? コマンドは FTP クライアントでサポートされるすべてのコマンドを表示します。

? *command-name* コマンドはコマンドのヘルプ情報を表示します。

FTP client view において**?**コマンドは、**help** コマンドと同一です。

例

FTP クライアントでサポートされるすべてのコマンドを表示します。

ftp> ?

```
Commands may be abbreviated.  Commands are:

append          delete          ls              quit            rmdir
ascii           debug           mkdir           reget           status
binary          dir             newer           rstatus         system
bye             disconnect      open            rhelp           user
cd              get             passive         rename          verbose
cdup            help            put             reset           ?
close           lcd             pwd             restart
```

dir コマンドのヘルプ情報を表示します。

ftp> ? dir

```
dir             list contents of remote directory
```

関連コマンド

help

目次

このセクションのページは **1-x-x** です。

5 章 TFTP 5-1
5.1 TFTP 設定コマンド 5-1
5.1.1 tftp 5-1
5.1.2 tftp client source 5-3
5.1.3 tftp-server acl 5-4

5章 TFTP

5.1 TFTP設定コマンド

5.1.1 tftp

Syntax

tftp *tftp-server* { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }] *

View

User view

定義済みユーザロール

network-admin

パラメータ

tftp-server: TFTP サーバの IPv4 アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1～253 文字で、大文字、小文字を区別しません。ホスト名で使用できる文字列は英字、数字、ハイフン（-)、アンダーライン（-)、ドット（.）です。

get: ファイルをダウンロードし、宛先ファイルにファイルのディレクトリを書き込みます。宛先ファイルがすでに存在する場合、システムはダウンロードを開始する前に既存のファイルを削除します。ダウンロードが失敗しても既存のファイルは完全に削除されます。

put: ファイルをアップロードします。

sget: ファイルをダウンロードし、宛先ファイルを書き込みする前に、メモリにファイルを保存します。ダウンロードされたファイルが正常にメモリにダウンロードされたのち宛先ファイルにダウンロードされたファイルの書き込みを行います。宛先ファイルがすでに存在する場合、ダウンロードされたファイルは既存のファイルに上書きします。ダウンロードあるいはメモリへの書き込みが失敗すると、既存のファイルは上書きされません。

source-filename: 送信元ファイル名を指定します。設定範囲は 1～255 文字で、大文字、小文字を区別しません。

destination-filename: 宛先ファイル名を指定します。設定範囲は 1～255 文字で、大文字、小文字を区別しません。この引数が指定されない場合、ファイルは送信元ファイル名を使用します。

dscp *dscp-value*: 送信する TFTP パケットの IPv4 パケットの DSCP 値です。パケットを転送する優先度を示します。設定範囲は 0～63 です。デフォルトは 0 です。

source { **interface** *interface-type interface-number* | ip *source-ip-address* }: 送信する TFTP パケットの送信元アドレスを指定します。キーワードが指定されない場合、装置は送信元 IPv4 アドレスとして TFTP サーバへのルートの出力インタフェースのプライマリ IPv4 アドレスを使用します。

- **interface** *interface-type interface-number*: インタフェースのタイプと番号を指定します。インタフェースのプライマリ IPv4 アドレスは送信する TFTP パケットの送信元 IPv4 アドレスとして使用されます。インタフェースが UP でプライマリ IPv4 アドレスが設定されている必要があります。そうでなければ転送が失敗します。
- **ip** *source-ip-address*: IPv4 アドレスを指定します。インタフェースが UP でアドレスが IPv4 アドレスである必要があります。そうでなければ転送が失敗します。

説明

tftp コマンドは TFTP サーバからファイルをダウンロードあるいは IPv4 ネットワークの TFTP サーバにファイルをアップロードします。

tftp コマンドで指定された送信元アドレスは **tftp client source** コマンドで指定された送信元アドレスよりも優先されます。

tftp client source コマンドで指定された送信元アドレスはすべての TFTP 接続に適用されます。**tftp** コマンドで指定された送信元アドレスは現在の TFTP 接続に適用されます。

例

TFTP サーバ 192.168.1.1 から new.bin ファイルをダウンロードし、new.bin として保存します。

<AC> tftp 192.168.1.1 get new.bin

```
Press CTRL+C to abort.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time   Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 13.9M  100 13.9M    0     0  1206k      0  0:00:11  0:00:11  --:--:-- 1206k
Writing file...Done.
```

<AC>

表 5-1 コマンド出力

フィールド	説明
%	ファイル転送の進捗状況を%で示します。
Total	転送されたファイルサイズです。単位はbyteです。
%	全ファイルサイズに対する受信したファイルサイズの割合を%で示します。
Received	受信したファイルサイズです。単位はbyteです。
%	全ファイルサイズに対する送信したファイルサイズの割合を%で示します。

フィールド	説明
Xferd	送信したファイルサイズです。単位はbyteです。
Average Dload	平均ダウンロード速度です。単位はbpsです。
Speed Upload	平均アップロード速度です。単位はbpsです。
Writing file…	システムがダウンロードファイルを記憶媒体に書き込みを行っています。**get**パラメータあるいは**sget**パラメータを指定したときのみ表示されます。 処理が成功すると、フィールドの最後に**Done**と表示します。 処理が失敗すると、フィールドの最後に**Failed**と表示します。

関連コマンド

tftp client source

5.1.2 tftp client source

Syntax

tftp client source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }

undo tftp client source

デフォルト

TFTP サーバに送信する TFTP パケットで設定された送信元 IPv4 アドレスはありません。装置はルートの出力インタフェースのプライマリ IPv4 アドレスを送信元 IP アドレスとして使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 確立する TFTP 接続の送信元インタフェースを指定します。送信元インタフェースのプライマリ IPv4 アドレスは TFTP サーバに送信されるパケットの送信元 IPv4 アドレスとして使用されます。インタフェースが UP でプライマリ IPv4 アドレスが設定されている必要があります。そうでなければ転送が失敗します。

ip *source-ip-address*: 送信する TFTP パケットの送信元 IPv4 アドレスを指定します。UP 状態のインタフェースのアドレスが IPv4 アドレスである必要があります。そうでなければ転送が失敗します。

説明

tftp client source コマンドは TFTP サーバに送信する TFTP パケットの送信元 IPv4 アドレスを指定します。

undo tftp client source コマンドはデフォルトに戻します。

このコマンドを複数実行した場合、最後に実行したコマンドが適用されます。

tftp コマンドで送信元アドレスが指定されている場合、**tftp client source** コマンドで指定された送信元アドレスよりも優先されます。

tftp client source コマンドで指定された送信元アドレスはすべての TFTP 接続に適用されます。**tftp** コマンドで指定された送信元アドレスは現在の TFTP 接続に適用されます。

例

TFTP サーバに送信する TFTP パケットの送信元 IP アドレスを 192.168.20.222 として指定します。

<AC> system-view

[AC] tftp client source ip 192.168.20.222

関連コマンド

tftp

5.1.3 tftp-server acl

Syntax

tftp-server acl *acl-number*

undo tftp-server acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

acl-number: 標準 ACL の番号を指定します。設定範囲は 2000～2999 です。

説明

tftp-server acl コマンドは IPv4 ネットワークの TFTP サーバへの装置のアクセスを制御する ACL を使用します。

undo tftp-server acl コマンドはデフォルトに戻します。

ACL を使用して、装置から指定された TFTP サーバへのアクセスを許可または禁止することができます。

例

TFTP サーバ 1.1.1.1 へのアクセスのみを許可します。

<AC> system-view

[AC] acl basic 2000

[AC -acl-ipv4-basic-2000] rule permit source 1.1.1.1 0

[AC -acl-ipv4-basic-2000] quit

[AC] tftp-server acl 2000

目次

このセクションのページは **1-x-x** です。

6 章 ファイルシステム管理 6-1
6.1 ファイルシステム管理設定コマンド 6-1
6.1.1 cd 6-2
6.1.2 copy 6-2
6.1.3 delete 6-4
6.1.4 dir 6-5
6.1.5 file prompt 6-7
6.1.6 fixdisk 6-8
6.1.7 format 6-8
6.1.8 gunzip 6-9
6.1.9 gzip 6-10
6.1.10 mkdir 6-11
6.1.11 more 6-12
6.1.12 move 6-12
6.1.13 pwd 6-13
6.1.14 rename 6-14
6.1.15 reset recycle-bin 6-14
6.1.16 rmdir 6-15
6.1.17 tar create 6-16
6.1.18 tar extract 6-17
6.1.19 tar list 6-19
6.1.20 undelete 6-20

6章 ファイルシステム管理

6.1 ファイルシステム管理設定コマンド

⚠ **注意：**

- 記録媒体、ファイル、ディレクトリを管理する前に、設定が装置に与える影響を確認してから行ってください。
- ピリオド（．）の名前で始まるファイルあるいはディレクトリは、隠しファイルあるいは隠しディレクトリです。ファイルあるいはディレクトリの先頭にピリオド（．）を使用しないでください。
- いくつかの隠しファイルと隠しディレクトリが存在します。ファイルシステムの管理を行う際は、隠しファイルや隠しディレクトリを修正しないでください。

⚠ **注意：**

- 表示される空き容量は実際のファイルサイズで計算されています。保存に必要なサイズはファイルの種類によって実際のファイルサイズと異なる場合がありますので、ファイルの保存は十分な空き容量があることを確認してから行ってください。
- ファイルのダウンロードやコピーを行う場合は、十分な空き容量を確保してから行ってください。空き容量が不足している場合には、エラーとなり異常なファイルが残る場合があります。保存に失敗した場合は、不要なファイルを削除してください。

装置はフラッシュメモリだけをサポートします。

ファイルシステムはフラッシュメモリなどの記憶媒体です。

ファイル名、ディレクトリ名はファイル名のフォーマットで指定されています。詳細はオペレーションマニュアルのセクション 1 *はじめに “ファイルシステム管理”* を参照してください。

別のユーザがファイルシステムのフォーマットを行っている間、ファイルシステムにアクセスすることはできません。

フォーマットの後、ファイルシステムにアクセスする場合、以下のいずれかの作業を行ってください。

- コマンドのファイルシステムの名前を指定してください。たとえば、フラッシュメモリのすべてのファイル、ディレクトリを表示する **dir cfa0:/**コマンドを使用してください。

- コマンドを使用する前に、ファイルシステムにディレクトリを変更する場合、**cd** コマンドを使用してください。たとえば、フラッシュメモリのルートディレクトリに移動する場合、コ **cd cfa0:/**コマンドを使用してください。そしてすべてのファイル、ディレクトリを表示するために **dir** コマンドを使用してください。

6.1.1 cd

Syntax

cd { *directory* | **..** }

View

User view

定義済みユーザロール

network-admin

パラメータ

directory: 宛先ディレクトリの名前を指定します。

..: 上位ディレクトリに戻ります。現在のディレクトリがルートディレクトリである場合、コマンドを実行したときエラーメッセージが表示されます。このパラメータに対するコマンドラインヘルプはありません。

説明

cd コマンドは現在の作業ディレクトリを変更します。

例

装置にログインした後、ディレクトリ test にアクセスします。

<AC> cd test

上位ディレクトリに戻ります。

<AC> cd

6.1.2 copy

Syntax

copy *source-file* { *dest-file* | *dest-directory* } [**source interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

source-file: ファイルの名前あるいは URL を指定します。ファイルが装置上ではなく FTP、TFTP サーバにある場合、ファイル URL を指定します。URL が大文字、小文字を区別するかどうかはサーバによって異なります。

{ *dest-file* | *dest-directory* }: 宛先ファイルの名前あるいは URL を指定します。送信元ファイルを FTP あるいは TFTP サーバにコピーする場合、URL を指定します。ディレクトリを指定する場合、装置は指定したファイルをディレクトリにコピーしもとのファイル名で保存します。URL が大文字、小文字を区別するかどうかはサーバによって異なります。

source interface *interface-type interface-number*: サーバに接続するために使用される送信元インタフェースを指定します。送信元インタフェースを指定すると、装置外部向けパケットの送信元 IP アドレスとして、装置は送信元インタフェースのプライマリ IP アドレスを使用します。本オプションを指定しなかった場合、装置は送信元インタフェースとして外向きインタフェースを使用します。

説明

copy コマンドはファイルをコピーします。

以下の処理を実行することができます。

- ローカルファイルをコピーし、ローカルに保存します。
- ローカルファイルをコピーし、FTP あるいは TFTP サーバに保存します。
- FTP あるいは TFTP サーバのファイルをコピーし、ローカルに保存します。

ファイルあるいはディレクトリを指定するため、以下のガイドラインを使用します。

位置	フォーマット	補足
装置	オペレーションマニュアルのセクション1 *はじめに“ファイルシステム管理”の“ファイル名のガイドライン”*を参照してください。	―
FTPサーバ	以下の形式のURLを入力します。 ftp://FTP username[:password]@server address[:port number]/file path[/file name].	ユーザ名とパスワードはFTPサーバで設定されているユーザ名とパスワードと同一にしてください。 サーバがユーザ名のみでユーザを認証する場合、パスワードを入力する必要はありません。 たとえばユーザ名1、パスワード1、FTPサーバ1.1.1.1で許可された作業ディレクトリのstartup.cfgを指定する場合、ftp://1:1@1.1.1.1/startup.cfgを入力します。

位置	フォーマット	補足
TFTPサーバ	以下の形式のURLを入力します。 tftp://server address[:port number]/file path[/file name].	たとえば、TFTPサーバ1.1.1.1の作業ディレクトリのstartup.cfgをしている場合、tftp://1.1.1.1/startup.cfgを入力します。

例

現在のディレクトリのファイル test.cfg をコピーし、ファイル名を testbackup.cfg として現在のディレクトリに保存します。

<AC> copy test.cfg testbackup.cfg

```
Copy cfa0:/test.cfg to cfa0:/testbackup.cfg? [Y/N]:y
Copying file cfa0:/test.cfg to cfa0:/testbackup.cfg...Done.
```

6.1.3 delete

Syntax

delete [**/unreserved**] *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

/unreserved: 指定されたファイルを完全に削除します。このパラメータを指定しない場合、ごみ箱にファイルを移動します。

file: 削除するファイル名を指定します。アスタリスク（*）はワイルドカードとして使用できます。たとえば、現在のディレクトリにある拡張子が“.txt”のファイルを削除する場合、“*.txt”と入力します。

説明

delete コマンドはファイルを削除します。

delete /unreserved *file* コマンドを使用する場合、削除されたファイルを復元することができません。

/unreserved パラメータを使用しないで **delete** *file* コマンドは指定したファイルをごみ箱に移動します。システムが記憶領域を使い切っていた場合、本コマンドはファイルを永久に削除します。

ごみ箱に移動したファイルは **undelete** コマンドを使用して復元することができます。

ごみ箱のファイルを削除する際に **delete** コマンドを使用しないでください。ごみ箱のファイルを削除する場合、**reset recycle-bin** コマンドを使用してください。

異なるディレクトリにある同一ファイル名の 2 つのファイルを削除する場合､2 つのファイルはごみ箱に保存されます。同一ディレクトリの同一ファイル名の 2 つのファイルを削除した場合、最後に削除されたファイルのみがごみ箱に保存されています。

例

現在のディレクトリからファイル 1.cfg を削除します。

<AC> delete 1.cfg

```
Delete cfa0:/1.cfg? [Y/N]:y
Deleting file cfa0:/1.cfg...Done.
```

現在のディレクトリからファイル 1.cfg を完全に削除します。

<AC> delete /unreserved 1.cfg

```
The file cannot be restored. Delete cfa0:/1.cfg? [Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Deleting file cfa0:/1.cfg...Done.
```

関連コマンド

- **reset recycle-bin**
- **undelete**

6.1.4 dir

Syntax

dir [**/all**] [*file* | *directory* | **/all-filesystems**]

View

User view

定義済みユーザロール

network-admin

パラメータ

/all: 現在のディレクトリのすべてのファイルとディレクトリを隠しファイル、隠しディレクトリを含めてすべて表示します。このパラメータを指定しない場合、隠しファイル、隠しディレクトリを除いたファイルとディレクトリが表示されます。

file: 指定したファイルを表示します。アスタリスク（*）はワイルドカードとして使用できます。たとえば、現在のディレクトリにある拡張子が“.txt”のファイルを表示する場合、**dir** **.txt* と入力します。

directory: 指定したディレクトリを表示します。

/all-filesystems: 装置のすべてのファイルシステムのルートディレクトリのファイルとディレクトリを表示します。

説明

dir コマンドはファイルあるいはディレクトリを表示します。

パラメータを指定しない場合、現在のディレクトリの隠しファイル、隠しディレクトリを除いたファイルとディレクトリを表示します。

ごみ箱のディレクトリ名は“.trash”です。ごみ箱のファイルを表示する場合、以下のどちらかの方法を使用します。

- **dir /all** *.trash* コマンドを実行します。
- **cd** *.trash* コマンドを実行し、**dir** コマンドを実行します。

例

現在のディレクトリにあるすべてのファイルとディレクトリを表示します。

<AC> dir /all

```
Directory of cfa0:/
...
```

装置のすべてのファイルシステムのルートディレクトリにあるすべてのファイルとディレクトリを表示します。

<AC> dir /all-filesystems

```
Directory of cfa0:/
...
```

表 6-1 コマンド出力

フィールド	説明
Directory of	現在のディレクトリです。
0 -rwh 3144 Apr 26 2014 13:45:28 xx.xx	ファイルあるいはディレクトリ情報です。 • **0**—ファイルあるいはディレクトリ番号です。システムによって自動で割り当てられます。 • **-rwh**—ファイルあるいはディレクトリの属性です。最初の文字はディレクトリを示します。**d**はディレクトリで、ーはファイルです。2番目の文字はファイルあるいはディレクトリが読み込み可能かどうかを示します。**r**は読み込み可能です。3番目の文字はファイルあるいはディレクトリが書き込み可能かどうかを示します。**w**は書き込み可能です。4番目の文字はファイルあるいはディレクトリが隠しファイルあるいは隠しディレクトリかどうかを示します。**h**は隠しファイルあるいは隠しディレクトリで、ーは通常のファイルあるいはディレクトリです。変更、名前の変更、隠しファイルあるいは隠しディ

フィールド	説明
	レクトリの削除は機能に影響します。 • **3144**—ファイルサイズです。単位はbyteです。ディレクトリはハイフン（－）が表示されます。 • **Apr 26 2014 13:45:28**—ファイルあるいはディレクトリが変更された最後の日時です。 • **xx.xx**—ファイルあるいはディレクトリ名です。

6.1.5 file prompt

Syntax

file prompt { **alert** | **quiet** }

undo file prompt

デフォルト

alert

View

System view

定義済みユーザロール

network-admin

パラメータ

alert: ファイルの破損やデータの損失など、望ましくない結果を引き起こす可能性のある操作について、システムが警告できるようにします。

quiet: ファイルあるいはディレクトリの操作に関する警告を行いません。

説明

file prompt コマンドはファイル、ディレクトリのプロンプトモードを設定します。

undo file prompt コマンドはデフォルトに戻します。

quiet モードである場合、システムはいかなるファイル操作に関しても警告を行いません。**alert** モードである場合、望ましくない結果を引き起こす可能性のある操作を中止できるように、警告を表示します。

例

ファイル、ディレクトリのプロンプトモードを alert に設定します。

<AC> system-view

[AC] file prompt alert

6.1.6 fixdisk

Syntax

fixdisk *filesystem*

View

User view

定義済みユーザロール

network-admin

パラメータ

filesystem: ファイルシステムの名前を指定します。値は装置の種類によって異なります。

説明

fixdisk コマンドは何らかの異常操作によりファイルシステムが使用できなくなった場合、ファイルシステムを確認し、ダメージ領域を復元します。

本コマンドは、ファイルシステムの空きスペースが使用できないあるいは異常な操作により解放されたとき、ファイルシステムを修正します。

ファイルシステムへのアクセスがないときのみ、ファイルシステムをフォーマットすることができます。

例

ファイルシステムの空きスペースを復元します。

<AC> fixdisk cfa0:

```
Restoring cfa0: may take some time...
Restoring cfa0:...Done.
```

6.1.7 format

Syntax

format *filesystem*

View

User view

定義済みユーザロール

network-admin

パラメータ

filesystem: ファイルシステムの名前を指定します。値は装置の種類によって異なります。

説明

format コマンドはファイルシステムをフォーマットします。

ファイルシステムをフォーマットすると、ファイルシステムにあるすべてのファイルを完全に削除します。ファイルシステムに起動設定ファイルが存在する場合は、必要であればバックアップを取ってください。

ファイルシステムへのアクセスがないときのみ、ファイルシステムをフォーマットすることができます。

例

ファイルシステムをフォーマットします。

<AC> format cfa0:

```
All data on cfa0: will be lost, continue? [Y/N]:y
Formatting cfa0:... Done.
```

6.1.8 gunzip

Syntax

gunzip *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

file: 解凍するファイルの名前を指定します。拡張子は“.gz”にする必要があります。

説明

gunzip コマンドはファイルを解凍します。

本コマンドは解凍した後、もとのファイルを削除します。

例

ファイル system.bin.gz を解凍します。

1)　ファイルを解凍する前に、system の文字列で始まる名前のファイルを表示します。

<AC> dir system.*

```
Directory of cfa0:
  1 -rw-        20 Jun 14 2012 10:18:53   system.bin.gz
472972 KB total (472840 KB free)
```

2)　ファイル system.bin.gz を解凍します。

<AC> gunzip system.bin.gz

```
Decompressing file cfa0:/system.bin.gz..... Done.
```

3)　解凍した操作の確認を行います。

<AC> dir system.*

```
Directory of cfa0:
  1 -rw-         0 May 30 2012 11:42:25   system.bin
472972 KB total (472844 KB free)
```

6.1.9 gzip

Syntax

gzip *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

file: 圧縮するファイル名を指定します。圧縮するファイルの拡張子は、“.gz”で保存されます。

説明

gzip コマンドはファイルを圧縮します。

本コマンドは圧縮した後、もとのファイルを削除します。

例

ファイル system.bin を圧縮します。

1)　ファイルを圧縮する前に、system の文字列で始まる名前のファイルを表示します。

<AC> dir system.*

```
Directory of cfa0:
  1 -rw-         0 May 30 2012 11:42:24   system.bin
472972 KB total (472844 KB free)
```

2)　ファイル system.bin を圧縮します。

<AC> gzip system.bin

```
Compressing file cfa0:/system.bin..... Done.
```

3)　圧縮した操作の確認を行います。

<AC> dir system.*

```
Directory of cfa0:
   1 -rw-         20 Jun 14 2012 10:18:53   system.bin.gz
472972 KB total (472840 KB free)
```

6.1.10 mkdir

Syntax

mkdir *directory*

View

User view

定義済みユーザロール

network-admin

パラメータ

directory: ディレクトリの名前を指定します。

説明

mkdir コマンドは現在のディレクトリの下にディレクトリを作成します。

ディレクトリの名前は指定されたディレクトリ内で一意にする必要があります。

既に存在するディレクトリに対してのみ新しいディレクトリを作成可能です。たとえば、ディレクトリ cfa0:/test/mytest を作成する場合、ディレクトリ test は既に存在している必要があります。

例

現在のディレクトリにディレクトリ test を作成します。

<AC> mkdir test

```
Creating directory cfa0:/test... Done.
```

現在のディレクトリにディレクトリ test/subtest を作成します。

<AC> mkdir test/subtest

```
Creating directory cfa0:/test/subtest... Done.
```

6.1.11 more

Syntax

more *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

file: ファイル名を指定します。

説明

more コマンドはテキストファイルの内容を表示します。

例

ファイル test.txt の内容を表示します。

<AC> more test.txt

```
Have a nice day.
```

ファイル testcfg.cfg の内容を表示します。

<AC> more testcfg.cfg

```
#
version 7.1.064, ESS 5103
#
 sysname AC
#
  ---- More ----
```

6.1.12 move

Syntax

move *source-file* { *dest-file* | *dest-directory* }

View

User view

定義済みユーザロール

network-admin

パラメータ

source-file: ソースファイルの名前を指定します。

dest-file: ターゲットファイルの名前を指定します。

dest-directory: ターゲットファイルあるいはディレクトリの名前を指定します。

説明

move コマンドはファイルを移動します。

ターゲットディレクトリを指定する場合、システムはファイル名を変更しないで指定したディレクトリにソースファイルを移動します。

例

ファイル cfa0:/test/sample.txt を cfa0:/に移動し、ファイル 1.txt として保存します。

<AC> move test/sample.txt 1.txt

```
Move cfa0:/test/sample.txt to cfa0:/1.txt? [Y/N]:y
Moving file cfa0:/test/sample.txt to cfa0:/1.txt ...Done.
```

ファイル b.cfg をディレクトリ test2 に移動します。

<AC> move b.cfg test2

```
Move cfa0:/b.cfg to cfa0:/test2/b.cfg? [Y/N]:y
Moving file cfa0:/b.cfg to cfa0:/test2/b.cfg... Done.
```

6.1.13 pwd

Syntax

pwd

View

User view

定義済みユーザロール

network-admin

説明

pwd コマンドは現在の作業ディレクトリを表示します。

例

現在の作業ディレクトリを表示します。

<AC> pwd

```
cfa0:
```

6.1.14 rename

Syntax

rename { *source-file* | *source-directory* } { *dest-file* | *dest-directory* }

View

User view

定義済みユーザロール

network-admin

パラメータ

source-file: ソースファイルの名前を指定します。

source-directory:ソースディレクトリの名前を指定します。

dest-file: ターゲットファイルの名前を指定します。

dest-directory:ターゲットディレクトリの名前を指定します。

説明

rename コマンドはファイルあるいはディレクトリの名前を変更します。

現在の作業ディレクトリのファイルあるいはディレクトリに変更しようとするファイルあるいはディレクトリの名前が存在する場合、本コマンドは実行されません。

例

ファイル copy.cfg をファイル test.cfg に変更します。

<AC> rename copy.cfg test.cfg

```
Rename cfa0:/copy.cfg as cfa0:/test.cfg? [Y/N]:y
Renaming cfa0:/copy.cfg as cfa0:/test.cfg... Done.
```

6.1.15 reset recycle-bin

Syntax

reset recycle-bin [**/force**]

View

User view

定義済みユーザロール

network-admin

パラメータ

/force: 確認のプロンプトの表示を行わず、ごみ箱のすべてのファイルを削除します。このパラメータを指定しない場合、確認のプロンプトが表示されます。

説明

reset recycle-bin コマンドはごみ箱からファイルを削除します。

delete *file* コマンドはごみ箱にファイルを移動します。ファイルを完全に削除する場合、**reset recycle-bin** コマンドを使用してごみ箱を消去します。

ファイルが壊れている場合、**reset recycle-bin** コマンドではファイルを削除できない可能性があります。その場合は、**reset recycle-bin /force** コマンドを使用します。

例

2 つのファイルが存在しているごみ箱からファイルを削除します。

<AC> reset recycle-bin

```
Clear cfa0:/a.cfg? [Y/N]:y
Clearing file cfa0:/a.cfg... Done.
Clear cfa0:/b.cfg? [Y/N]:y
Clearing file cfa0:/b.cfg... Done.
```

2 つのファイルが存在しているごみ箱からファイル b.cfg を削除します。

<AC> reset recycle-bin

```
Clear cfa0:/a.cfg? [Y/N]:n
Clear cfa0:/b.cfg? [Y/N]:y
Clearing file cfa0:/b.cfg... Done.
```

関連コマンド

delete

6.1.16 rmdir

Syntax

rmdir *directory*

View

User view

定義済みユーザロール

network-admin

パラメータ

directory: ディレクトリ名を指定します。

説明

rmdir コマンドはディレクトリを削除します。

ディレクトリを削除するため、ディレクトリのすべてのファイルとサブディレクトリを完全に削除するかごみ箱に移動する必要があります。ごみ箱に移動する場合、**rmdir** コマンドを実行して完全に削除することができます。

例

ディレクトリ subtest を削除します。

Delete the subtest directory.

<AC> rmdir subtest/

```
Remove directory cfa0:/test/subtest and the files in the recycle-bin under this
directory will be deleted permanently. Continue? [Y/N]:y
Removing directory cfa0:/test/subtest... Done.
```

6.1.17 tar create

Syntax

tar create [**gz**] *archive-file dest-file* [**verbose**] **source** { *source-file* | *source-directory* }&<1-5>

View

User view

定義済みユーザロール

network-admin

パラメータ

gz: ファイル、ディレクトリをアーカイブする前に **gzip** コマンドでファイル、ディレクトリを圧縮します。指定しない場合、圧縮しないでファイル、ディレクトリをアーカイブします。

archive-file dest-file: アーカイブファイル名を指定します。**gz** パラメータを指定する場合、引数の拡張子は“.tar.gz”にする必要があります。**gz** パラメータを指定しない場合、引数の拡張子は“.tar”にする必要があります。

verbose: 正常にアーカイブされたファイル、ディレクトリの名前を表示します。指定しない場合、ファイル、ディレクトリの名前を表示しません。

source { *source-file* | *source-directory* }&<1-5>: アーカイブされるファイル、ディレクトリを指定します。引数は半角スペースで区切ることで 5 つまで指定することができます。

説明

tar create コマンドはファイル、ディレクトリをアーカイブします。

例

ファイル 1.cfg、2.cfg、ディレクトリ test をファイル a.tar にアーカイブします。

<AC> tar create archive-file a.tar source 1.cfg 2.cfg test

```
Creating archive cfa0:/a.tar Done.
```

ファイル 1.cfg、2.cfg、ディレクトリ test をファイル b.tar.gz に圧縮してアーカイブします。

<AC> tar create gz archive-file b.tar.gz source 1.cfg 2.cfg test

```
Creating archive cfa0:/b.tar.gz Done.
```

ファイルとディレクトリを圧縮、アーカイブします。アーカイブしたファイルとディレクトリを表示します。

<AC> tar create gz archive-file c.tar.gz verbose source 1.cfg 2.cfg test

```
1.cfg
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

関連コマンド

- **tar extract**
- **tar list**

6.1.18 tar extract

Syntax

tar extract archive-file *file* [**verbose**] [**screen** | **to** *directory*]

View

User view

定義済みユーザロール

network-admin

パラメータ

archive-file *file*: アーカイブファイル名を指定します。拡張子は “.tar” あるいは “.tar.gz” です。

verbose: 正常に解凍したファイルとディレクトリの名前を表示します。

screen: 画面に解凍したファイルとディレクトリの内容を表示します。解凍したファイルは保存されません。

to *directory*: 解凍したファイルとディレクトリをパスに保存します。directory 引数はディレクトリを指定します。

説明

tar extract コマンドはファイルとディレクトリを解凍します。

screen パラメータあるいは **to** *directory-name* パラメータを指定しない場合、解凍したファイルとディレクトリを解凍し、解凍ファイルとして同一ディレクトリに保存します。

コマンドはもとの名前を使用して、解凍したファイル、ディレクトリを保存します。既に同一ファイル、ディレクトリが存在する場合、解凍したファイル、ディレクトリを既存のファイル、ディレクトリに上書きします。

例

アーカイブファイル a.tar からファイル、ディレクトリを解凍します。

<AC> tar extract archive-file a.tar

```
Extracting archive cfa0:/a.tar Done.
```

アーカイブファイル a.tar からファイルとディレクトリを解凍し、アーカイブしたファイルとディレクトリの名前を表示します。

<AC> tar extract archive-file a.tar.gz verbose

```
1.cfg
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

アーカイブファイル a.tar からファイルを解凍し、アーカイブしたファイルの内容を表示します。

<AC> tar extract archive-file a.tar.gz screen

```
#
 version 7.1.055, Demo 2501008
#
```

```
 sysname AC
#
...
```

関連コマンド

- **tar create**
- **tar list**

6.1.19 tar list

Syntax

tar list archive-file *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

archive-file *file*: アーカイブファイル名を指定します。拡張子は “.tar” あるいは “.tar.gz” です。

説明

tar list コマンドはアーカイブしたファイルとディレクトリの名前を表示します。

例

アーカイブしたファイルとディレクトリの名前を表示します。

<AC> tar list archive-file a.tar

```
1.cfg
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

関連コマンド

- **tar create**
- **tar extract**

6.1.20 undelete

Syntax

undelete *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

file: 復元するファイルの名前を指定します。

説明

undelete コマンドはごみ箱からファイルを復元します。

ディレクトリに同一名のファイルが存在する場合、既存のファイルに上書きするかどうかの画面を表示します。“Y”を入力した場合、既存のファイルは上書きされます。“N”を入力した場合、このコマンドは実行されません。

例

copy.cfg ファイルを復元します。このファイルはディレクトリ cfa0:からごみ箱に移動されたファイルです。

<AC> undelete copy.cfg

```
Undelete cfa0:/copy.cfg? [Y/N]:y
Undeleting file cfa0:/copy.cfg... Done.
```

ファイル startup.cfg を復元します。このファイルはディレクトリ cfa0:/seclog からごみ箱に移動されたファイルです。

- 方法 1:

<AC> undelete seclog/startup.cfg

```
Undelete cfa0:/seclog/startup.cfg? [Y/N]:y
Undeleting file cfa0:/seclog/startup.cfg... Done.
<AC>
```

- 方法 2:

<AC> cd seclog

<AC> undelete startup.cfg

```
Undelete cfa0:/seclog/startup.cfg? [Y/N]:y
Undeleting file cfa0:/seclog/startup.cfg... Done.
```

目次

このセクションのページは **1-x-x** です。

7 章 コンフィグレーションファイル管理 7-1
7.1 コンフィグレーションファイル管理設定コマンド 7-1
7.1.1 backup startup-configuration 7-1
7.1.2 display current-configuration 7-2
7.1.3 display current-configuration diff 7-3
7.1.4 display default-configuration 7-5
7.1.5 display diff 7-6
7.1.6 display saved-configuration 7-8
7.1.7 display startup 7-10
7.1.8 display this 7-11
7.1.9 reset saved-configuration 7-12
7.1.10 restore startup-configuration 7-14
7.1.11 save 7-15
7.1.12 startup saved-configuration 7-17

7章 コンフィグレーションファイル管理

7.1 コンフィグレーションファイル管理設定コマンド

7.1.1 backup startup-configuration

Syntax

backup startup-configuration to *ipv4-server* [*dest-filename*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ipv4-server: IPv4 アドレスあるいはホスト名で TFTP サーバを指定します。ホスト名は大文字小文字を区別しない 1～253 文字の文字列です。大文字、小文字を区別しません。ホスト名で使用できる文字列は文字、数字、ハイフン（-）、アンダーライン（-）、ドット（.）です。

dest-filename: サーバの次回起動時に使用する起動コンフィグレーションファイルを保存するためのターゲットファイル名を指定します。ファイル名の拡張子は.“cfg”です。ターゲットファイル名を指定しない場合、ソースファイル名が使用されます。

説明

backup startup-configuration コマンドは TFTP サーバに次回の起動に使用する起動コンフィグレーションファイルをバックアップします。

例

TFTP サーバ 2.2.2.2 に次回の起動に使用する起動コンフィグレーションファイル 192-168-1-26.cfg をバックアップします。

<AC> backup startup-configuration to 2.2.2.2 192-168-1-26.cfg

```
Backing up the main startup cofiguration file to 2.2.2.2…
Done.
```

関連コマンド

restore startup-configuration

7.1.2 display current-configuration

🕮 **メモ：**

by-section のパラメータはソフトウェアバージョン 7.2.93a を含む以降のソフトウェアからサポートしています。

Syntax

display current-configuration [**configuration** [*module-name*] | **interface** [*interface-type* [*interface-number*]]] [**by-section** { **begin** | **exclude** | **include** } *regular-expression*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

configuration [*module-name*]: 機能の設定を表示します。*module-name* 引数は機能モジュールを指定します。指定されない場合、設定されたすべての機能を表示します。有効な機能モジュールは装置の設定に依存します。

interface [*interface-type* [*interface-number*]]: インタフェースの設定を表示します。*interface-type* 引数はインタフェースタイプで、*interface-number* 引数はインタフェース番号を示します。

by-section: 現在の有効な設定をセクションごとに表示します。各セクションはコマンドビューで構成されており、隣接する 2 つのセクションはシャープ記号（#）で区切られています。このキーワードを指定しない場合、コマンドは実行中の設定を行ごとに表示します。

{ **begin** | **exclude** | **include** }: 実行中の設定を表示するためのルールを指定します。

- **begin**: 指定した正規表現に一致する最初の設定セクションと、それ以降のすべての設定セクションを表示します。
- **exclude**: 指定した正規表現に一致しないすべての設定セクションを表示します。
- **include**: 指定した正規表現に一致するすべての設定セクションを表示します。

regular-expression: 設定セクションをフィルタリングするための正規表現を指定します。1～256 文字の大文字・小文字を区別する文字列です。

説明

display current-configuration コマンドは現在の有効な設定を表示します。

本コマンドを使用して設定の確認を行うことができます。

システムは自動的にパラメータの設定を変更します。たとえば、システムの制限に合わない設定がある場合、自動的に変更します。設定が変更されると、システムの制限に適合した設定を表示します。

デフォルトの設定を使用しないパラメータは表示されません。

例

ローカルユーザの設定を表示します。

<AC> display current-configuration configuration local-user

```
#
local-user ftp
 password                                                                hash
$h$6$Twd73mLrN8O2vvD5$Cz1vgdpR4KoTiRQNE9pg33gU14Br2p1VguczLSVyJLO2huV5Syx/LfD
If8ROLtVErJ/C31oq2rFtmNuyZf4STw==
 service-type ftp
 authorization-attribute user-role network-operator
#
local-user root
 password                                                                hash
$h$6$Twd73mLrN8O2vvD5$Cz1vgdpR4KoTiRQNE9pg33gU14Br2p1VguczLSVyJLO2huV5Syx/LfD
If8ROLtVErJ/C31oq2rFtmNuyZf4STw==
 service-type ssh telnet terminal
 authorization-attribute user-role network-admin
#
return
```

7.1.3 display current-configuration diff

Syntax

display current-configuration diff

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display current-configuration diff コマンドは現在のコンフィグレーションファイルと次回の起動に使用するコンフィグレーションファイル間のコンフィグレーション差分を表示します。

本コマンドは、以下のステップで現在のコンフィグレーションファイルと次回の起動に使用するコンフィグレーションファイルを比較します。

1) 現在のコンフィグレーションファイルと、次回の起動に使用するメインのコンフィグレーションファイルを比較します。
2) 次回の起動に使用するメインのコンフィグレーションファイルが利用不可の場合は、本コマンドはバックアップの次回の起動に使用するコンフィグレーションファイルと現在のコンフィグレーションファイルを比較します。

メインとバックアップの両方の次回の起動に使用するコンフィグレーションファイルが利用不可の場合は、システムは、次回の起動に使用するコンフィグレーションファイルが存在しないことを示すメッセージを表示します。

例

現在のコンフィグレーションファイルと次回の起動に使用するコンフィグレーションファイル間のコンフィグレーション差分を表示します。

<AC> display current-configuration diff

```
--- Startup configuration
+++ Current configuration
@@ -17,7 +17,9 @@
 #
 vlan 200
 #
-vlan 300
+vlan 400
+#
+vlan 500
 #
 interface Vlan-interface1
 #
<AC>
```

表 7-1 コマンド出力

フィールド	説明
---A +++ B	● **A**－比較元のコンフィグレーションファイルを表示します。**Startup configuration**、**Current configuration**、ディレクトリ情報を含む比較元設定ファイル名のいずれかを示します。 ● **B**－比較対象のコンフィグレーションファイルを表示します。**Current configuration**、**Startup configuration**、ディレクトリ情報を含む比較対象設定ファイル名のいずれかを示します。 この例では**Startup configuration**、**Current configuration**はそれぞ

フィールド	説明
	れ比較元のコンフィグレーションファイル、比較先コンフィグレーションファイルです。
@@ *-linenumber1,number1* *+linenumber2,number2* @@	コマンドラインの相違に関する位置の概要です。 ● *-linenumber1,number1*—相違が含まれる比較元の設定です。*linenumber1*はセクションの開始行を示します。*nunber1*のセクションの開始行と最終行間での行の数を示します。 ● *+linenumber2,number2*—相違が含まれる比較先の設定です。*linenumber2*はセクションの開始行を示します。*nunber2*のセクションの開始行と最終行間での行の数を示します。
cmd1 - cmd2 + cmd3 cmd4	比較したコンフィグレーションファイルの相違を示します。 ● *cmd1*、*cmd4*ーコマンドラインの先頭に（-）あるいは（+）がついていない場合、比較元と比較先のコンフィグレーションファイルの両方のコマンドラインの行が含まれます。これはコマンドラインの相違の位置を示すための情報です。 ● *-cmd2*ーコマンドラインに比較元のコンフィグレーションファイルに記載されているが、比較先のコンフィグレーションファイルに記載されていない場合、（-）の記号がコマンドラインの先頭に表示されます。 ● *-cmd3*ーコマンドラインに比較先のコンフィグレーションファイルに記載されているが、比較元のコンフィグレーションファイルに記載されていない場合、（+）の記号がコマンドラインの先頭に表示されます。 この例ではVLAN 200、Vlan-interface1が両方のコンフィグレーションファイルに含まれていることを示します。VLAN 400、VLAN 500は**Current configuration**にのみ含まれています。VLAN 300は**Startup configuration**にのみ含まれています。

関連コマンド

- **display current-configuration**
- **display diff**
- **display saved-configuration**

7.1.4 display default-configuration

Syntax

display default-configuration

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display default-configuration コマンドは工場出荷状態のデフォルトコンフィグレーション設定を表示します。

工場出荷状態のコンフィグレーションはデフォルトコンフィグレーションファイルにあります。製品仕様のデフォルト設定は初期設定と異なります。設定ファイルがない場合あるいは設定ファイルが壊れている場合、デフォルト設定によって装置が起動し、正常に動作するようにします。

例

デフォルトコンフィグレーション設定を表示します。

<AC> display default-configuration

7.1.5 display diff

Syntax

display diff configfile *file-name-s* { **configfile** *file-name-d* | **current-configuration** | **startup-configuration** }

display diff current-configuration { **configfile** *file-name-d* | **startup-configuration** }

display diff startup-configuration { **configfile** *file-name-d* | **current-configuration** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

configfile *file-name-s*: 比較元のコンフィグレーションファイルを指定します。

configfile *file-name-d*: 比較先のコンフィグレーションファイルを指定します。

current-configuration: 現在のコンフィグレーションファイルを指定します。**display diff current-configuration** コマンドにおいて、このパラメータは、比較元のコンフィグ

レーションファイルを指定します。他の 2 つの **display diff** コマンドにおいて、このパラメータは比較先のコンフィグレーションファイルを指定します。

startup-configuration: 次回の起動に使用するコンフィグレーションを指定します。**display diff startup-configuration** コマンドにおいて、このパラメータは比較元のコンフィグレーションを指定します。他の 2 つの **display diff** コマンドにおいて、このパラメータは比較先のコンフィグレーションを指定します。

説明

display diff コマンドはコンフィグレーション差分を表示します。

startup-configuration キーワードを指定した場合、システムは次回の起動に使用するメインのコンフィグレーションを比較するために、以下の順序で検索します。

1) 次回の起動に使用するメインのコンフィグレーションファイル
2) 次回の起動に使用するメインのコンフィグレーションファイルが利用不可な場合は、本コマンドはバックアップの次回の起動に使用するコンフィグレーションファイル

メインとバックアップの両方の次回の起動に使用するコンフィグレーションファイルが利用不可な場合は、システムは、次回の起動に使用するコンフィグレーションファイルが存在しないことを示すメッセージを表示します。

例

startup.cfg と test.cfg の差分を表示します。

<AC> display diff configfile startup.cfg configfile test.cfg

```
--- cfa0:/startup.cfg
+++ cfa0:/test.cfg
@@ -17,7 +17,9 @@
 #
 vlan 200
 #
-vlan 300
+vlan 400
+#
+vlan 500
 #
 interface Vlan-interface1
 #
<AC>
```

出力では、VLAN200 と VLAN-interface 1 は両方のコンフィグレーションに含まれています。は VLAN 400、VLAN 500 は test.cfg のみに含まれますが、VLAN 300 は startup.cfg のみに含まれます。

現在のコンフィグレーションファイルと次回の起動に使用するコンフィグレーションファイル間の差分を表示します。

<AC> display diff current-configuration startup-configuration

```
--- Current configuration
+++ Startup configuration
@@ -17,9 +17,7 @@
 #
 vlan 200
 #
-vlan 400
-#
-vlan 500
+vlan 300
 #
 interface Vlan-interface1
 #
<AC>
```

出力では、VLAN 200 と VLAN-interface 1 は両方のコンフィグレーションに含まれています。は VLAN 400、VLAN 500 は test.cfg のみに含まれますが、VLAN 300 は startup.cfg のみに含まれます。

出力の詳細は表 7-1 を参照してください。

関連コマンド

- **display current-configuration**
- **display current-configuration diff**
- **display saved-configuration**

7.1.6 display saved-configuration

🕮 **メモ：**

by-section のパラメータはソフトウェアバージョン 7.2.93a を含む以降のソフトウェアからサポートしています。

Syntax

display saved-configuration [**by-section** { **begin** | **exclude** | **include** } *regular-expression*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

by-section: 装置が次回に起動に使用するために保存されているコンフィグレーションファイルの内容をセクションごとに表示します。各セクションはコマンドビューで構成されており、隣接する 2 つのセクションはシャープ記号（#）で区切られています。このキーワードを指定しない場合、コマンドは実行中の設定を行ごとに表示します。

{ **begin** | **exclude** | **include** }: 実行中の設定を表示するためのルールを指定します。

- **begin**: 指定した正規表現に一致する最初の設定セクションと、それ以降のすべての設定セクションを表示します。
- **exclude**: 指定した正規表現に一致しないすべての設定セクションを表示します。
- **include**: 指定した正規表現に一致するすべての設定セクションを表示します。

regular-expression: 設定セクションをフィルタリングするための正規表現を指定します。1～256 文字の大文字・小文字を区別する文字列です。

説明

display saved-configuration コマンドは装置が次回に起動に使用するために保存されているコンフィグレーションファイルの内容を表示します。

本コマンドは、装置の次回に起動するときに使用できるように重要な設定がコンフィグレーションファイルに保存されているかどうかを確認することができます。

以下の順番でコンフィグレーションファイルを選択します。

1) メインのコンフィグレーションファイルが有効である場合、メインのコンフィグレーションファイルの内容を表示します。
2) バックアップのコンフィグレーションファイルが有効である場合、バックアップのコンフィグレーションファイルの内容を表示します。
3) メインのコンフィグレーションファイルとバックアップのコンフィグレーションファイルが有効でない場合、何も表示されません。

例

次回に起動するコンフィグレーションファイルの内容を表示します。

<AC> display saved-configuration

```
#
 version 7.1.1
#
 sysname AC
#
 undo copyright-info enable
#
 undo info-center logfile enable
#
 undo lldp global enable#
#
vlan 1
```

```
#
  ---- More ----
```

関連コマンド

- **reset saved-configuration**
- **save**

7.1.7 display startup

Syntax

display startup

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display startup コマンドは現在のスタートアップコンフィグレーションファイルと次回に起動するコンフィグレーションファイルの名前を表示します。

例

スタートアップコンフィグレーションファイルの名前を表示します。

<AC> display startup

```
Current startup saved-configuration file: cfa0:/startup.cfg
Next main startup saved-configuration file: cfa0:/startup.cfg
Next backup startup saved-configuration file: NULL
```

表 7-2 コマンド出力

フィールド	説明
Current startup saved-configuration file	装置が起動した際のコンフィグレーションファイルです。
Next main startup saved-configuration file	次回起動する際に使用するメインコンフィグレーションファイルです。
Next backup startup saved-configuration file	次回起動する際に使用するバックアップコンフィグレーションファイルです。

関連コマンド

startup saved-configuration

7.1.8 display this

🕮 **メモ：**

by-section のパラメータはソフトウェアバージョン 7.2.93a を含む以降のソフトウェアからサポートしています。

Syntax

display this [**by-section** { **begin** | **exclude** | **include** } *regular-expression*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

by-section: 現在の view の有効な設定をセクションごとに表示します。各セクションはコマンドビューで構成されており、隣接する 2 つのセクションはシャープ記号（#）で区切られています。このキーワードを指定しない場合、コマンドは実行中の設定を行ごとに表示します。

{ **begin** | **exclude** | **include** }: 実行中の設定を表示するためのルールを指定します。

- **begin**: 指定した正規表現に一致する最初の設定セクションと、それ以降のすべての設定セクションを表示します。
- **exclude**: 指定した正規表現に一致しないすべての設定セクションを表示します。
- **include**: 指定した正規表現に一致するすべての設定セクションを表示します。

regular-expression: 設定セクションをフィルタリングするための正規表現を指定します。1～256 文字の大文字・小文字を区別する文字列です。

説明

display this コマンドは現在の view の有効な設定を表示します。

現在の view で行った設定を確認するために使用します。

このコマンドはデフォルト設定のパラメータは表示されません。

パラメータに関する機能が無効であったとしても、パラメータを設定することができます。これらのパラメータは機能が有効になったのち、表示されます。

すべての line view でこのコマンドを使用すると、すべてのラインインタフェースで有効な設定情報を表示します。

例

system view で有効な設定を表示します。

<AC> system-view

[AC] display this

```
#
 sysname AC
#
 undo copyright-info enable
#
 telnet server enable
#
 password-recovery enable
#
 undo info-center logfile enable
#
 domain default enable system
#
 ip http enable
 ip https enable
#
return
```

7.1.9 reset saved-configuration

Syntax

reset saved-configuration [**backup** | **main**]

View

User view

定義済みユーザロール

network-admin

パラメータ

backup: バックアップの次回の起動時に使用するコンフィグレーションファイルを削除します。

main: メインの次回の起動時に使用するコンフィグレーションファイルを削除します。

説明

reset saved-configuration コマンドは次回の起動時に使用するコンフィグレーションファイルを削除します。

注意:

本コマンドの使用にあたっては注意してください。本コマンドは次回の起動時に使用するコンフィグレーションファイルを削除します。

ソフトウェアバージョンが一致していない、あるいはコンフィグレーションファイルが壊れている場合、次回の起動時に使用するコンフィグレーションファイルを削除します。

メイン、バックアップ、あるいは両方の次回の起動時に使用するコンフィグレーションファイルを削除することができます。

メインとバックアップの次回の起動時に使用するコンフィグレーションファイルを削除するため、**reset saved-configuration backup** コマンドと **reset saved-configuration main** コマンドの両方を実行する必要があります。コマンドの一方を削除することで、ファイルの削除の代わりに指定したファイルの属性を削除することができます。

たとえば、**reset saved-configuration backup** コマンドが実行されるとバックアップの次回の起動時に使用するコンフィグレーションファイルは NULL に設定されます。しかしファイルはメインファイルとして使用されます。ファイルを削除するために、**reset saved-configuration main** コマンドを実行する必要があります。

コンフィグレーションファイルの属性が指定されていない場合、**reset saved-configuration** コマンドはメインの次回の起動時に使用するコンフィグレーションファイルを削除します。

例

メインの次回の起動時に使用するコンフィグレーションファイルを削除します。

<AC> reset saved-configuration

```
The saved configuration file will be erased. Are you sure? [Y/N]:y
Configuration file in cfa0: is being cleared.
Please wait ...........
Configuration file is cleared.
```

関連コマンド

display saved-configuration

7.1.10 restore startup-configuration

Syntax

restore startup-configuration from *ipv4-server src-filename*

View

User view

定義済みユーザロール

network-admin

パラメータ

ipv4-server: IPv4 アドレスあるいはホスト名で TFTP サーバを指定します。ホスト名は大文字小文字を区別しない 1～253 文字の文字列です。大文字、小文字を区別しません。ホスト名で使用できる文字列は文字、数字、ハイフン（-）、アンダーライン（-）、ドット（.）です。

src-filename: 拡張子が“.cfg”の、ダウンロードされたコンフィグレーションファイルのファイル名を指定します。拡張子を除くファイル名は大文字小文字を区別しない 1～255 文字の文字列です。

説明

restore startup-configuration コマンドは指定した TFTP サーバからコンフィグレーションファイルをダウンロードし、次回の起動時に使用するメインのコンフィグレーションファイルとして指定します。

次回の起動時に使用するコンフィグレーションファイルを指定する前に、以下の要件を確認してください。

- サーバへ到達可能であること。
- サーバが TFTP サービスを有効にしています。
- サーバへの読み込み、書き込み許可があります。

本コマンドは、メインの次回の起動時に使用するコンフィグレーションファイルの復旧を自動で行うことで、コンフィグレーションファイルの復旧を簡単に行うことができます。

自動的にフラッシュメモリのルートディレクトリにコンフィグレーションファイルをダウンロードし、主要な次のスタートアップコンフィグレーションファイルとしてファイルを指定します。

例

TFTP サーバ 2.2.2.2 からコンフィグレーションファイル test.cfg をダウンロードし、次回の起動時に使用するコンフィグレーションファイルとして指定します。

<AC> restore startup-configuration from 2.2.2.2 test.cfg

```
Restoring the next startup-configuration file from 2.2.2.2…
```

```
Done.
```

関連コマンド

backup startup-configuration

7.1.11 save

Syntax

save *file-url*

save [**safely**] [**backup** | **main**] [**force**]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

file-url: 動作中のコンフィグレーションを指定されたファイルに“.cfg”拡張子で、ファイルを次回起動時のコンフィグレーションファイルとして指定せずに保存します。“.cfg”拡張子を除き、ファイル名は大文字小文字を区別しない 1～255 文字の文字列で、パス情報を含むことができます。有効な文字は、文字、数字、ハイフン（-）、アンダーライン（-）、ドット（.）です。

safely: safe モードでコンフィグレーションファイルを保存します。このパラメータを指定しない場合、装置は fast モードでコンフィグレーションファイルを保存します。safe モードは fast モードよりも保存に要する時間が遅くなりますが、安全に行うことができます。

backup: 動作中のコンフィグレーションを指定したファイルに保存し、バックアップの次回に起動するコンフィグレーションファイルとして指定します。**backup** パラメータあるいは **main** パラメータを指定しない場合、保存したファイルをメインの次回に起動するコンフィグレーションファイルに指定します。

main: 動作中のコンフィグレーションを指定したファイルに保存し、メインの次回に起動するコンフィグレーションファイルとして指定します。**main** パラメータあるいは **backup** パラメータを指定しない場合、保存したファイルをメインの次回に起動するコンフィグレーションファイルに指定します。

force: 動作中のコンフィグレーションを、確認の表示を行わずに保存します。本パラメータを指定しない場合、操作を実行する際に確認メッセージが表示されます。30 秒以内に操作を行わない場合、システムは自動で操作を中止します。30 秒以内に“Y”を入力すると、保存処理を継続し、処理中のターゲットファイル名を変更することができます。

説明

save *file-url* [**all**]コマンドは動作中のコンフィグレーションをコンフィグレーションファイルに保存します。次回に起動するコンフィグレーションファイルとして指定しません。

save [**safely**] [**backup** | **main**] [**force**]コマンドは記憶媒体のルートディレクトリのファイルに動作中のコンフィグレーションを保存します。本コマンドは次回に起動するコンフィグレーションファイルとして自動的に指定します。

本コマンドで指定されたファイルが存在しない場合、設定を保存する前、システムはファイルを作成します。すでにファイルが存在する場合、システムはファイルを上書きするかどうか確認メッセージを表示します。ファイルを上書きしない場合、システムは**save** コマンドの操作を中止します。

コマンドの *file-url* パラメータを指定しない場合、コマンドはテキストファイル“.cfg”と、バイナリファイル“.mdb”に動作中のコンフィグレーションを保存します。2 つのファイルは同一ファイル名です。バイナリファイル“.mdb”はテキストファイル“.cfg”よりも保存に要する時間が短くなります。

safe モードでは、システムは一時ファイルに設定を保存し、保存が完了した後、ターゲットの次回の起動に使用するコンフィグレーションファイルの上書きを開始します。動作に、再起動、電源の故障あるいはメモリ容量の不足が発生した場合、次回の起動に使用するコンフィグレーションファイルは保持されています。

fast モードでは、装置は直接ターゲットの次回の起動に使用するコンフィグレーションファイルを上書きします。動作中に、再起動、電源の故障あるいはメモリ容量の不足が発生した場合、次回の起動に使用するコンフィグレーションファイルが消失します。

例

動作中のコンフィグレーションをコンフィグレーションファイル backup.cfg に保存し、次回に起動するコンフィグレーションファイルとして指定しません。

<AC> save backup.cfg

```
The current configuration will be saved to cfa0:/backup.cfg. Continue? [Y/N]:y
Now saving current configuration to the device.
Saving configuration
cfa0:/backup.cfg. Please wait...
Configuration is saved to successfully.
```

動作中のコンフィグレーションをメインの次回の起動に使用するコンフィグレーションファイルに、確認の表示を行わずに保存します。

<AC> save force

```
Validating file. Please wait....
Saved the current configuration to mainboard device successfully.
```

動作中のコンフィグレーションを記憶媒体のルートディレクトリのファイルに保存し、メインの次回の起動に使用するコンフィグレーションファイルとして指定します。

<AC> save

```
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[ cfa0:/backup.cfg]
(To leave the existing filename unchanged, press the enter key):test.cfg
 Validating file. Please wait.....
 Configuration is saved to device successfully.
```

関連コマンド

- **display current-configuration**
- **display saved-configuration**

7.1.12 startup saved-configuration

Syntax

startup saved-configuration *cfgfile* [**backup** | **main**]

undo startup saved-configuration

デフォルト

次回の起動に使用するコンフィグレーションファイルは指定されていません。

View

User view

定義済みユーザロール

network-admin

パラメータ

cfgfile: “.cfg”拡張子をつけてコンフィグレーションファイル名を指定します。“.cfg”拡張子を除き、ファイル名は大文字小文字を区別しない 1～255 文字の文字列で、パス情報を含むことができます。有効な文字は、文字、数字、ハイフン(-)、アンダーライン(-)、ドット（.）です。ファイルパスがディレクトリ名を含む場合は、ディレクトリが既に存在している必要があります。

backup: コンフィグレーションファイルをバックアップの次回の起動に使用するコンフィグレーションファイルとして指定します。

main: コンフィグレーションファイルをメインの次回の起動に使用するコンフィグレーションファイルとして指定します。これは、装置が起動時に読み込みを行うメインのコンフィグレーションファイルです。読み込みに失敗した場合、装置はバックアップの次回の起動に使用するコンフィグレーションファイルの読み込みを行います。

説明

startup saved-configuration コマンドはファイルを次回の起動に使用するコンフィグレーションファイルとして指定します。

undo startup saved-configuration コマンドは次回の起動時に工場出荷状態で起動します。

backup パラメータあるいは **main** パラメータの両方とも指定されていない場合、**startup saved-configuration** コマンドはメインの次回の起動に使用するコンフィグレーションファイルとして指定します。

メインとバックアップのコンフィグレーションファイルを同一にすることができますが、高可用性のために、別々のファイル名としてファイルを指定することを推奨します。

undo startup saved-configuration コマンドはメインとバックアップの次回の起動に使用するコンフィグレーションファイルの属性を NULL に変更しますが、コンフィグレーションファイルを削除しません。

save コマンドで動作中のコンフィグレーションを保存したとき、次回の起動に使用するコンフィグレーションファイルとして設定することができます。

例

メインの次回の起動に使用するコンフィグレーションファイルを指定します。

<AC> startup saved-configuration testcfg.cfg

```
Please wait ....
... Done!
```

関連コマンド

display startup

目次

このセクションのページは **1-x-x** です。

8 章 ソフトウェアのアップグレード 8-1
8.1 ソフトウェアのアップグレード設定コマンド 8-1
8.1.1 boot-loader file 8-1
8.1.2 bootrom update 8-3
8.1.3 display boot-loader 8-4

8章 ソフトウェアのアップグレード

8.1 ソフトウェアのアップグレード設定コマンド

8.1.1 boot-loader file

⚠ **重要**：

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアにアップグレードする場合、“**boot-loader file** *ipe-filename*”コマンドにてイメージパッケージファイル.ipe のファイルパスを指定してください。“**boot-loader file boot** *boot-package* **system** *system-package*”コマンドでBootイメージファイル.binのファイルパスを指定した場合、アップグレード後に接続した AP にソフトウェアを自動配布できなくなります。

Syntax

boot-loader file boot *boot-package* **system** *system-package* { **all** | **slot** *slot-number* } **{ backup | main }**

boot-loader file *ipe-filename* { **all** | **slot** *slot-number* } { **backup** | **main** }

View

User view

定義済みユーザロール

network-admin

パラメータ

boot *boot-package*: Boot イメージファイル.bin のファイルパスを指定します。大文字、小文字を区別しません。ファイルはシステムの記憶媒体のルートディレクトリに格納されます。ファイルパスの記憶媒体:/ファイル名.bin セグメントの設定範囲は 1～63 文字です。ファイルパスの指定の詳細はオペレーションマニュアルのセクション 1 の*はじめに*“*ファイルシステム管理*”を参照してください。

system *filename*: System イメージファイル.bin のファイルパスを指定します。大文字、小文字を区別しません。ファイルはシステムの記憶媒体のルートディレクトリに格納されます。ファイルパスの記憶媒体:/ファイル名.bin セグメントの設定範囲は 1～63 文字です。ファイルパスの指定の詳細はオペレーションマニュアルのセクション 1 の*はじめに*“*ファイルシステム管理*”を参照してください。

ipe-filename: イメージパッケージファイル.ipe のファイルパスを指定します。大文字、小文字を区別しません。ファイルはシステムの記憶媒体のルートディレクトリに格納されます。ファイルパスの記憶媒体:/ファイル名.ipe セグメントの設定範囲は 1～63 文字です。ファイルパスの指定の詳細はオペレーションマニュアルのセクション 1 の*はじめに*“*ファイルシステム管理*”を参照してください。

all: IRF スタックユニットのすべてのメンバ装置に対してスタートアップイメージを指定します。このパラメータを指定した場合、IRF スタックユニットのすべてのメンバ装置をアップグレードします。

slot *slot-number*: IRF スタックユニットのメンバ装置の IRF メンバ ID を指定します。

backup: バックアップの次回の起動に使用するファイルを指定します。バックアップの次回の起動に使用するイメージファイルはメインの次回の起動に使用するイメージファイルが有効でないときのみ使用されます。

main: メインの次回の起動に使用するファイルを指定します。装置は起動時には常にメインの次回の起動に使用するファイルで起動を行います。

説明

boot-loader file コマンドは次回の起動に使用するソフトウェアイメージファイルを指定します。

コンフィグレーション失敗を避けるために、他のユーザが装置の設定や管理をしていないかどうか確認してください。

次回の起動に使用するソフトウェアイメージファイルを読み込む場合、システムの再起動が必要です。

次回の起動に使用するソフトウェアイメージファイルを指定する前に、アップグレードファイルをファイルシステムのルートディレクトリに保存してください。

boot-loader file コマンドはすべての次回の起動に使用するソフトウェアイメージリストを上書きします。

例

cfa0:/all.ipe をメイン起動イメージファイルとして指定します。

<AC> boot-loader file cfa0:/all.ipe slot 1 main

```
Verifying the IPE file and the images.....Done.
QX-W2230 images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:Y
Add images to the device.
File cfa0:/boot.bin already exists on the device.
File cfa0:/system.bin already exists on the device.
Overwrite the existing files? [Y/N]:Y
Decompressing file boot.bin to cfa0:/boot.bin.....Done.
```

```
Decompressing file system.bin to
cfa0:/system.bin.............................Done.
The images that have passed all examinations will be used as the main startup
software images at the next reboot on the device.
```

cfa0:/boot.bin と cfa0:/system.bin をメイン起動ブートイメージとシステムイメージファイルとして指定します。

<AC> boot-loader file boot cfa0:/boot.bin system cfa0:/system.bin slot 1 main

```
This command will set the main startup software images. Continue? [Y/N]:y
The images that have passed all examinations will be used as the main startup
software images at the next reboot on the device.
```

関連コマンド

display boot-loader

8.1.2 bootrom update

Syntax

bootrom update file *file-url*

View

User view

定義済みユーザロール

network-admin

パラメータ

file *file-url*: フラッシュの Boot ROM イメージが含まれるファイルを指定します。設定範囲は 1～63 です。

説明

bootrom update コマンドはフラッシュの Boot ROM イメージを、Boot ROM の通常エリアに読み込みます。

ソフトウェアアップグレードを行う際、Boot ROM イメージのアップグレードが必要な場合、Comware イメージ（Boot イメージと System ソフトウェアイメージ）をアップグレードする前に、このコマンドを使用して Boot ROM に新しい Boot ROM イメージをアップグレードします。このコマンドは、予期しない電気的な故障によってアップグレードの失敗が発生するリスクを減少させ、アップグレードを行う時間を削減することができます。

アップグレードを完了させるために、装置を再起動します。

領域を節約するために、Boot ROM イメージのアップグレードを完了した後に、ファイルシステム内の Boot ROM イメージを削除することができます。

例

Boot ROM イメージをアップグレードするために、ファイル a.bin を使用します。

<AC> bootrom update file a.bin

```
  This command will update the Boot ROM file on the specified board(s), Continue?
[Y/N]:y
  Now updating the Boot ROM, please wait.............Done.
```

関連コマンド

boot-loader file

8.1.3 display boot-loader

Syntax

display boot-loader

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display boot-loader コマンドは現在のソフトウェアイメージと次回の起動に使用するソフトウェアイメージを表示します。

例

現在のソフトウェアイメージとスタートアップソフトウェアイメージを表示します。

<AC> display boot-loader

```
Software images on the device:
Current software images:
  cfa0:/boot.bin
  cfa0:/system.bin
Main startup software images:
  cfa0:/boot.bin
  cfa0:/system.bin
Backup startup software images:
  cfa0:/boot.bin
```

```
cfa0:/system.bin
```

表 8-1 コマンド出力

フィールド	説明
Current software images	Comwareイメージが読み込まれました。
Main startup software images	次回の起動に使用するメインのComwareイメージです。
Backup startup software images	次回の起動に使用するバックアップのComwareイメージです。

関連コマンド

boot-loader file

目次

このセクションのページは **1-x-x** です。

9 章 装置管理 9-1
9.1 装置管理コマンド 9-1
9.1.1 clock datetime 9-1
9.1.2 clock protocol 9-2
9.1.3 clock summer-time 9-3
9.1.4 clock timezone 9-5
9.1.5 command 9-6
9.1.6 copyright-info enable 9-7
9.1.7 diag boot-info display 9-8
9.1.8 display clock 9-11
9.1.9 display cpu-usage 9-12
9.1.10 display cpu-usage history 9-13
9.1.11 display device 9-16
9.1.12 display device manuinfo 9-17
9.1.13 display diagnostic-information 9-18
9.1.14 display environment 9-20
9.1.15 display maintain cpu-usage history process 9-21
9.1.16 display memory 9-22
9.1.17 display memory-threshold 9-23
9.1.18 display scheduler job 9-25
9.1.19 display scheduler logfile 9-26
9.1.20 display scheduler reboot 9-27
9.1.21 display scheduler schedule 9-27
9.1.22 display transceiver alarm 9-29
9.1.23 display transceiver diagnosis 9-30
9.1.24 display transceiver interface 9-31
9.1.25 display transceiver manuinfo 9-33
9.1.26 display version 9-34
9.1.27 header 9-34
9.1.28 job 9-36
9.1.29 locator blink 9-37
9.1.30 memory-threshold 9-38
9.1.31 monitor cpu-usage enable 9-39
9.1.32 monitor cpu-usage interval 9-40
9.1.33 monitor cpu-usage threshold 9-41
9.1.34 password-recovery enable 9-42

9.1.35 reboot 9-43
9.1.36 reset scheduler logfile 9-44
9.1.37 restore factory-default 9-45
9.1.38 scheduler job 9-46
9.1.39 scheduler logfile size 9-47
9.1.40 scheduler reboot at 9-47
9.1.41 scheduler reboot delay 9-49
9.1.42 scheduler schedule 9-50
9.1.43 shutdown-interval 9-51
9.1.44 sysname 9-52
9.1.45 temperature-limit 9-53
9.1.46 time at 9-54
9.1.47 time once 9-55
9.1.48 time repeating 9-57
9.1.49 user-role 9-59

9章 装置管理

9.1 装置管理コマンド

9.1.1 clock datetime

Syntax

clock datetime *time date*

View

User view

定義済みユーザロール

network-admin

パラメータ

time: 設定時刻（形式は *hh:mm:ss* （時/分/秒））を指定します。*hh* の設定範囲は 0～23 です。*mm* の設定範囲は 0～59 です。*ss* の設定範囲は 0～59 です。*hh, mm, ss* において最初の 0 は省略可能です。*ss* が 00 の場合 *hh:mm* で表し、*mm* と *ss* が 00 の場合 *hh* で示します。たとえば 08:00:00 を指定する場合、*hh* に 8 を設定できます。

date: 現在の日付（形式は *MM/DD/YYYY* あるいは *YYYY/MM/DD*）を指定します。*MM* は 1～12 の月、*DD* は各月の日付、*YYYY* は 2000～2035 の年です。

説明

clock datetime コマンドは装置の現在の日時を設定します。

正しいシステムクロックの設定はネットワーク管理と通信に不可欠です。ネットワークで装置を動作させる前に、装置のシステム時間を設定してください。

装置を、ローカルシステム時間または NTP 時間ソースを使用するように設定可能です。

装置がローカルシステム時間を使用する場合、装置のシステム時間は以下の要素に依存します。

- ローカルタイムゾーン
- UTC 時間
- サマータイム

システム時間を確認するには、**display clock** コマンドを使用します。

例

装置の現在の日時をローカルシステム時間で 08:08:08 01/01/2017 に設定します。

<AC> clock datetime 8:8:8 1/1/2017

装置の現在の日時をローカルシステム時間で 08:10:00 01/01/2017 に設定します。

<AC> clock datetime 8:10 2017/1/1

関連コマンド

- **clock protocol**
- **clock summer-time**
- **clock timezone**
- **display clock**

9.1.2 clock protocol

Syntax

clock protocol { **none** | **ntp** }

undo clock protocol

デフォルト

NTP

View

System view

定義済みユーザロール

network-admin

パラメータ

none:ローカルシステム時間です。

ntp: UTC 時間を含む NTP です。正しい NTP を設定してください。NTP の詳細はオペレーションマニュアルのセクション 11 *システム管理　"NTP"* を参照してください。

説明

clock protocol コマンドはシステムクロックソースを指定します。

undo clock protocol コマンドはデフォルトに戻します。

正しいシステム時間はネットワーク管理やネットワーク通信に必須です。ネットワーク装置を動作させる前に、システム時間を設定します。装置はローカルに設定されたシステム時間を使うか、UTC 時間をネットワークの上の時間ソースから得て、システム時間を計算することができます。

- **clock protocol none** コマンドを使用する場合、装置はローカルシステム時間を設定します。装置はその時、システム時間を維持するためにその内蔵の水晶発振器によって生成されたクロック信号を使います。

- **clock protocol ntp** コマンドを使用する場合、装置は NTP によって UTC 時間を得て、システム時間を計算します。装置は周期に UTC 時間を同期させて、システム時間を再計算します。

NTP 時間ソースから UTC 時間を使って計算されたシステム時間はより精密です。

コマンドを複数回実行した場合、最新の設定が有効になります。

例

ローカルシステム時間を使用するように設定します。

<AC> system-view

[AC] clock protocol none

9.1.3 clock summer-time

Syntax

clock summer-time *name start-time start-date end-time end-date add-time*

undo clock summer-time

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

name: サマータイム名を指定します。設定範囲は大文字小文字を区別する 1～32 文字です。

start-time: 開始時刻を指定します。形式は *hh:mm:ss* （時/分/秒）です。*hh* の設定範囲は 0～23 です。mm の設定範囲は 0～59 です。ss の設定範囲は 0～59 です。*hh, mm, ss* において最初の 0 は省略可能です。*ss* が 00 の場合 *hh:mm* で表し、*mm* と *ss* が 00 の場合 *hh* で示します。たとえば 08:00:00 を指定する場合、*hh* に 8 を設定できます。

start-date: 開始日を以下の形式の 1 つで指定します。

- *MM*/*DD*：*MM* の設定範囲は 1～12 です。*DD* の設定範囲は月によって変わります。
- *month week date*
  - **month**−月を指定します。January、February、March、April、May、June、July、August、September、October、November、December が指定できます。
  - **week**−月で開始する週を指定します。first、second、third、fourth、fifth、last が指定できます。

- **day**−日を指定します。Sunday、Monday、Tuesday、Wednesday、Thursday、Friday、Saturday が指定できます。

end-time: 終了時刻を指定します。形式は *hh:mm:ss* （時/分/秒）です。*hh* の設定範囲は 0～23 です。mm の設定範囲は 0～59 です。ss の設定範囲は 0～59 です。*hh, mm, ss* において最初の 0 は省略可能です。*ss* が 00 の場合 *hh:mm* で表し、*mm* と *ss* が 00 の場合 *hh* で示します。たとえば 08:00:00 を指定する場合、*hh* に 8 を設定できます。

end-date: 終了日を以下の形式の 1 つで指定します。

- *MM*/*DD* : *MM* の設定範囲は 1～12 です。*DD* の設定範囲は月によって変わります。
- *month week date*
  - **month**−月を指定します。January、February、March、April、May、June、July、August、September、October、November、December が指定できます。
  - **week**−月で開始する週を指定します。first、second、third、fourth、fifth、last が指定できます。
  - **day**−日を指定します。Sunday、Monday、Tuesday、Wednesday、Thursday、Friday、Saturday が指定できます。

add-time: 標準時刻に追加する時間です。形式は *hh:mm:ss* （時/分/秒）です。*hh* の設定範囲は 0～23 です。mm の設定範囲は 0～59 です。ss の設定範囲は 0～59 です。*hh, mm, ss* において最初の 0 は省略可能です。*ss* が 00 の場合 *hh:mm* で表し、*mm* と *ss* が 00 の場合 *hh* で示します。たとえば 08:00:00 を指定する場合、*hh* に 8 を設定できます。

説明

clock summer-time コマンドは指定した期間サマータイムを使用します。

undo clock summer-time コマンドは設定を削除します。

正しいシステムクロックの設定はネットワーク管理と通信に不可欠です。ネットワークで装置を動作させる前に、装置のシステム時間を設定してください。

装置を、ローカルシステム時間または NTP 時間ソースを使用するように設定可能です。

装置がローカルシステム時間を使用する場合、装置のシステム時間は以下の要素に依存します。

- ローカルタイムゾーン
- UTC 時間

システム時間を確認するには、**display clock** コマンドを使用します。

例

08/01 の 06:00:00 から 09/01 の 06:00:00 の間、システムの時間を 1 時間進めます。

<AC> system-view

[AC] clock summer-time PDT 6 08/01 6 09/01 1

関連コマンド

- **clock datetime**
- **clock timezone**

- **display clock**

9.1.4 clock timezone

Syntax

clock timezone *zone-name* { **add** | **minus** } *zone-offset*

undo clock timezone

デフォルト

UTC 時間

View

System view

定義済みユーザロール

network-admin

パラメータ

zone-name: タイムゾーン名を名前で指定します。大文字小文字を区別する 1～32 文字の文字列です。

add: UTC 時間（協定世界時 : universal time coordinated）に対する正（+）のオフセットです。

minus: UTC 時間に対する負（-）のオフセットです。

zone-offset: UTC 時間に対するオフセットです。形式は *hh:mm:ss* （時/分/秒）です。*hh* の設定範囲は 0～23 です。mm の設定範囲は 0～59 です。ss の設定範囲は 0～59 です。*hh, mm, ss* において最初の 0 は省略可能です。*ss* が 00 の場合 *hh:mm* で表し、*mm* と *ss* が 00 の場合 *hh* で示します。たとえば 08:00:00 を指定する場合、*hh* に 8 を設定できます。

説明

clock timezone コマンドはタイムゾーンを設定します。

undo clock timezone コマンドはデフォルトに戻します。

正しいシステムクロックの設定はネットワーク管理と通信に不可欠です。ネットワークで装置を動作させる前に、装置のシステム時間を設定してください。

装置を、ローカルシステム時間または NTP 時間ソースを使用するように設定可能です。

装置がローカルシステム時間を使用する場合、装置のシステム時間は以下の要素に依存します。

- ローカルタイムゾーン
- UTC 時間

システム時間を確認するには、**display clock** コマンドを使用します。

例

UTC より 5 時間進めたタイムゾーン名を Z5 に設定します。

<AC> system-view

[AC] clock timezone Z5 add 5

関連コマンド

- **clock datetime**
- **clock summer-time**
- **display clock**

9.1.5 command

Syntax

command *id command*

undo command *id*

デフォルト

設定なし

View

Job view

定義済みユーザロール

network-admin

パラメータ

id: コマンドの ID を指定します。設定範囲は 0～4294967295 です。コマンドの ID は job を一意に識別します。job のコマンドは昇順で実行されます。

command: job に割り当てられたコマンドを指定します。

説明

command コマンドはジョブにコマンドを割り当てます。

undo command コマンドはコマンドを取り消します。

コマンド（コマンド A）を job に割り当てるため、コマンド A の view に移行するコマンドを job に割り当ててください。

スケジュールのすべてのコマンドがコマンド構文に合致していることを確認してください。コマンドをジョブに割り当てる際、システムは構文を検査しません。

telnet コマンド、ftp コマンド、ssh2 コマンド、monitor process コマンドはスケジュール自動実行することはできません。

スケジュール自動実行機能はユーザがインタラクティブにコマンドの操作を扱うことができません。もしコマンドが”YES”あるいは”NO”の答えを要求する場合、システムはいつも”Y”あるいは”YES”が入力されます。もし文字列の入力が必要な場合、システムは自動的にデフォルト文字列を入力するか、デフォルト文字列がない場合、空の文字列を入力します。

コマンドが既存のコマンドの ID を使用する場合、既存のコマンドは置き換えられます。

例

job 名が **backupconfig** の job に、コンフィグレーションファイル **startup.cfg** を TFTP サーバ 192.168.100.11 にバックアップを行うコマンドを割り当てます。

<AC> system-view

[AC] scheduler job backupconfig

[AC-job-backupconfig] command 2 tftp 192.168.100.11 put cfa0:/startup.cfg backup.cfg

job 名が **shutdownGE** の job に GigabitEthernet 1/0/1 をシャットダウンするコマンドを割り当てます。

<AC> system-view

[AC] scheduler job shutdownGE

[AC-job-shutdownGE] command 1 system-view

[AC-job-shutdownGE] command 2 interface gigabitethernet 1/0/1

[AC-job-shutdownGE] command 3 shutdown

関連コマンド

scheduler job

9.1.6 copyright-info enable

Syntax

copyright-info enable

undo copyright-info enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

copyright-info enable コマンドは著作権情報の表示を有効にします。

undo copyright-info enable コマンドは著作権情報の表示を無効にします。

例

著作権情報の表示を有効にします。

<AC> system-view

[AC] copyright-info enable

9.1.7 diag boot-info display

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.49 を含む以降のソフトウェアからサポートしています。

Syntax

diag boot-info display

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

diag boot-info display コマンドは装置の再起動履歴を表示します。

AC の再起動履歴は、直近で最大 10 件まで表示されます。

例

AC の再起動履歴を表示します。

<AC> diag boot-info display

```
******************************************************************************
PowerOn BootTimes   : 136
```

```
Watchdog BootTimes  : 0
Software BootTimes  : 188
Hardware BootTimes  : 2
MotherBoard BootTimes: 0
Backup BootTimes    : 3
SlotOut BootTimes   : 0
Current Boot Type   : Software-boot
Current Running Time: 280080(s)
Running Time        : 451(d)8(h)
*** Boot History(Startup Time and Reason) ***
2021-12-07 11:29:18 User soft reboot
2021-11-13 09:04:07 User soft reboot
2021-09-27 06:35:11 User soft reboot
2021-09-23 08:35:49 User soft reboot
2021-09-10 11:33:12 Power on
2021-09-10 11:25:43 Power on
2021-09-05 08:33:10 Power on
2021-09-01 09:30:16 User soft reboot
2021-08-24 10:36:21 User soft reboot
2021-08-24 10:34:33 User soft reboot
```

表 9-1 コマンド出力

フィールド	説明
PowerOn BootTimes	Power onが原因で再起動した合計回数です。
Watchdog BootTimes	Watchdog rebootが原因で再起動した合計回数です。
Software BootTimes	soft rebootが原因で再起動した合計回数です。
Hardware BootTimes	Hard rebootが原因で再起動した合計回数です。
MotherBoard BootTimes	Master slotの合計再起動回数です。
Backup BootTimes	Standby slotの合計再起動回数です。
SlotOut BootTimes	Stanby slotが外れた合計回数です。
Current Boot Type	現在のBootタイプ。 • Unknown • Poweron-boot • Software-boot • Watchdog-boot • Hardware-boot • MotherBoard-boot • ExtendWatchdog-boot • Backup-boot • ExtendedModuleRemoved-boot

フィールド	説明
Current Running Time	直近のBootの動作時間です。
Running Time	合計の動作時間です。
Boot History	下記が表示されます。 原因： ● Power on ● Hard reboot ● Watchdog reboot ● User soft reboot ● Kernel exception soft reboot ● Kernel deadloop soft reboot ● DevHandShake soft reboot ● Lic overTime soft reboot ● Slave switch soft reboot ● IRF mergesoft reboot ● Auto update soft reboot ● Memory-exhausted reboot ● -Crypto self-test failed reboot サブカテゴリ： ● Reset by admin ● Image was downloaded successfully ● Stayed in idle state for a long time ● WTU reboot because of offline WT ● AP reset from Cloud ● Anomaly detected ● Inconsistent BSS states on AC and AP ● Inconsistent BSS states on AP and in drive ● Inconsistent radio states on AC and AP ● Inconsistent radio modes on AC and AP ● Inconsistent radio rates on AC and AP ● Inconsistent radio channels on AC and AP ● Inconsistent radio bandwidth on AC and AP ● Inconsistent radio interface states on AC and AP ● Inconsistent radio states on AP and in drive ● Inconsistent radio modes on AP and in drive ● Inconsistent radio channels on AP and in drive ● Inconsistent radio bandwidth on AP and in drive

フィールド	説明
	• Anchor AC detected another anchor AC with smaller MAC address and switched its role to AP • Anchor AC received a discovery response and switched its role to AP • Anchor AP failed to detect other anchor ACs or ACs and switched its role to AC • Anchor AC detected another anchor AC with higher priority and switched its role to AP • Configure the anchor device as an AC • Configure the anchor device as an AP • Manually configure the AP to act as a fit AP • Manually configure the AP to act as a fat AP • Manually configure the inside AP to act as a fat AP • Local AC image download • Device role changed from common to local • Device role changed from local to common • Device role changed from common to central • Device role changed from central to common • WT version changed • Cannot process subslot insert event • Cannot send subslot insert event to next step for processing

9.1.8 display clock

Syntax

display clock

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

システムの現在時刻、日付、タイムゾーン、サマータイムを表示するには、display clock コマンドを使用します。

例

ローカルタイムゾーンが指定されていないとき、システム時間を表示します。

<AC> display clock

```
10:09:00 UTC Fri 02/16/2017
```

ローカルタイムゾーン Z5 が指定されているとき、システム時間を表示します。

<AC> display clock

```
15:10:00 Z5 Fri 02/16/2017
Time Zone : Z5 add 05:00:00
```

ローカルタイムゾーン Z5 が指定され、PDT サマータイムが指定されているとき、システム時間を表示します。

<AC> display clock

```
15:11:00 Z5 Fri 02/16/2017
Time Zone : Z5 add 05:00:00
Summer Time : PDT 06:00:00 08/01 06:00:00 09/01 01:00:00
```

関連コマンド

- **clock datetime**
- **clock timezone**
- **clock summer-time**

9.1.9 display cpu-usage

Syntax

display cpu-usage

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display cpu-usage コマンドは CPU 使用率の統計情報を表示します。

起動後、装置は平均 CPU 使用率を以下の間隔で記録します。

- 5 秒
- 1 分
- 5 分

本コマンドは、最新の 5 秒間、1 分間、5 分間の CPU 使用率の平均値を表示します。

例

現在の CPU 使用率の統計情報をテキスト形式で表示します。

<AC> display cpu-usage

```
Unit CPU usage:
      1% in last 5 seconds
      1% in last 1 minute
      1% in last 5 minutes
```

表 9-2 コマンド出力

フィールド	説明
Unit CPU usage	CPU使用率統計情報
x% in last 5 seconds Last 5 sec	最後の5秒のCPU使用率の平均です。
y% in last 1 minute Last 1 min	最後の1分のCPU使用率の平均です。
z% in last 5 minutes Last 5 min	最後の5分のCPU使用率の平均です。

9.1.10 display cpu-usage history

Syntax

display cpu-usage history [**job** *job-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

job *job-id*: job の ID のプロセスを指定します。指定しない場合、すべてのプロセスのシステム全体の CPU 使用率履歴の統計情報を表示します。

説明

display cpu-usage history コマンドは CPU 使用率履歴の統計情報を表示します。

CPU 使用率のモニタリングが有効にされたのち、システムはある時間での CPU 使用率統計情報を取得し、履歴記録領域に統計結果を保存します。このコマンドは最後の 60 分間の CPU 使用率の統計情報レコードを座標で表示します。

Y 座標は、CPU 使用率を示します。もし統計情報が使用率のステップの倍数でない場合、もっとも近いステップに切り下げあるいは切り上げされます。たとえば CPU 使用率のステップが 5%である場合、統計情報が 53%である場合 55%に切り上げされます。統計情報が 52%である場合、50%に切り下げられます。

X 座標は時間を示します。

シャープ（#）は、ある時点における CPU 使用率を示します。ある時点上で#マークが 1 つ以上あるとき、一番高い位置の#マークが、現時点での CPU 使用率です。

例

CPU 使用率履歴の統計情報を表示します。

<AC> display cpu-usage history

```
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|           #
 10%|          ###  #
  5%|         ########
    ------------------------------------------------------------
            10        20        30        40        50        60  (minutes)
                  cpu-usage last 60 minutes (SYSTEM)
```

出力は以下のアイテムを示します。

- プロセス名：**SYSTEM**（全システムを示します。）
- 最新の 60 分間の CPU 使用率
  - 12 分前：5%

- 13 分前：10%
- 14 分前：15%
- 15 分前：10%
- 16 分前：5%
- 17 分前：5%
- 18 分前：10%
- 19 分前：5%
- その他の時間：2%または 2%未満

プロセス 1 の CPU 使用率履歴の統計情報を表示します。

<AC> display cpu-usage history job 1

```
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|
 10%|
  5%|                #
    ------------------------------------------------------------
            10       20       30       40       50       60  (minutes)
                   cpu-usage last 60 minutes (STSTEM)
```

出力は以下のアイテムを示します。

- プロセス名：**SYSTEM**（[ ]内のプロセス名はカーネルプロセスを示します）
- 最新の 60 分間の CPU 使用率
  - 20 分前：5%
  - その他の時間：2%または 2%未満

関連コマンド

- **monitor cpu-usage enable**
- **monitor cpu-usage interval**

9.1.11 display device

Syntax

display device [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose: 詳細ハードウェア情報を表示します。本キーワードを指定しない場合、概要情報を表示します。

説明

display device コマンドは装置情報を表示します。

例

装置情報を表示します。

<AC> display device

```
Slot No.  Subslot No. Board Type       Status    Max Ports
1         0          QX-W2230AC      Normal      6
```

表 9-3 コマンド出力

フィールド	説明
Slot No.	スロット番号（1固定）
Subslot No.	サブカードのサブスロット番号（0固定）
Board Type	ハードウェアタイプ
Status	ハードウェア状態： ● Normal—ハードウェアは正常に動作 ● Fault—ハードウェアは正常に動作していない
Max Ports	サポートされる最大ポート数

9.1.12 display device manuinfo

Syntax

display device manuinfo

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display device manuinfo コマンドは装置の電子ラベル情報を表示します。

電子ラベル情報とは、装置またはカードのプロファイルです。シリアル番号、製造年月日、MAC アドレス、ベンダ名といった固定的な設定情報を含んでいます。データはデバッグまたはテスト中に記憶媒体に書き込まれます。

例

装置の電子ラベル情報を表示します。

<AC> display device manuinfo

```
DEVICE_NAME:QX-W2230AC
DEVICE_SERIAL_NUMBER:210235A1JMC166000028
MAC_ADDRESS:84D9-3110-9FD8
MANUFACTURING_DATE:2016-06-04
VENDOR_NAME:NEC
```

表 9-4 コマンド出力

フィールド	説明
DEVICE_NAME	装置名
DEVICE_SERIAL_NUMBER	シリアル番号
MAC_ADDRESS	MACアドレス
MANUFACTURING_DATE	製造年月日
VENDOR_NAME	ベンダ名

9.1.13 display diagnostic-information

Syntax

display diagnostic-information [**hardware** | **infrastructure** | **l2** | **l3** | **service**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

hardware: ハードウェアに関する稼働状態の診断情報を表示します。

infrastructure: 基本機能に関する稼働状態の診断情報を表示します。

l2: レイヤ 2 機能に関する稼働状態の診断情報を表示します。

l3: レイヤ 3 機能に関する稼働状態の診断情報を表示します。

service: 上位レイヤ機能に関する稼働状態の診断情報を表示します。

説明

display diagnostic-information コマンドはデバイス診断情報を表示または保存します。

診断とトラブルシューティングにあたり、稼働統計情報を収集するために以下の方法のうち 1 つを使用します。

- 機能ごと、またはモジュールごとの稼働情報を収集するため、個別の display コマンドを使用します。
- 複数またはすべての機能とハードウェアのモジュールの稼働情報を収集するため、**display diagnostic-information** コマンドを使用します。

ストレージスペースを節約するために、情報をファイルに保存する前に、このコマンドは自動的に情報を圧縮します。ファイル内容を見るには:

1) ファイルを解凍するために、**tar extract** コマンドを使用します。
2) 解凍されたファイルを解凍するために、**gunzip** コマンドを使用します。
3) 解凍されたファイルを見るために、**more** コマンドを使用します。

コマンドのためにファイル名を指定しない場合、システムは、情報を表示するか保存するかを決めるように促します。情報の保存を選択した場合、システムは自動的にファイル名を割り当てて、ブラケットの中でファイル名を表示します。ファイル名は独自性であるために、ファイル名は装置名と現在のシステム時間を含みます。装置名が以下の特殊文字のいずれかを含んでいる場合、システムは各特殊文字を下線(_)に変換します：スラッシュ(/)、バックスラッシュ(¥)、コロン(：)、アスタリスク(*)、より大きい(>)、パイプ(|)、より少ない(<)、疑問符(？)、引用符(")。

例えば、装置名が **A/B**、ファイル名が **A_B** であるならば、**cfa0:/diag_A_B_20170101-000438.tar.gz** となります。

display diagnostic-information コマンドは **|**、**>**、**>>**、のオプションをサポートしません。

どの機能パラメータも指定しなかった場合、本コマンドはすべての機能とモジュールの動作情報を表示または保存します。

例

装置の診断情報を表示します。

<AC> display diagnostic-information

```
Save or display diagnostic information (Y=save, N=display)? [Y/N]:n
================================================
  ===============display clock===============
14:03:55 UTC Thu 01/05/2017
================================================
  ===============display version===============
...
```

システム内のすべての機能モジュールの稼働状態を保存します。

<AC> display diagnostic-information

```
Save or display diagnostic information (Y=save, N=display)? [Y/N]:y
Please input the file name(*.tar.gz)[ cfa0:/diag_QX-W2230AC_20171123-172616.ta
r.gz]:
Diagnostic information is outputting to cfa0:/diag_QX-W2230AC_20171123-172616.t
ar.gz.
Please wait...
Save successfully
```

ファイル名を入力後、**Enter** を押してください。

ファイル **test.tar.gz** に装置診断情報を保存します。

```
<AC> display diagnostic-information test.tar.gz
Diagnostic information is outputting to cfa0:/test.tar.gz.
Please wait...
Save successfully.
```

関連コマンド

- **gunzip**
- **more**
- **tar extract**

9.1.14 display environment

Syntax

display environment

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display environment コマンドを使用して温度情報を表示します。

例

温度情報を表示します。

<AC> display environment

```
System Temperature information (degree centigrade):
---------------------------------------------------
Slot  Sensor       Temperature LowerLimit WarningLimit AlarmLimit ShutdownLimit
1     inflow  1    29          3          58           70          N/A
1     hotspot 1(cpu)73          20         85           100         N/A
```

表 9-5 diplay environment コマンドの表示情報の説明

フィールド	説明
System Temperature information (degree centigrade)	温度情報（℃）
sensor	温度センサ ● hotspot−ホットスポットセンサ ● inflow−吸気口周辺の温度センサ
Slot	スロット番号
Temperature	現在の温度
LowerLimit	下限しきい値。このフィールドをサポートしていない場合はNAと表示します。
WarningLimit	ワーニングしきい値。このフィールドをサポートしていない場合は、NAと表示します。
AlarmLimit	アラームしきい値。このフィールドをサポートしていない場合はNAと表示します。

フィールド	説明
ShutdownLimit	シャットダウンしきい値。シャットダウンしきい値を超えると、装置は再起動します。このフィールドをサポートしていない場合は、NAと表示します。 シャットダウンしきい値は**temperature-limit**コマンドで変更できません。

9.1.15 display maintain cpu-usage history process

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

display maintain cpu-usage history process *process-name* [**days-ago** *days*] [**start-time** *value*] [**interval** *interval*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

process *process-name*: プロセス名を指定します。

days-ago *days*: 指定した日数前に生成された情報を表示します。指定できる範囲は 1~7 です。

start-time *value*: 指定した時間以降に生成された情報を表示します。指定できる範囲は 0~23 です。

interval *interval*: WLAN プロセスの CPU 使用率の表示間隔を指定します。指定できる間隔は、1 分、5 分、20 分です。

verbose: WLAN プロセスの CPU 使用率の詳細情報を表示します。この引数を指定しない場合、このコマンドは簡易情報を表示します。

説明

display maintain cpu-usage history process コマンドは WLAN プロセスの CPU 使用率の統計情報ヒストリを表示します。

例

STAMGR プロセスの CPU 使用率の詳細情報を表示します。

<AC> display maintain cpu-usage history process process-name stamgr verbose

```
Process                : stamgrd
Interval               : 5min
Slot                   : 1
Time                   CPU utilization rate
02-01 15:44             9%
02-01 15:49             9%
02-01 15:54             9%
```

表 9-6 コマンド出力

フィールド	説明
Process	プロセス名
Interval	CPU使用率のサンプリング間隔
Slot	メンバ装置ID
Time	情報の開始時間
CPU utilization rate	CPU使用率

9.1.16 display memory

Syntax

display memory

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display memory コマンドは装置のメモリ使用率を表示します。

例

メモリ使用情報を簡易表示します。

<AC> display memory

表 9-7 コマンド出力

フィールド	説明
Mem	メモリ使用率
Total	割り当てることができる物理メモリサイズの合計 メモリサイズは2つの部分に分けられる。 1番目は単独でカーネルコード、カーネル管理に使用される。2番目は稼働サービスモジュールのようなタスク、ファイルの格納に使用される。2番目のサイズはトータルの物理メモリサイズから1番目のメモリサイズを引いたサイズとなる。
Used	使用されている物理メモリ
Free	使用されていない物理メモリ
Shared	プロセスによって共有されている物理メモリ
Buffers	バッファで使用されている物理メモリ
Cached	キャッシュで使用されている物理メモリ
FreeRatio	使用されていないメモリの割合です。
-/+ Buffers/Cache	-/+ Buffers/Cache:Used = Mem:Used － Mem:Buffers － Mem:Cached ここで物理メモリはアプリケーションで使用されていることを示す -/+ Buffers/Cache:Free = Mem:Free + Mem:Buffers + Mem:Cached ここで物理メモリはアプリケーションで使用可能であることを示す
Swap	スワップメモリ

9.1.17 display memory-threshold

Syntax

display memory-threshold

View

すべての view

定義済みユーザロール

network-admin

説明

display memory-threshold コマンドは装置のメモリしきい値とメモリ使用率通知の統計情報を表示します。

メモリ使用率通知の詳細は以下のログ情報を参照してください。

MEM_EXCEED_THRESHOLD あるいは MEM_BELOW_THRESHOLD

例

装置のメモリしきい値とメモリ使用率通知の統計情報を表示します。

<AC> display memory-threshold

```
Memory usage threshold: 100%
Free memory threshold:
    Minor: 64M
    Severe: 48M
    Critical: 32M
    Normal: 96M
Current memory state: Normal
Event statistics:
 [Back to normal state]
   First notification: 2017-2-15 09:21:35.546
   Latest notification: 2017-2-15 09:21:35.546
   Total number of notifications sent: 1
 [Enter minor low-memory state]
   First notification at: 2017-2-15 09:07:05.941
   Latest notification at: 2017-2-15 09:07:05.941
   Total number of notifications sent: 1
 [Back to minor low-memory state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
 [Enter severe low-memory state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
 [Back to severe low-memory state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
 [Enter critical low-memory state]
   First notification at: 0.0
```

```
Latest notification at: 0.0
Total number of notifications sent: 0
```

9.1.18 display scheduler job

Syntax

display scheduler job [*job-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

job-name: job の名前を指定します。設定範囲は 1～47 文字で、大文字小文字を区別します。指定しない場合、すべての job の設定情報を表示します。

説明

display scheduler job コマンドは job 設定情報を表示します。

例

すべての job の設定情報を表示します。

<AC> display scheduler job

```
Job name: saveconfig
 copy startup.cfg backup.cfg

Job name: backupconfig

Job name: creat-VLAN100
 system-view
 vlan 100
```

// 出力では、装置は 3 つの job があることを示します。最初の job には 1 つのコマンドがあります。2 番目の job にはコマンドがありません。3 番目の job には 2 つのコマンドがあります。job は空白行で区切られます。

9.1.19 display scheduler logfile

Syntax

display scheduler logfile

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display scheduler logfile コマンドは job 実行のログ情報を表示します。

例

実行された job のログ情報を表示します。

<AC> display scheduler logfile

```
Logfile Size: 1902 Bytes.

Job name       : shutdown
Schedule name   : shutdown
Execution time  : Tue Feb 27 10:44:42 2017
Completion time : Tue Feb 27 10:44:47 2017
---------------------------------                  Job                    output
-----------------------------------
<AC>system-view
System View: return to User View with Ctrl+Z.
[AC]interface rang gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[AC-if-range]shutdown
```

表 9-8 コマンド出力

フィールド	説明
Logfile Size	ログファイルのサイズ。byteで表示される。
Schedule name	jobが所属するスケジュール
Execution time	jobが開始されたときの時間
Completion time	jobが完了したときの時間 jobが実行されなかった、あるいはjobにコマンドがない場合、このフィールドは表示されない

フィールド	説明
Job output	jobのコマンドと出力

関連コマンド

reset scheduler logfile

9.1.20 display scheduler reboot

Syntax

display scheduler reboot

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display scheduler reboot コマンドは自動再起動のスケジュールを表示します。

例

装置の自動再起動スケジュールを表示します。

<AC> display scheduler reboot

```
System will reboot at 16:32:00 03/03/2017 (in 1 hours and 39 minutes).
```

関連コマンド

- **scheduler reboot at**
- **scheduler reboot delay**

9.1.21 display scheduler schedule

Syntax

display scheduler schedule [*schedule-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

schedule-name: スケジュール名を指定します。設定範囲は 1～47 文字で大文字小文字を区別します。指定しない場合、すべてのスケジュールの情報を表示します。

説明

display scheduler schedule コマンドはスケジュール情報を表示します。

例

すべてのスケジュールの情報を表示します。

<AC> display scheduler schedule

```
Schedule name       : shutdown
Schedule type       : Run once after 0 hours 2 minutes
Start time          : Tue Feb 27 10:44:42 2017
Last execution time  : Tue Feb 27 10:44:42 2017
Last completion time : Tue Feb 27 10:44:47 2017
Execution counts    : 1
------------------------------------------------------------------------
Job name                                    Last execution status
shutdown                                    Successful
```

表 9-9 コマンド出力

フィールド	説明
Schedule type	スケジュールが実行される時間です。実行時間が指定されていない場合、このフィールドは表示されません。
Start time	初回にスケジュールが実行される時間です。実行時間が指定されていない場合、このフィールドは表示されません。
Last execution time	スケジュールが実行されたときの最後の時間です。実行時間が指定されていない場合、このフィールドは表示されません。スケジュールが実行されていない場合、"Yet to be executed"と表示されます。
Last completion time	スケジュールが完了した最後の時間です。実行時間が指定されていない場合、このフィールドは表示されません。
Execution counts	スケジュールが実行された回数です。実行時間が指定されていない場合、このフィールドは表示されません。
Job name	スケジュールのjob名です。

フィールド	説明
Last execution status	最後に実行された結果です。 Successful Failed Waiting–装置はスケジュールを実行し、jobが実行待ちです。 In process–jobが実行されています。 -NA-–実行時間になっていません。 jobのコマンドが実行されたかどうかについての情報および実行結果を表示するには、display scheduler logfileコマンドを実行してください。

9.1.22 display transceiver alarm

Syntax

display transceiver alarm interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number:タイプと番号でインタフェースを指定します。インタフェースを指定しない場合、このコマンドはすべてのトランシーバモジュールに存在するアラームを表示します。

説明

display transceiver alarm コマンドは、プラガブルインタフェースモジュールのアラームを表示します。

表 9-10 は、一般的なトランシーバアラームの構成要素を示しています。エラーが発生しない場合は「None」と表示されます。

表 9-10 一般的なトランシーバアラーム構成要素

フィールド	説明
APD	アバランシェフォトダイオード
PCS	物理符号化サブレイヤ
PHY XS	PHY拡張サブレイヤ
PMA/PMD	物理媒体アタッチメント部 / 物理媒体依存部

フィールド	説明
power	光出力
REFCLK	基準クロック
RX	受信
TEC	熱電冷却器
Temp	温度
TX	送信
WIS	WANインタフェースサブレイヤ

例

GigabitEthernet 1/0/1 のトランシーバモジュールに存在するアラームを表示します。

<AC> display transceiver alarm interface gigabitethernet 1/0/1

```
GigabitEthernet1/0/1 transceiver current alarm information:
  RX signal loss
  RX power low
```

表 9-11 display transceiver コマンドの表示情報の説明

フィールド	説明
transceiver current alarm information	トランシーバの現在のアラーム情報
RX loss of signal	受信信号損失
RX power low	受信出力低下

9.1.23 display transceiver diagnosis

Syntax

display transceiver diagnosis interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface [*interface-type interface-number*]:タイプと番号でインタフェースを指定します。指定しない場合、各トランシーバモジュールのデジタル診断パラメータの現在値を表示します。

説明

display transceiver diagnosis コマンドはトランシーバモジュールのデジタル診断パラメータの現在値を表示します。

例

GigabitEthernet 1/0/6 のトランシーバモジュールのデジタル診断パラメータの現在値を表示します。

<AC> display transceiver diagnosis interface GigabitEthernet 1/0/6

```
GigabitEthernet1/0/6 transceiver diagnostic information:
 Current diagnostic parameters:
  Temp(°C)  Voltage(V)  Bias(mA)  RX power(dBm)  TX power(dBm)
  36        3.31        6.13      -35.64         -5.19
 Alarm thresholds:
         Temp(°C)   Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM)
  High   50         3.55        1.44      -10.00         5.00
  Low    30         3.01        1.01      -30.00         0.00
```

表 9-12 コマンド出力

フィールド	説明
transceiver diagnostic information	インタフェースのトランシーバモジュールのデジタル診断パラメータの情報
Temp.(°C)	温度(単位は℃)　1℃単位で表示
Voltage(V)	電圧（単位はV）0.01V単位で表示
Bias(mA)	バイアス電流（単位はmA）0.01 mA単位で表示
RX power(dBm)	受信電圧（単位はdBm）0.01dBm単位で表示
TX power(dBm)	送信電圧（単位はdBm）0.01dBm単位で表示

9.1.24 display transceiver interface

Syntax

display transceiver interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: タイプと番号でインタフェースを指定します。指定しない場合、各トランシーバモジュールの主なパラメータを表示します。

説明

display transceiver interface コマンドはトランシーバモジュールの主要パラメータを表示します。

例

GigabitEthernet 1/0/6 のトランシーバモジュールの主なパラメータを表示します。

<AC> display transceiver interface GigabitEthernet 1/0/6

```
GigabitEthernet1/0/6 transceiver information:
  Transceiver Type            : 1000_BASE_SX_SFP
  Connector Type              : LC
  Wavelength(nm)              : 850
  Transfer Distance(m)         : 550(50um),270(62.5um)
  Digital Diagnostic Monitoring : YES
  Vendor Name                 : AVAGO
```

表 9-13 コマンド出力

フィールド	説明
Connector Type	コネクタタイプ • SC: NTTによって提供されているファイバコネクタ • LC: 1.25 mm/RJ-45 ファイバコネクタ • RJ-45 • CX 4
Wavelength(nm)	• **光ファイバトランシーバ**: 送信されたレーザの中心波長（mm） 複数の波長をサポートしている場合、コンマで区切られて波長が記載される。銅線ケーブルでは、本フィールドは**N/A**と表示される。

フィールド	説明
Transfer Distance(xx)	伝送距離。xxは距離の単位。 • km—キロメートル（シングルモードトランシーバ用） • m—メートル（その他のトランシーバ用） トランシーバが複数の伝送媒体をサポートしている場合、本フィールドはタイプごとの伝送距離を、transmission distance (medium type)の形式で表示する。 伝送媒体は下記を含む。 • **9 um**：9/125 umシングルモードファイバ • **50 um**：50/125 umマルチモードファイバ • **62.5 um**：62.5/125 umマルチモードファイバ • **TP**：ツイストペアケーブル • **CX4**：CX4 ケーブル
Digital Diagnostic Monitoring	デジタル診断機能がサポートされているか • **YES**：サポート • **NO**：未サポート

9.1.25 display transceiver manuinfo

Syntax

display transceiver manuinfo interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: タイプおよび番号でインタフェースを指定します。インタフェースが指定されていない場合、このコマンドはすべてのインタフェース上のトランシーバモジュールの電子ラベル情報を表示します。

説明

display transceiver interface コマンドは、トランシーバモジュールの電子ラベル情報を表示します。

本コマンドをサポートしていないモジュールでは、以下のメッセージが表示されます。

```
The transceiver does not support this function.
```

本コマンドをサポートしていないモジュールの情報を確認するには、**display transceiver interface** コマンドを使用してください。

例

GigabitEthernet 1/0/1 のトランシーバーモジュールの電子ラベル情報を表示します。

<AC> display transceiver manuinfo interface gigabitethernet 1/0/1

```
GigabitEthernet1/0/1 transceiver manufacture information:
  Manu. Serial Number : 210231A1RPN22600345K
  Manufacturing Date  : 2022-06-27
  Vendor Name         : Hisense
```

9.1.26 display version

Syntax

display version

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display version コマンドはシステムバージョン情報を表示します。

例

システムのバージョン情報を表示します。

<AC> display version

9.1.27 header

Syntax

header { **incoming** | **legal** | **login** | **motd** | **shell** } *text*

undo header { **incoming** | **legal** | **login** | **motd** | **shell** }

View

System view

定義済みユーザロール

network-admin

パラメータ

incoming: モデムのログインユーザが user view に移行する際に表示されるバナーを設定します。認証が必要な場合、認証にパスしたのちバナーが表示されます。

legal: ユーザがユーザ名およびパスワードを CLI にアクセスして入力する前にバナーを設定します。

login: ログインユーザによってパスワードまたは scheme 認証される前にバナーを設定します。

motd: **legal** バナーが表示される前に greeting（あいさつ）バナーを設定します。

shell: 非モデムログインユーザが user view に移行する際に表示されるバナーを設定します。

text: バナーメッセージです。パラメータあるいは複数行の 2 つの形式で入力できます。詳細は、オペレーションマニュアルのセクション 1 *はじめに “装置管理”* を参照してください。

説明

header コマンドはバナーを設定します。

undo header コマンドはバナーを削除します。

例

incoming バナー、legal バナー、login バナー、MOTD バナー、shell バナーを作成します。

<AC> system-view

[AC] header incoming

```
Please input banner content, and quit with the character '%'.
Welcome to incoming(header incoming)%
```

[AC] header legal

```
Please input banner content, and quit with the character '%'.
Welcome to legal (header legal)%
```

[AC] header login

```
Please input banner content, and quit with the character '%'.
Welcome to login(header login)%
```

[AC] header motd

```
Please input banner content, and quit with the character '%'.
Welcome to motd(header motd)%
```

[AC] header shell

```
Please input banner content, and quit with the character '%'.
Welcome to shell(header shell)%
```

本例では、パーセント記号（%）は各バナーの開始及び終了文字で、バナー内には含まれません。

設定をテストするために telnet を実行します。ログインバナーは、password または scheme ログイン認証が設定されている場合のみ表示されます。

```
Welcome to legal (header legal)
 Press Y or ENTER to continue, N to exit.

Welcome to motd(header motd)

Welcome to login(header login)

Login authentication


Password:

Welcome to shell(header shell)
```

9.1.28 job

Syntax

job *job-name*

undo job *job-name*

デフォルト

設定なし

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

job-name: job 名を指定します。設定範囲は 1～47 文字で、大文字、小文字を区別します。

説明

job コマンドはスケジュール自動実行機能のスケジュールに job を割り当てます。

undo job コマンドは job を削除します。

スケジュールに複数の job を割り当てることができます。スケジュールの job は連続して実行されます。

スケジュールに割り当てられる job はあらかじめ作成されている必要があります。job を作成する場合、**scheduler job** コマンドを使用します。

例

スケジュール saveconfig に job 名が save-job の job を割り当てます。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] job save-job

関連コマンド

- **scheduler job**
- **scheduler schedule**

9.1.29 locator blink

🕮 **メモ：**

locator blink コマンドはソフトウェアバージョン 7.2.67 を含む以降のソフトウェアからサポートしています。

Syntax

locator blink *blink-time* [**ap** *ap-name*]

locator blink stop [**ap** *ap-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

blink-time:Power LED を点滅させる時間を秒単位で指定します。設定範囲は 5 から 120 秒です。

stop:Power LED の点滅を停止します。

ap *ap-name*: AP 名を指定します。設定範囲は 1～64 文字で大文字、小文字を区別します。文字列には、英字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含めることができます。

🕮 **メモ：**

ap *ap-name* パラメータは、ソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

説明

locator blink *blink-time* コマンドは、指定した装置の Power LED を blink-time で指定した時間緑→赤の順に点滅させます。**locator blink stop** コマンドを実行すると、**locator blink** *blink-time* コマンドによる Power LED の点滅を停止します。

本機能は装置の位置を特定する際に役立ちます。

例

点滅時間を 30 秒に指定して Power LED の点滅を開始します。

<AP> locator blink 30

Power LED の点滅を停止します。

<AP> locator blink stop

9.1.30 memory-threshold

Syntax

memory-threshold minor *minor-value* **severe** *severe-value* **critical** *critical-value* **normal** *normal-value*

undo memory-threshold

デフォルト

Minor: 96 MB.

Severe: 64 MB.

Critical: 48 MB.

Normal: 128 MB.

View

System view

定義済みユーザロール

network-admin

パラメータ

minor *minor-value*: **minor** アラームのしきい値を指定します。設定範囲は 0～992 です。しきい値は **normal** しきい値以下にする必要があります。0 に指定すると **minor** アラーム機能を無効にします。

severe *severe-value*: **severe** アラームのしきい値を指定します。設定範囲は **minor** アラームのしきい値によって変わります。しきい値は **minor** しきい値以下にする必要があります。0 に指定すると **severe** アラーム機能を無効にします。

critical *critical-value*: **critical** アラームのしきい値を指定します。設定範囲は **severe** アラームのしきい値によって変わります。しきい値は **severe** しきい値以下にする必要があります。0 に指定すると **critical** アラーム機能を無効にします。

normal *normal-value*: **normal** アラームのしきい値を指定します。設定範囲は **minor** アラームのしきい値によって変わります。しきい値はメモリサイズの合計以下にする必要があります。

説明

memory-threshold コマンドは空きメモリ容量のしきい値を設定します。

undo memory-threshold コマンドはデフォルトに戻します。

正常な動作とメモリ使用率を改善するため、システムはリアルタイムで使用可能なメモリサイズをモニタします。しきい値が超過すると、モジュールあるいはプロセスで対策を行うことができるように、システムはアラーム通知あるいはアラーム解除通知を関係するモジュールあるいはプロセスに通知します。しきい値の詳細はオペレーションマニュアルのセクション 1 *はじめに* *“装置管理”* を参照してください。

例

minor アラームを 64MB、severe アラームを 48MB、critical アラームを 32MB、normal アラームを 96MB に設定します。

<AC> system-view

[AC] memory-threshold minor 64 severe 48 critical 32 normal 96

関連コマンド

display memory-threshold

9.1.31 monitor cpu-usage enable

Syntax

monitor cpu-usage enable

undo monitor cpu-usage enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

monitor cpu-usage enable コマンドは CPU 使用率の監視を有効にします。

undo monitor cpu-usage enable コマンドは CPU 使用率の監視を無効にします。

CPU 使用率の監視を有効にしたのち、**monitor cpu-usage interval** コマンドで指定したサンプリング間隔で CPU 使用率を監視、保存します。最新の CPU 使用率を表示する場合、**display cpu-usage history** コマンドを使用します。

例

CPU 使用率の監視を有効にします。

<AC> system-view

[AC] monitor cpu-usage enable

関連コマンド

- **display cpu-usage configuration**
- **display cpu-usage history**
- **monitor cpu-usage interval**

9.1.32 monitor cpu-usage interval

Syntax

monitor cpu-usage interval *interval-value*

デフォルト

1 分

View

System view

定義済みユーザロール

network-admin

パラメータ

interval-value: CPU 使用率のサンプリング間隔を指定します。5Sec、1Min、5Min から指定します。5Sec は 5 秒、**1Min** は 1 分、**5Min** は 5 分です。

説明

monitor cpu-usage interval コマンドは CPU 使用率のサンプリング間隔を設定します。

CPU 使用率の監視を有効にしたのち、指定したサンプリング間隔で CPU 使用率を監視し、保存します。最新の CPU 使用率を表示する場合、**display cpu-usage history** コマンドを使用します。

例

CPU 使用率のサンプリング間隔を 5 秒に設定します。

<AC> system-view

[AC] monitor cpu-usage interval 5Sec

関連コマンド

- **display cpu-usage configuration**
- **display cpu-usage history**
- **monitor cpu-usage enable**

9.1.33 monitor cpu-usage threshold

Syntax

monitor cpu-usage threshold *cpu-threshold*

undo monitor cpu-usage threshold

デフォルト

99%

View

System view

定義済みユーザロール

network-admin

パラメータ

cpu-threshold: CPU 使用率のしきい値を指定します。設定範囲は 0～100%です。

説明

monitor cpu-usage threshold コマンドは CPU 使用率のしきい値を設定します。

undo monitor cpu-usage threshold コマンドはデフォルトに戻します。

装置は 1 分間隔で CPU 使用率をサンプリングします。サンプリングした値と CPU の使用率のしきい値を比較します。CPU 使用率のしきい値より大きい場合、装置は trap を送信します。

例

CPU 使用率のしきい値を 80%に設定します。

<AC> system-view

[AC] monitor cpu-usage threshold 80

関連コマンド

display cpu-usage configuration

9.1.34 password-recovery enable

Syntax

password-recovery enable

undo password-recovery enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

password-recovery enable コマンドはパスワードリカバリ機能を有効にします。

undo password-recovery enable コマンドはパスワードリカバリ機能を無効にします。

パスワードリカバリ機能は Boot ROM メニューからデバイス構成と SDRAM へのアクセスを制御できます。

パスワードリカバリ機能が有効である場合、コンソールからのユーザは認証なしで装置にアクセスでき、新しいパスワードを設定することができます。

パスワードリカバリ機能が無効である場合、コンソールからのユーザは、新しいパスワードを設定する前に、工場出荷状態にする必要があります。工場出荷状態に戻すと次回に起動で使用するコンフィグレーションファイルを削除します。

セキュリティを強化するためには、パスワードリカバリ機能は無効にします。

Boot ROM メニューオプションが利用できるかは、パスワードリカバリ機能背亭に依存します。追加の情報については、リリースノートを参照ください。

例

パスワードリカバリ機能を無効にします。

<AC> system-view

[AC] undo password-recovery enable

9.1.35 reboot

Syntax

reboot [**slot** *slot-number*] [**force**]

View

User view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: **メンバ ID によって IRF スタックのメンバ装置を指定します。このオプションが指定されない場合、IRF スタックではすべての装置を再起動します。**

force: ソフトウェアの確認を行わず、すぐに装置を再起動します。本キーワードを指定しない場合、システムは、再起動によってデータ紛失あるいはシステムの故障が発生するかどうかを確認します。たとえば、システムはメインシステムソフトウェアのファイルが存在するか、および書き込み操作が記憶媒体で進行中であるかどうか確認します。再起動によって問題は発生すると認識した場合、システムは装置の再起動を行いません。

説明

reboot コマンドは装置を再起動します。

例

最後に稼働中のコンフィグレーションを保存してから設定変更されていない場合、装置を再起動します。

<AC> reboot

```
Start to check configuration with next startup configuration file, please
wait.........DONE!
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

設定変更があった場合は、装置を再起動して設定を保存します。

<AC> reboot

```
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration?
[Y/N]:y
Please input the file name(*.cfg)[ cfa0:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
cfa0:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to cfa0 successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

設定変更があった場合は、装置を再起動しますが、設定は保存しません。

<AC> reboot

```
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration?
[Y/N]:n
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

ソフトウェアチェックを行わず、すぐに装置を再起動します。

<AC> reboot force

```
A forced reboot might cause the storage medium to be corrupted. Continue? [Y/N]:y
Now rebooting, please wait..
```

9.1.36 reset scheduler logfile

Syntax

reset scheduler logfile

View

User view

定義済みユーザロール

network-admin

説明

reset scheduler logfile コマンドはスケジュール自動実行機能のログ情報の削除を行います。

例

スケジュール自動実行機能のログ情報を削除します。

<AC> reset scheduler logfile

関連コマンド

display scheduler logfile

9.1.37 restore factory-default

Syntax

restore factory-default

View

User view

定義済みユーザロール

network-admin

説明

restore factory-default コマンドは装置を工場出荷時のデフォルト状態に復元します。

⚠ **注意：**

このコマンドは注意して使用してください。デバイスを別の用途で使用する場合、または他の方法を使用してデバイスのトラブルシューティングを行うことができない場合のみ、このコマンドを使用してください。

例

装置を工場出荷時のデフォルト状態に復元します。

<AC> restore factory-default

```
This command will restore the system to the factory default configuration and clear
the operation data, and forcibly reboot the system. Continue [Y/N]:y
Restoring the factory default configuration. This process might take a few minutes.
Please wait....Done.
The system is rebooting...
```

関連コマンド

reboot

9.1.38 scheduler job

Syntax

scheduler job *job-name*

undo scheduler job *job-name*

デフォルト

なし

View

System view

定義済みユーザロール

network-admin

パラメータ

job-name: job 名を指定します。設定範囲は 1～47 文字で大文字、小文字を区別します。

説明

scheduler job コマンドはスケジュール自動実行機能の job を作成し、job view に移行します。すでに job が存在する場合、直接 job view に移行します。

undo scheduler job コマンドは job を削除します。

job は複数のスケジュールから参照可能です。job view で job にコマンドを割り当てることができます。

例

job 名が **backupconfig** の job を作成し、job view に移行します。

<AC> system-view

[AC] scheduler job backupconfig

[AC-job-backupconfig]

関連コマンド

- **command**
- **scheduler schedule**

9.1.39 scheduler logfile size

Syntax

scheduler logfile size *value*

デフォルト

16KB

View

System view

定義済みユーザロール

network-admin

パラメータ

value: job を実行するログファイルのサイズを KB で設定します。設定範囲は 16～1024 です。

説明

scheduler logfile size コマンドはスケジュール自動実行機能の job を実行するログファイルのサイズを設定します。

job を実行するログファイルは、job が実行される情報を保存します。ファイルの容量が一杯である場合、古い記録が削除され、新しい記録が保存されます。もしファイルサイズよりもログファイルのサイズが大きい場合、実行される情報はファイルに保存されません。

例

job を実行するログファイルのサイズを 32KB に設定します。

<AC> system-view

[AC] scheduler logfile size 32

関連コマンド

display scheduler logfile

9.1.40 scheduler reboot at

Syntax

scheduler reboot at *time* [*date*]

undo scheduler reboot

デフォルト

設定なし

View

User view

定義済みユーザロール

network-admin

パラメータ

time: 再起動する時間を指定します。形式は *hh*:*mm* です。*hh* の設定範囲は 0～23 です。*mm* の設定範囲は 0～59 です。

date: 再起動する日時を指定します。形式は *MM*/*DD*/*YYYY* あるいは *YYYY*/*MM*/*DD* です。*YYYY* の設定範囲は 2000～2035 です。*MM* の設定範囲は 1～12 です。*DD* の設定範囲は月によって変わります。

説明

scheduler reboot at コマンドはスケジュール再起動機能の日時、時間を指定します。

undo scheduler reboot コマンドはスケジュール再起動機能の設定を削除します。

⚠ **注意：**

装置を再起動するとネットワークサービスが中断されます。

---

date 引数が指定されていないときは、以下の動作を行います。

- 再起動時間が現在時刻より遅い場合、再起動は当日の再起動時間に行われます。
- 再起動時間が現在時刻より早い場合、再起動は次の日の再起動時間に行われます。

データ保護のため、ファイルの操作を実行している間、システムは装置の再起動を行いません。

装置はスケジュール再起動機能を 1 回のみサポートします。もし **schedule reboot delay** コマンドと **scheduler reboot at** コマンドの両方が設定されている場合、あるいはどちらかのコマンドを複数回設定した場合、最後に設定したコマンドが適用されます。

例

装置を PM12:00 に再起動します。現在時刻は 2017 年 2 月 6 日 11:43 であると仮定します。

<AC> scheduler reboot at 12:00

```
Reboot system at 12:00:00 06/02/2017 (in 0 hours and 16 minutes). Confirm? [Y/N]:
```

関連コマンド

scheduler reboot delay

9.1.41 scheduler reboot delay

Syntax

scheduler reboot delay *time*

undo scheduler reboot

デフォルト

設定なし

View

User view

定義済みユーザロール

network-admin

パラメータ

time: 再起動する時間を指定します。形式は *hh*:*mm* あるいは *mm* です。パラメータは 6 文字まで設定することができます。形式が *hh*:*mm* である場合、*mm* の設定範囲は 0～59 です。

説明

scheduler reboot delay コマンドはスケジュール再起動機能の再起動遅延時間を指定します。

undo scheduler reboot コマンドはスケジュール再起動機能の再起動遅延時間を削除します。

⚠ **注意**：

装置を再起動するとネットワークサービスが中断されます。

データ保護のため、ファイルの操作を実行している間、システムは装置の再起動を行いません。

装置はスケジュール再起動機能を 1 回のみサポートします。もし **schedule reboot delay** コマンドと **scheduler reboot at** コマンドの両方が設定されている場合、あるいはどちらかのコマンドを複数回設定した場合、最後に設定したコマンドが適用されます。

例

装置を 88 分後に再起動します。現在時刻は 2017 年 2 月 6 日の 11:48 であると仮定します。

<AC> scheduler reboot delay 88

```
Reboot system at 13:16 06/02/2017(in 1 hours and 28 minutes). Confirm? [Y/N]:
```

9.1.42 scheduler schedule

Syntax

scheduler schedule *schedule-name*

undo scheduler schedule *schedule-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

schedule-name: スケジュール名を指定します。設定範囲は 1～47 文字で大文字、小文字を区別します。

説明

scheduler schedule コマンドはスケジュール自動実行機能のスケジュールを作成し、schedule view に移行します。すでにスケジュールが存在する場合はすぐに schedule view に移行します。

undo scheduler schedule コマンドはスケジュールを削除します。

管理に影響を与えずに自動的にコマンドあるいはコマンドセットを装置が実行するように、スケジュールを設定することができます。

スケジュールを設定するには以下を行います。

1) **scheduler job** コマンドを使用して job を作成します。
2) job view で **command** コマンドを使用して job にコマンドを割り当てます。
3) **scheduler schedule** コマンドを使用してスケジュールを作成します。
4) schedule view で **job** コマンドを使用してスケジュールに job を割り当てます。複数の job をスケジュールに割り当てることができます。job はすでに作成している必要があります。

5) schedule view で **user-role** コマンドを使用してスケジュールにユーザロールを割り当てます。スケジュールに最大 64 のユーザロールを割り当てることができます。
6) schedule view で **time at** コマンド、**time once** コマンド、あるいは **time repeating** コマンドを使用して、スケジュールを実行する時間を指定します。1 つのスケジュールに 1 つの実行時間のみ指定することができます。

例

スケジュール名が saveconfig のスケジュールを作成します。

<AC> system-view

[AC] scheduler schedule saveconfig

関連コマンド

- **job**
- **time at**
- **time once**

9.1.43 shutdown-interval

Syntax

shutdown-interval interval

undo shutdown-interval

デフォルト

30 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

time: 検出間隔を指定します。設定範囲は 0～300 秒です。0 秒に設定すると検出を行いません。

説明

shutdown-interval コマンドはポートの状態検出タイマを設定します。

undo shutdown-interval コマンドはデフォルトに戻します。

プロトコルによってポートがシャットダウンされる際、装置はポート状態検出タイマを開始します。タイマ経過後、装置はポートの物理状態を反映するため、ポートを起動します。

ポートの検出期間にタイマを変更した場合、装置は新しい設定 T1 とポートがシャットダウンしてから経過した時間 T を比較します。

もし T<T1 の場合、ポートは T1-T 秒後に起動します。

もし T>=T1 の場合、ポートはすぐに起動します。

たとえば、ポートがシャットダウンしてから 2 秒後にタイマを 30 秒から 10 秒に変更した場合、ポートは 8 秒後に起動します。ポートがシャットダウンしてから 10 秒後にタイマを 30 秒から 2 秒に変更した場合、ポートはすぐに起動します。

例

ポートの状態を検出する検出間隔を 100 秒に設定します。

<AC> system-view

[AC] shutdown-interval 100

9.1.44 sysname

Syntax

sysname *sysname*

undo sysname

デフォルト

装置名

View

System view

定義済みユーザロール

network-admin

パラメータ

sysname: 装置名を指定します。設定範囲は 1～64 文字です。

説明

sysname コマンドは装置名を設定します。

undo sysname コマンドはデフォルトに戻します。

装置名はネットワークの装置を識別し、CLI の user view のプロンプトとして使用されます。装置名が Switch である場合、user view のプロンプトは<Switch>です。

例

装置名を R2000 に設定します。

<AC> system-view

[AC] sysname R2000

[R2000]

9.1.45 temperature-limit

Syntax

temperature-limit slot *slot-number* { **hotspot** | **inflow** } *sensor-number lowlimit warninglimit* [*alarmlimit*]

undo temperature-limit slot *slot-number* { **hotspot** | **inflow** } *sensor-number*

デフォルト

inflow の *lowlimit* は 3

inflow の *warninglimit* は 58

inflow の *alarmlimit* は 70

hotspot の *lowlimit* は 3

hotspot の *warninglimit* は 58

hotspot の *alarmlimit* は 70

View

System view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number* : IRF スタックのメンバ装置のメンバ ID を指定します。

hotspot：ホットスポットセンサの温度アラームしきい値を設定します。ホットスポットセンサは通常、大量の熱を発生させるチップの近くにあり、チップの監視に使用されます。

inflow：吸気口センサの温度アラームしきい値を設定します。吸気口の近くに吸気口センサがあり、周囲温度の監視に使用されます。

sensor-nummber：センサを番号で指定します。番号は 1 を指定します。

lowlimit：摂氏温度表示による下限温度を指定します。

warninglimit：摂氏温度表示による高温時のワーニングしきい値を指定します。しきい値は下限温度よりも高い値にする必要があります。

alarmlimit : 摂氏温度表示による高温時のアラームしきい値を指定します。しきい値はワーニングしきい値よりも高い値にする必要があります。

説明

temperature-limit コマンドは温度アラームのしきい値を設定します。

undo temperature-limit コマンドはデフォルトに戻します。

しきい値の設定範囲は、CLI オンラインヘルプを使用して確認してください。

装置の温度が下限温度を下回るか、高温時のワーニング、またはアラームしきい値に到達したとき、装置は次の操作を実行します。

- ログメッセージとトラップを送信します。
- 装置の前面にある LED 表示で通知します。

例

スロット 1 内の hotspot センサ 1 の温度アラームしきい値を設定します。

<AC> system-view

[AC] temperature-limit slot 1 hotspot 1 40 70 80

9.1.46 time at

Syntax

time at *time date*

undo time

デフォルト

スケジュールの実行日と時間は指定されていません。

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

time: スケジュールを自動で実行する時間を指定します。形式は *hh*:*mm* です。*hh* の設定範囲は 0～23 です。*mm* の設定範囲は 0～59 です。

date: スケジュールを自動で実行する実行日を指定します。形式は *MM*/*DD*/*YYYY* あるいは *YYYY*/*MM*/*DD* です。YYYY の設定範囲は 2000～2035 です。MM の設定範囲は 1～12 です。DD の設定範囲は月によって変わります。

説明

time at コマンドは 1 回のみのスケジュール自動実行機能の実行日と時間を指定します。

undo time コマンドはスケジュール自動実行機能の実行日と時間の設定を削除します。

指定時間（実行日と時間）は現在時刻よりも後にする必要があります。

time at コマンド、**time once** コマンド、**time repeating** コマンドは、同時に設定することはできません。最後に設定したコマンドが適用されます。

例

2017 年 5 月 11 日の AM01:01 にスケジュール saveconfig を実行するように設定します。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] time at 1:1 2017/05/11

関連コマンド

scheduler schedule

9.1.47 time once

Syntax

time once at *time* [**month-date** *month-day* | **week-day** *week-day*&<1-7>]

time once delay *time*

undo time

デフォルト

スケジュールの実行日と時間は指定されていません。

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

at *time*: スケジュールを実行する時間を指定します。形式は *hh*:*mm* です。*hh* の設定範囲は 0～23 です。*mm* の設定範囲は 0～59 です。

month-date *month-day*: 月日を指定します。設定範囲は 1～31 です。当月に指定した日が存在しない場合、翌月の該当する日が適用されます。

week-day *week-day*&<1-7>: スケジュールを実行する曜日を指定します。半角スペースで区切り、曜日を最大 7 つまで指定します。値は Mon、Tue、Wed、Thu、Fri、Sat、Sun です。

delay *time*: スケジュールを実行する時間を指定します。形式は *hh*:*mm* あるいは *mm* です。パラメータは 6 文字まで設定することができます。形式が *hh*:*mm* である場合、*mm* の設定範囲は 0～59 です。

説明

time once コマンドは 1 回のみのスケジュール自動実行機能の複数の実行日と時間を指定します。

undo time コマンドはスケジュール自動実行機能の実行日と時間の設定を削除します。

指定された時間が過ぎている場合、次の日の指定された時間が適用されます。

指定された月日が過ぎている場合、次の月の指定された日が適用されます。

指定された曜日が過ぎている場合、次の週の指定された曜日が適用されます。

time at コマンド、**time once** コマンド、**time repeating** コマンドは、同時に設定することはできません。最後に設定したコマンドが適用されます。

例

15:00 にスケジュール **saveconfig** を実行するように設定します。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] time once at 15:00

```
Schedule starts at 15:00 5/11/2011.
```

今月の 15 日後の 15:00 にスケジュール **saveconfig** を実行するように設定します。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] time once at 15:00 month-date 15

次の月曜日、金曜日の PM12:00 にスケジュール **saveconfig** を実行するように設定します。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] time once at 12:00 week-day mon fri

10 分後にスケジュール **saveconfig** を実行するように設定します。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] time once delay 10

関連コマンド

scheduler schedule

9.1.48 time repeating

Syntax

time repeating [**at** *time* [*date*]] **interval** *interval-time*

time repeating at *time* [**month-date** [*month-day* | **last**] | **week-day** *week-day*&<1-7>]

undo time

デフォルト

設定なし

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

at *time*: スケジュールを実行する時間を指定します。形式は *hh*:*mm* です。*hh* の設定範囲は 0～23 です。*mm* の設定範囲は 0～59 です。指定しない場合、現在のシステム時間が指定されます。

date: スケジュールを定期的に自動で実行する開始日を指定します。形式は *MM*/*DD*/*YYYY* あるいは *YYYY*/*MM*/*DD* です。YYYY の設定範囲は 2000～2035 です。MM の設定範囲は 1～12 です。DD の設定範囲は月によって変わります。指定しない場合、指定した時間になったときの最初の日が指定されます。

interval *interval-time*: スケジュールを実行する時間を指定します。形式は *hh*:*mm* あるいは *mm* です。*mm* は 6 文字まで設定することができます。形式が *hh*:*mm* である場合、*mm* の設定範囲は 0～59 です。形式が *mm* である場合、パラメータは 1 分以上にする必要があります。

month-date [*month-day* | **last**]: 今月の日を指定します。設定範囲は 1～31 です。今月の日で指定した日が存在しない場合、次の月の該当する日が適用されます。

week-day *week-day*&<1-7>: スケジュールを実行する曜日を指定します。半角スペースで区切り、曜日を最大 7 つまで指定します。値は Mon、Tue、Wed、Thu、Fri、Sat、Sun です。

説明

time repeating コマンドは定期的にスケジュールを実行するタイムテーブルを指定します。

undo time コマンドはスケジュール自動実行機能の時間の設定を削除します。

time repeating [**at** *time* [*date*]] **interval** *interval-time* コマンドは 1 日内の指定した時間で定期的にスケジュールを実行するように設定します。

time repeating at *time* [**month-date** [*month-day* | **last**] | **week-day** *week-day*&<1-7>] コマンドは月あるいは曜日内の指定した日で定期的にスケジュールを実行するように設定します。

time at コマンド、**time once** コマンド、**time repeating** コマンドは、同時に設定することはできません。最後に設定したコマンドが適用されます。

例

本日の 8:00 から 1 時間ごとにスケジュール **saveconfig** を実行するように設定します。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] time repeating at 8:00 interval 60

毎日 PM12:00 にスケジュール **saveconfig** を実行するように設定します。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] time repeating at 12:00

毎月 5 日の AM8:00 にスケジュール **saveconfig** を実行するように設定します。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] time repeating at 8:00 month-date 5

毎月最終日の AM8:00 にスケジュール **saveconfig** を実行するように設定します。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] time repeating at 8:00 month-date last

各金曜日と各土曜日の AM8:00 にスケジュール **saveconfig** を実行するように設定します。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] time repeating at 8:00 week-day fri sat

関連コマンド

scheduler schedule

9.1.49 user-role

Syntax

user-role *role-name*

undo user-role *role-name*

デフォルト

Schedule 作成者のユーザロール

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

role-name: ユーザロール名を指定します。1~63 文字の大文字と小文字を区別する文字列です。ユーザロールはユーザ定義または事前定義されているものが使用できます。事前定義されたユーザロールには、network-admin、network-operator、level-0 から level-15 があります。

説明

user-role コマンドは、Schedule にユーザロールを割り当てます。

undo user-role コマンドは Sceduler からユーザロールを削除します。

Schedule には 1 つ以上のユーザロールが必要です。Schedule 内のコマンドは、その Schedul**e** の 1 つ以上のユーザロールによって許可されている場合に実行できます。ユーザロールに関する詳細は、“*1* はじめに”の“*2* 章 *RBAC*”を参照してください。

例

スケジュール test にユーザロール rolename を割り当てます。

<AC> system-view

[AC] scheduler schedule test

[AC] user-role rolename

関連コマンド

scheduler schedule

目次

このセクションのページは **1-x-x** です。

10 章 Tcl の使用 10-1
10.1 Tcl 設定コマンド 10-1
10.1.1 cli 10-1
10.1.2 tclquit 10-2
10.1.3 tclsh 10-2

10章 Tcl の使用

10.1 Tcl設定コマンド

10.1.1 cli

Syntax

cli *command*

View

Tcl configuration view

定義済みユーザロール

network-admin

パラメータ

command: 実行するコマンドを指定します。完全なコマンドラインである必要があります。

説明

cli コマンドは Tcl コマンドと衝突した場合の Tcl configuration view での Comware コマンドの実行を有効にします。

Tcl configuration view では、Comware コマンドが Tcl コマンドと衝突した場合 Tcl コマンドが実行されます。衝突発生時に Comware コマンドを実行するには、**cli** コマンドを実行します。

Tcl コマンドを実行するためには **cli** コマンドを使用することはできません。

例

Tcl configuration view で Tcl コマンドと衝突する Comware コマンドを実行するには以下の手順を実施します。

1) Tcl configuration view で Comware コマンドを実行します。出力は、Comware コマンドが Tcl コマンドと衝突するために実行できないことを示しています。

<AC> tclsh

<AC-tcl> system-view

[AC-tcl] user-interface vty 0 31

[AC-tcl-line-vty0-31] set authentication password simple password1

```
Wrong # args: should be "set verName ?newValue?"
```

2) cli コマンドを設定し、再度 Comware コマンドを実行します。

[AC-tcl-linr-vty0-31] cli set authentication password simple password1

Radio view に移行するため、1 回の操作で複数の Comware コマンドを実行します。

方法 1:

[AC-tcl] cli "wlan ap ap1 model QX-W1020 ; radio 1"

[AC-tcl-wlan-ap-ap1-radio-1]

方法 2:

[AC-tcl] cli wlan ap ap1 model QX-W1020 ; cli radio 1

[AC-tcl- wlan-ap-ap1-radio-1]

10.1.2 tclquit

Syntax

tclquit

View

Tcl configuration view

定義済みユーザロール

network-admin

説明

tclquit コマンドは Tcl configuration view から user view に戻ります。

Tcl configuration view から user view に戻る場合 **quit** コマンドも使用可能です。

system view または Comware feature view に移行するために Comware コマンドを実行した後に上位レベルの view に戻る場合は、**quit** コマンドを使用します。

例

Tcl configuration view から user view に戻ります。

<AC-tcl> tclquit

<AC>

関連コマンド

tclsh

10.1.3 tclsh

Syntax

tclsh

View

User view

定義済みユーザロール

network-admin

説明

tclsh コマンドは user view から Tcl configuration view に移行します。

Tcl configuration view では以下のコマンドが実行可能です。

- すべての Tcl 8.5 コマンド。
- Comware コマンド。Tcl configuration view は user view と同等です。user view で使用される同じ方法で、Tcl configuration view で Comware コマンドを使用可能です。

user view に戻る場合 **quit** コマンドも使用可能です。

system view または Comware feature view に移行するために Comware コマンドを実行した後に上位レベルの view に戻る場合は、**quit** コマンドを使用します。

例

user view から Tcl configuration view に移行します。

<AC> tclsh

<AC-tcl>

関連コマンド

tclquit

目次

このセクションのページは **1-x-x** です。

11 章 Python の使用 11-1
11.1 Python コマンド 11-1
11.1.1 python 11-1
11.1.2 python *filename* 11-1

11章 Python の使用

11.1 Pythonコマンド

11.1.1 python

Syntax

python

View

User view

定義済みユーザロール

network-admin

説明

python コマンドは Python シェルに移行します。

Python シェルでは以下が利用可能です。

- Python 2.7 コマンド
- Python 2.7 標準 API
- Comware 7 拡張 API

Python シェルから user view に戻るには、**exit()**を実行します。

例

Python シェルに移行します。

<AC> python

```
Python 2.7.3 (default, Dec 22 2012, 11:39:05)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>> exit()
```

<AC>

11.1.2 python *filename*

Syntax

python *filename* [*param*]

View

User view

定義済みユーザロール

network-admin

パラメータ

filename: 装置の記録媒体上にある Python スクリプト名を指定します。スクリプト名は大文字小文字を区別し、拡張子.py を使用している必要があります。拡張子.py は大文字小文字を区別しません。

param: スクリプトに渡されるパラメータを指定します。複数のパラメータを入力するには、区切り文字としてスペースを使用します。

説明

python *filename* コマンドは Python スクリプトを実行します。

コマンドで Python スクリプトが実行されている間はどの操作も実行できません。

スクリプト内のステートメントが構文の要求に合致していることを確認してください。ステートメントで構文エラーがあった場合、システムは Python スクリプトの実行を停止します。

スクリプトの実行中、システムは対話的なステートメントに対してはデフォルトを使用します。システムが手動入力で止まることはありません。

例

Python スクリプト test.py を実行します。

<AC> python test.py 1 2

```
['/ cfa0:/test.py', '1', '2']
```

目次

このセクションのページは **1-x-x** です。

12 章 ライセンス管理.....12-1
12.1 ライセンス管理設定コマンド.....12-1
12.1.1 display license.....12-1
12.1.2 display license device-id.....12-2
12.1.3 display license feature.....12-3
12.1.4 license activation-file install.....12-4
12.1.5 license activation-file uninstall.....12-5
12.1.6 license compress.....12-6

12章 ライセンス管理

12.1 ライセンス管理設定コマンド

12.1.1 display license

Syntax

display license [**activation-file**] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

activation-file: アクティベーションファイルの情報を表示します。

slot *slot-number*: IRF スタックのメンバ装置のメンバ ID を指定します。メンバ装置を指定しない場合、IRF スタックのすべてのメンバ装置のライセンス情報を表示します。

説明

display license コマンドは詳細ライセンス情報を表示します。

キーワードを指定せずに **display license** コマンドを使用した場合、すべてのライセンスに関する詳細情報を表示します。

例

詳細なライセンス情報を表示します。

<AC> display license

```
cfa0:/license/210235A1AMB145000027201505231709259248l.ak
Feature: APMGR
Product Description: Enhanced Access Controller License,128 APs,for Verticals,for
V7 Registered at: 2015-05-28 16:54:24
License Type: Trial (days restricted)
Trial Time Left (days): 30
Current State: In use
```

表 12-1 コマンド出力

フィールド	説明
Feature	機能名
Registered at	ライセンスインストール日時です。
License Type	有効期間によるライセンス種別です。 • **NA**—ライセンス種別を取得できません。 • **Permanent**—購入ライセンスは永続します。 • **Days restricted**—購入ライセンスは日数分（例：30日）有効です。 • **Trial (days restricted)**—トライアルライセンスは日数分有効です。
Trial Time Left (days)	トライアル期間の残り日数です。 本フィールドはトライアルライセンスで利用可能です。
Time Left (days)	ライセンスの残り日数です。 本フィールドは購入ライセンスで利用可能です。
Current State	ライセンス状態です。 • **In use**—ライセンスは使用中です。 • **Usable**—ライセンスは利用可能です。1つの機能に対して複数の期間限定ライセンスがインストールされている場合は、1つのライセンスのみが**In use**状態で、残りのライセンスは**Usable**状態です。 • **Expired**—ライセンスは期限切れしています。 • **Uninstalled**—ライセンスはアンインストールされています。 • **Unusable**—ライセンスは利用できません。 • **Invalid**—ライセンスは不正で、利用できません。
Uninstall Date	ライセンスのアンインストール日時 本フィールドはアンインストールされたライセンスで利用可能です。

12.1.2 display license device-id

Syntax

display license device-id slot *slot-number*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

slot *slot-number*: IRF スタックのメンバ装置のメンバ ID を指定します。

説明

display license device コマンドは装置の SN と DID 情報を表示します。

各装置は固有の SN および DID を有しています。装置のライセンスを登録する際、SN と DID を提供する必要があります。

DID は、ライセンスストレージを圧縮する **license compress** コマンドを実行するたびに変化します。ライセンス登録ごとに最新の DID を確認するには、**display license device-id** コマンドを実行します。

DID は.id ファイルとして生成されます。ライセンスセンタにライセンスを登録する際にファイルをアップロードします。

例

装置の SN と DID を表示します。

<AC> display license device-id

```
SN: 210235A0VSB011000029
SN CHECK_SUM: FFFFFFEA
Device ID: cfa0:/license/210235A0VSB011000029.did
```

12.1.3 display license feature

Syntax

display license feature

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display license feature コマンドは機能に関する要約ライセンス情報を表示します。

機能ライセンス情報は以下の情報を含みます。

- 装置がサポートするライセンスの総数
- インストールされているライセンスの数
- 装置で動作させるためにライセンスが必要な機能

例

機能の要約ライセンス情報を表示します。

<AC> display license feature

```
Total: 128  Usage: 2
Feature                      Licensed       State
APMGR                        Y              Trial
```

表 12-2 コマンド出力

フィールド	説明
Total	インストール可能なライセンスの総数です。
Usage	インストールされたライセンスの数です。
Feature	使用にあたりライセンスが必要な機能です。
Licensed	機能のライセンス状態です。 • **N**—ライセンスされていません。 • **Y**—ライセンスされています。
State	購入状態によるライセンス種別です。 • **Trial**—トライアルライセンス • **Formal**—購入ライセンス 機能がライセンスされていない場合、本フィールドにはハイフン（-）が表示されます。機能を使用するには、有効なライセンスファイルをインストールする必要があります。

12.1.4 license activation-file install

Syntax

license activation-file install *file-name* **slot** *slot-number*

View

System view

定義済みユーザロール

network-admin

パラメータ

file-name: ファイルパスを指定します。大文字小文字を区別する 1～127 文字の文字列です。アクティベーションファイルは有効かつ装置に保存される必要があります。

slot *slot-number*: IRF スタックのメンバ装置のメンバ ID を指定します。

説明

license activation-file install コマンドはライセンスアクティベーションファイルをインストールします。

ライセンスアクティベーションファイルを正しくインストールするために、機能ライセンスを登録するために使用される SN および DID が、装置の現行の SN および DID に合致していることを確認してください。

アクティベーションファイルは MPU ロックではなく装置ロックです。ライセンスされた機能は MPU 交換後もシステム全体で動作します。

例

アクティベーションファイル 20130812.ak を装置にインストールします。

<AC> system-view

[AC] license activation-file install cfa0:/license/20130812.ak

```
This operation might take some time. Do not perform any other operations until
the operation is completed or a failure message is displayed. Please wait...
```

関連コマンド

- **display license activation-file**
- **display license device-id**
- **license activation-file uninstall**

12.1.5 license activation-file uninstall

Syntax

license activation-file uninstall *file-name* **slot** *slot-number*

View

System view

定義済みユーザロール

network-admin

パラメータ

file-name: ファイルパスを指定します。大文字、小文字を区別する 1～127 文字の文字列です。

slot *slot-number*: IRF スタックのメンバ装置のメンバ ID を指定します。

説明

license activation-file uninstall コマンドはアクティベーションファイルをアンインストールします。

⚠ **注意**：

アンインストールを行ったライセンスは、同じ装置に再度適用することはできません。

すべてのアクティベーションファイルをアンインストールすると、その機能は装置上で動作しなくなります。

ライセンスを別の装置に移転したい場合は、期限切れしていないライセンスを無効にするために本コマンドを使用します。

アクティベーションファイルがアンインストールされると、システムはアンインストールキーを作成します。ライセンスを移転先に登録するには、移転先の SN、DID とこのキーを使用します。

トライアルライセンスは移転できません。トライアルライセンスのアクティベーションファイルをアンインストールした場合、アンインストールファイルは作成されません。

例

アクティベーションファイル cfa0:/license/20130812.ak を装置からアンインストールします。

<AC> system-view

[AC] license activation-file uninstall cfa0:/license/20130812.ak

```
This operation might take some time. Do not perform any other operations until
the operation is completed or a failure message is displayed. Please wait...
Uninstall file: cfa0:/license/20130812.uak
```

関連コマンド

- **display license activation-file**
- **license activation-file install**

12.1.6 license compress

Syntax

license compress slot *slot-number*

View

System view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number*: IRF スタックのメンバ装置のメンバ ID を指定します。

説明

license activation-file install コマンドはライセンスストレージを圧縮します。

⚠ **注意：**

DID はライセンスストレージが圧縮される度に変化します。圧縮を実行する前に、古い DID に基づいて生成されたすべてのアクティベーションファイルがインストールされていることを確認してください。圧縮後はそれらをインストールすることはできません。

ライセンスストレージ（**display license feature** コマンドを確認してください）の空きが十分でない場合に本コマンドを実行してください。

本コマンドは無効なライセンス（期限切れライセンス、アンインストールされたライセンス）およびアンインストールキーをライセンスストレージエリアから削除します。ライセンスストレージを圧縮する前に、アンインストールキーをバックアップしてください。

例

装置のライセンスストレージを圧縮します。

<AC> system-view

[AC] license compress

```
This command will delete all data relevant to uninstalled and expired keys/licenses,
including Uninstall keys, and create a new device ID for activation keys/files.
Make sure you have saved the Uninstall keys so you can apply for a new activation
key/file for the unexpired licenses that were covered by the uninstalled activation
keys/files.
```

Are you sure you want to continue? [Y/N]: Y

```
This operation might take some time. Do not perform any other operations until
the operation is completed or a failure message is displayed. Please wait...
```

QX-W2230AC アクセスコントローラ

コマンドマニュアル

2.WLAN

本マニュアルは以下に示す章で構成されています。

01-AP 管理

02-無線管理の設定

03-WLAN アクセスの設定

04-WLAN セキュリティ

05-WLAN 認証

06-WIPS の設定

07-WLAN QoS の設定

08-WLAN ローミングの設定

09-WLAN ロードバランスの設定

10-WLAN 無線リソースの計測の設定

11-チャネルスキャンの設定

12-バンドナビゲーションの設定

13-WLAN の高可用性の設定

14-WLAN RRM

15-WLAN IP スヌーピング

16-WLAN 最適化

17-WLAN 無線ロードバランス

18-WLAN メッシュの設定

19-コンフィグレーションプロファイルの設定

20-IoT 機能の設定

21-Web リダイレクトの設定

22-Hotspot 2.0 の設定

目次

このセクションのページは **2-x-x** です。

1 章 AP 管理 1-1
1.1 AP 管理コマンド 1-1
1.1.1 ac 1-1
1.1.2 ap 1-2
1.1.3 ap-model 1-3
1.1.4 bridge-aggregation 1-4
1.1.5 data-tunnel encryption 1-6
1.1.6 delete file 1-8
1.1.7 description (AP group view) 1-8
1.1.8 description (AP view) 1-9
1.1.9 description (AP's VLAN view) 1-10
1.1.10 display wlan ap 1-11
1.1.11 display wlan ap address 1-25
1.1.12 display wlan ap all feature capwap 1-26
1.1.13 display wlan ap connection 1-28
1.1.14 display wlan ap diagnostic-information 1-29
1.1.15 display wlan ap files 1-30
1.1.16 display wlan ap group-name 1-31
1.1.17 display wlan ap online-time 1-34
1.1.18 display wlan ap reboot-log 1-35
1.1.19 display wlan ap reboot-record 1-36
1.1.20 display wlan ap running-configuration 1-42
1.1.21 display wlan ap statistics association-failure-record 1-45
1.1.22 display wlan ap statistics image-download 1-46
1.1.23 display wlan ap statistics online-record 1-49
1.1.24 display wlan ap tunnel-down-record 1-50
1.1.25 display wlan ap-distribution 1-52
1.1.26 display wlan ap-distribution ap-name 1-53
1.1.27 display wlan ap-group 1-54
1.1.28 display wlan ap-model 1-55
1.1.29 display wlan tunnel latency ap name 1-57
1.1.30 dns domain 1-59
1.1.31 dns server 1-60
1.1.32 download file 1-61
1.1.33 echo-count 1-62
1.1.34 echo-interval 1-63

1.1.35 firmware-upgrade 1-64
1.1.36 fragment-size 1-65
1.1.37 gateway 1-66
1.1.38 gigabitethernet 1-67
1.1.39 hybrid-remote-ap 1-68
1.1.40 if-match ip 1-69
1.1.41 ip address 1-71
1.1.42 keepalive-interval 1-72
1.1.43 led-mode 1-72
1.1.44 mac-address(AP group view) 1-74
1.1.45 mac-address(AP view) 1-75
1.1.46 name 1-75
1.1.47 port access vlan 1-77
1.1.48 port hybrid pvid 1-78
1.1.49 port hybrid vlan 1-80
1.1.50 port-isolate enable 1-81
1.1.51 port link-aggregation group 1-83
1.1.52 port link-type 1-85
1.1.53 port trunk permit vlan 1-87
1.1.54 port trunk pvid 1-88
1.1.55 power-level default 1-90
1.1.56 priority 1-92
1.1.57 provision 1-93
1.1.58 provision auto-recovery 1-95
1.1.59 provision auto-update 1-96
1.1.60 qos priority 1-97
1.1.61 qos trust 1-99
1.1.62 remote-configuration 1-101
1.1.63 remote-configuration synchronize 1-102
1.1.64 reset wlan ap 1-104
1.1.65 reset wlan ap provision 1-105
1.1.66 reset wlan ap reboot-log 1-105
1.1.67 reset wlan tunnel latency ap 1-106
1.1.68 retransmit-count 1-107
1.1.69 retransmit-interval 1-108
1.1.70 save wlan ap provision 1-109
1.1.71 serial-id (AP group view) 1-111
1.1.72 serial-id (AP view) 1-112
1.1.73 smartrate-ethernet 1-112
1.1.74 snmp-agent trap enable wlan ap 1-113
1.1.75 snmp-agent trap enable wlan capwap 1-114
1.1.76 statistics-interval 1-115
1.1.77 tunnel encryption 1-116

1.1.78 tunnel latency-detect 1-117
1.1.79 usb 1-118
1.1.80 vlan 1-119
1.1.81 wlan ap 1-121
1.1.82 wlan apdb 1-123
1.1.83 wlan apdb file 1-124
1.1.84 wlan ap-group 1-125
1.1.85 wlan ap-image-deploy 1-126
1.1.86 wlan auto-ap enable 1-127
1.1.87 wlan auto-ap persistent 1-127
1.1.88 wlan auto-persistent enable 1-128
1.1.89 wlan capwap discovery-policy unicast 1-129
1.1.90 wlan detect-anomaly enable 1-130
1.1.91 wlan global-configuration 1-131
1.1.92 wlan image-load filepath 1-131
1.1.93 wlan re-group 1-132
1.1.94 wlan rename-ap 1-133
1.1.95 wlan save ap-configuration 1-134
1.1.96 wlan timezone-sync enable 1-135
1.1.97 wlan tcp mss 1-136

1章 AP 管理

1.1 AP管理コマンド

1.1.1 ac

Syntax

ac { **host-name** *hostname* | **ip** *ipv4-address* }

undo ac { **host-name** | **ip** [*ipv4-address*] }

デフォルト

AP provision view では、AP は AP group provision view で設定を使用します。

AP group provision view では、AP に AC は指定されていません。

View

AP provision view

AP group provision view

定義済みユーザロール

network-admin

パラメータ

host-name *host-name*: AC をホスト名で指定します。大文字、小文字を区別しない 1～253 文字です。文字列には、文字、数字、ハイフン（-）、アンダースコア（_）、ドット（.）を使用できます。

ip *ipv4-address*: AC の IPv4 アドレスを指定します。

説明

ac コマンドは AP に対して AC を指定します。

undo ac コマンドは指定された AC 情報を削除します。

最大 3 つの AC IPv4 アドレス、1 つのホスト名のみを設定できます。複数のホスト名を設定した場合、最新の設定が有効になります。

AP provision view の設定は、対象の AP にのみ有効です。AP group provision view の設定は、AP group 内のすべての AP に対して有効になります。

AP provision view の設定は、AP group provision view の設定よりも優先されます。

undo ac { **ip** [*ip-address*] }コマンドを使用する際に、*ip-address* を指定しない場合、すべての AC IPv4 アドレスが削除されます。

例

AP **ap1** に IP アドレスが 192.168.100.11 の AC を指定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] provision

[AC-wlan-ap-ap1-prvs] ac ip 192.168.100.11

AP group **group1** に IP アドレスが 192.168.100.11 の AC を指定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] provision

[AC-wlan-ap-group-group1-prvs] ac ip 192.168.100.11

1.1.2 ap

Syntax

ap *ap-name-list*

undo ap *ap-name-list*

デフォルト

AP 名による AP group ルールは作成されていません。

View

AP group view

定義済みユーザロール

network-admin

パラメータ

ap-name-list: スペースで区切られた最大 10 の AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

説明

ap コマンドは AP group ルールを作成します。

undo ap コマンドは AP group ルールを削除します。

このコマンドは、指定された AP が存在するかどうかを識別しません。

AP 名、シリアル ID、MAC アドレス、IP アドレスによる AP group ルールの優先順位は、降順になっています。AP が group ルールと一致しない場合、AP はデフォルトの AP group に追加されます。

AP group ルールがすでに AP group に存在する場合、このコマンドは AP group からルールを削除します。

デフォルトの AP group view でこのコマンドを実行することはできません。

例

AP 名で AP group ルールを作成するために、AP **ap1**、**ap2**、**ap3** を AP group **group1** に追加します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap ap1 ap2 ap3

関連コマンド

wlan ap-group

1.1.3 ap-model

Syntax

ap-model *ap-model*

undo ap-model *ap-model*

デフォルト

設定無し

View

AP group view

定義済みユーザロール

network-admin

パラメータ

ap-model: AP モデル名を指定します。

QX-W1010：QX-W1010 を指定します。

QX-W1020：QX-W1020 を指定します。

QX-W1030：QX-W1030 を指定します。

QX-W1110：QX-W1110 を指定します。

QX-W1120：QX-W1120 を指定します。

QX-W1130：QX-W1130 を指定します。

QX-W1210：QX-W1210 を指定します。

QX-W1230：QX-W1230 を指定します。

QX-W1240：QX-W1240 を指定します。

🕮 **メモ：**

QX-W1010 はソフトウェアバージョン 7.1.11 を含む以降のソフトウェアからサポートしています。
QX-W1130 はソフトウェアバージョン 7.2.27 を含む以降のソフトウェアからサポートしています。
QX-W1120 はソフトウェアバージョン 7.2.46 を含む以降のソフトウェアからサポートしています。
QX-W1110 はソフトウェアバージョン 7.2.55 を含む以降のソフトウェアからサポートしています。
QX-W1240 はソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。
QX-W1210 と QX-W1230 はソフトウェアバージョン 7.2.89 を含む以降のソフトウェアからサポートしています。

説明

ap-model コマンドは AP モデルを作成し、その view に移行します。

undo ap-model コマンドは AP モデルとその設定を削除します。

例

#AP グループ group1 に AP モデル QX-W1030 を作成します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1030

1.1.4 bridge-aggregation

🕮 **メモ：**

このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

bridge-aggregation *interface-number*

undo bridge-aggregation *interface-number*

デフォルト

AP view では、AP は AP group view の設定を使用します。

AP group view では、アグリゲートインタフェースは存在しません。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

interface-number: アグリゲートインタフェースの番号を指定します。

説明

bridge-aggregation コマンドはアグリゲートインタフェースを作成し、その view あるいは既存のアグリゲートインタフェース view に移行します。

Undo bridge-aggregation コマンドはアグリゲートインタフェースを削除します。

アグリゲートインタフェースを作成したとき、システムは自動的に同一番号のアグリゲーショングループを作成します。デフォルトのアグリゲーショングループはスタティックのアグリゲーションモードです。

アグリゲートインタフェースを削除するとアグリゲートグループも削除されます。同時にアグリゲーショングループのメンバポートがアグリゲーショングループから除外されます。

リモートコンフィグレーションシンクロナイゼーションを使用すると、オンラインのすべての AP に設定が同期されます。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 に対してアグリゲートインタフェース 1 を作成し、その view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] bridge-aggregation 1

[AC-wlan-ap-ap1-bridge-aggregation-1]

AP グループ group1 に対してアグリゲートインタフェース 1 を作成し、その view に移行します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] bridge-aggregation 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-bridge-aggregation-1]

関連コマンド

- **remote-configuration**
- **remote-configuration synchronize**

1.1.5 data-tunnel encryption

Syntax

data-tunnel encryption { **disable** | **enable** }

undo data-tunnel encryption

デフォルト

AP view：AP group view の設定を使用

AP group view：無効

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: CAPWAP データトンネル暗号化を無効にします。

enable: CAPWAP データトンネル暗号化を有効にします。

説明

🕮 **メモ：**

CAPWAP データトンネル暗号化には独自の証明書をしており、時刻の有効性を確認しています。CAPWAP トンネル暗号化を利用する場合は、事前に装置の時刻が正しく設定されているか確認してください。

data-tunnel encryption enable コマンドは CAPWAP データトンネル暗号化を有効にします。

data-tunnel encryption disable コマンドは CAPWAP データトンネル暗号化を無効にします。

undo data-tunnel encryption コマンドはデフォルトに戻します。

本コマンド適用時、CAPWAP トンネルが再接続されます。

本機能を有効にすると、AP は AC から初めて keepalive パケットを受信したとき、鍵を含む暗号化情報を CAPWAP トンネル経由で AC と交換します。交換後、AC と AP は CAPWAP データトンネル内で転送されたデータパケットを暗号化します。keepalive パケットは暗号化されません。

本機能を有効にする前に、CAPWAP 制御トンネル暗号化が有効になっていることを確認してください。AP view の設定は AP group view の設定より優先されます。

例

AP **ap1** に対して CAPWAP データトンネル暗号化を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] data-tunnel encryption enable

```
This operation will restart the AP. Continue? [Y/N]
```

APgroup **group1** の説明を設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] data-tunnel encryption enable

```
This operation will restart member APs that are not enabled with CAPWAP data tunnel
encryption. Continue? [Y/N]
```

関連コマンド

tunnel encryption

1.1.6 delete file

Syntax

delete file *filename*

View

AP view

定義済みユーザロール

network-admin

パラメータ

filename: ファイル名を 1～255 文字の文字列で指定します。

説明

delete file コマンドは AP からファイルを削除します。

このコマンドは、AP がマスタ AC と CAPWAP トンネルを確立した後でのみ有効です。

例

AP **ap1** から **startup.cfg** ファイルを削除します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] delete file startup.cfg

関連コマンド

- **display wlan ap files**
- **download file**

1.1.7 description (AP group view)

Syntax

description *text*

undo description

デフォルト

AP group には説明が設定されていません。

View

AP group view

定義済みユーザロール

network-admin

パラメータ

text: 1～64 文字で指定します。大文字、小文字を区別します。

説明

description コマンドは AP group の説明を設定します。

undo description コマンドは AP group の説明を削除します。

例

APgroup **group1** の説明を設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-ap-group-group1] description L3-office

関連コマンド

- **display wlan ap-group**
- **wlan ap-group**

1.1.8 description (AP view)

Syntax

description *text*

undo description

デフォルト

AP には説明が設定されていません。

View

AP view

定義済みユーザロール

network-admin

パラメータ

text: 1～64 文字で指定します。大文字、小文字を区別します。

説明

description コマンドは AP の説明を設定します。

undo description コマンドは AP の説明を削除します。

例

AP **ap1** の説明を設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-ap-ap1] description L3-office

関連コマンド

display wlan ap

1.1.9 description (AP's VLAN view)

Syntax

description *text*

undo description

デフォルト

AP's VLAN view では、VLAN は AP group's VLAN view で設定を使用します。

AP group's VLAN view では、VLAN の説明は **VLAN** *vlan-id* です。*vlan-id* 引数には、VLAN ID を 4 桁の形式で指定します。VLAN ID が 4 桁未満の場合、先頭にゼロが追加されます。たとえば VLAN 100 の場合、デフォルトの説明は **VLAN 0100** です。

View

AP's VLAN view

AP group's VLAN view

定義済みユーザロール

network-admin

パラメータ

text: 説明を指定します。大文字と小文字が区別される 1～255 文字の文字列です。

説明

🕮 **メモ**:

このコマンドのサポートは、AP モデルによって異なります。

---

description コマンドは AP VLAN の説明を設定します。

undo description コマンドはデフォルトに戻します。

VLAN を効率的に管理するには、機能や接続に基づいて説明を設定します。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

例

AP **ap1** の VLAN view で、VLAN 2 の説明を **sales-private** として設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] vlan 2

[AC-wlan-ap-ap1-vlan2] description sales-private

AP group1 の VLAN view で、VLAN 2 の説明を **sales-private** として設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] vlan 2

[AC-wlan-ap-group-1-vlan2] description sales-private

関連コマンド

remote-configuration

1.1.10 display wlan ap

🕮 **メモ**:

apid のパラメータは 7.2.56 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan ap { **all** | **apid** *ap-id* | **name** *ap-name* } [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

apid *ap-id*: AP を apid で指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

verbose: 詳細情報を表示します。

説明

display wlan ap コマンドは AP 情報を表示します。

例

すべての AP に関する情報を表示します。

<AC> display wlan ap all

```
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 48
Remaining APs: 47
Total AP licenses: 32
Remaining AP licenses: 31

                          AP information
 State : I = Idle,      J  = Join,      JA = JoinAck,    IL = ImageLoad
        C = Config,    DC = DataCheck,  R  = Run   M = Master,  B = Backup

AP name                    APID  State Model         Serial ID
ap1                        1     I     QX-W1020      210235A1BSC123000050
```

表 1-1 コマンド出力

フィールド	説明
Total number of APs	FITまたはAnchor-FIT APの総数です。
Total number of connected APs	接続されたFITまたはAnchor-FIT APの総数です。
Total number of connected manual APs	接続されている手動のFITまたはAnchor-FIT APの総数です。

フィールド	説明
Total number of connected auto APs	接続されている自動のFITまたはAnchor-FIT APの総数です。
Total number of connected common APs	接続されたFITまたはAnchor-FIT APの総数です。
Total number of connected WTUs	このフィールドは現在のソフトウェアではサポートしていません。
Total number of inside APs	接続されている内部APの総数です。内部APは、Anchor-ACモードでAPが機能するときに自動的に作成される手動APです。
Maximum supported APs	ACでサポートされるAPの最大数です。
Remaining APs	残りのAP数です。
Total AP licenses	APライセンスの総数です。
Remaining AP licenses	残りのAPライセンス数です。
APID	AC上のAPを一意に識別するためのIDです。
Stete	APの現在の状態を以下のように表示します。 • **I**－アイドル • **J**－ジョイン • **JA**－ジョイン確認 • **IL**－APがバージョンをダウンロードしています。 • **C**－APが初期設定をダウンロードしています。 • **DC**－APがデータをチェックしています。 • **R**－APが動作しています。これは、APとACがCAPWAPトンネルを正常に確立したことを示します。 • **R/M**－マスタCAPWAPトンネルが動作しています。これは、APとマスタACがCAPWAPトンネルを正常に確立したことを示します。 • **R/B**－バックアップCAPWAPトンネルが動作しています。これは、APとバックアップACがCAPWAPトンネルを正常に確立したことを示します。 • **M**－APはマスタACに接続されています。 • **B**－APはバックアップACに接続されています。
Serial ID	APのシリアルIDです。APのシリアルIDが設定されていない場合、このフィールドには**Not configured**が表示されます。

AP **ap1** に関する詳細情報を表示します。

<AC> display wlan ap name ap1 verbose

```
AP name                    : ap1
AP ID                      : 1
AP group name               : default-group
State                      : Run
Backup type                 : Master
Online time                 : 0 days 1 hours 25 minutes 12 seconds
System up time              : 0 days 2 hours 22 minutes 12 seconds
Model                      : QX-W1020
Region code                 : JP
Region code lock            : Disable
Serial ID                  : 219801A0CNC138011454
MAC address                 : 0AFB-423B-893C
IP address                 : 192.168.1.50
UDP control port number      : 18313
UDP data port number         : N/A
H/W version                : Ver.C
S/W version                : 7.1.0
Boot version               : 1.01
USB state                  : N/A
Power Level                : N/A
PowerInfo                  : N/A
Description                : wtp1
Priority                   : 4
Echo interval               : 10 seconds
Statistics report interval    : 50 seconds
Fragment size (data)         : 1500
Fragment size (control)      : 1450
MAC type                   : Local MAC & Split MAC
Tunnel mode                : Local Bridging & 802.3 Frame & Native Frame
Discovery type              : Static Configuration
Retransmission count         : 3
Retransmission interval      : 5 seconds
Firmware upgrade            : Enabled
Sent control packets         : 1
Received control packets     : 1
Echo requests              : 147
Lost echo responses          : 0
Average echo delay           : 3
Last reboot reason           : User soft reboot
Latest IP address           : 10.1.0.2
Tunnel down reason           : Request wait timer expired
Connection count            : 1
```

```
Backup Ipv4                : Not configured
Backup Ipv6                : Not configured
Tunnel encryption           : Disabled
LED mode                   : Normal
Remote configuration        : Enabled
Radio 1:
   Basic BSSID             : 0afb-42f6-3940
   Admin state             : Up
   Radio type              : 802.11ac
   Antenna type            : internal
   Client dot11ac-only      : Disabled
   Client dot11n-only       : Disabled
   Channel band-width       : 20/40/80MHz
   Active band-width        : 20/40/80MHz
   Secondary channel offset  : SCB
   Short GI for 20MHz       : Supported
   Short GI for 40MHz       : Supported
   Short GI for 80MHz       : Supported
   Short GI for 160MHz      : Not supported
   A-MSDU                  : Enabled
   A-MPDU                  : Enabled
   LDPC                    : Not Supported
   STBC                    : Supported
   Operational VHT-MCS Set:
      Mandatory            : Not configured
      Supported            : NSS1 0,1,2,3,4,5,6,7,8,9
                           NSS2 0,1,2,3,4,5,6,7,8,9
      Multicast            : Not configured
   Operational HT MCS Set:
      Mandatory            : Not configured
      Supported            : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                           10, 11, 12, 13, 14, 15
      Multicast            : Not configured
   Channel                 : 44(auto)
   Channel usage(%)         : 15
   Max power               : 20 dBm
   Operational rate:
      Mandatory            : 6, 12, 24 Mbps
      Multicast            : Auto
      Supported            : 9, 18, 36, 48, 54 Mbps
      Disabled             : Not configured
   Distance                : 1 km
   ANI                     : Enabled
```

```
    Fragmentation threshold   : 2346 bytes
    Beacon interval          : 100 TU
    Protection threshold     : 2346 bytes
    Long retry threshold     : 4
    Short retry threshold    : 7
    Maximum rx duration      : 2000 ms
    Noise Floor             : -102 dBm
    Smart antenna           : Enabled
    Smart antenna policy     : Auto
    Protection mode          : rts-cts
    Continuous mode          : N/A
    HT protection mode       : No protection
Radio 2:
    Basic BSSID             : 0afb-42f6-3950
    Admin state             : Down
    Radio type              : 802.11b
    Antenna type            : internal
    Client dot11n-only       : Disabled
    Channel band-width       : 20MHz
    Active band-width        : 20MHz
    Secondary channel offset  : SCN
    Short GI for 20MHz       : Supported
    Short GI for 40MHz       : Supported
    A-MSDU                  : Enabled
    A-MPDU                  : Enabled
    LDPC                    : Not Supported
    STBC                    : Supported
    Operational HT MCS Set:
       Mandatory            : Not configured
       Supported            : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                              10, 11, 12, 13, 14, 15
       Multicast            : Not configured
    Channel                 : 5(auto)
    Channel usage(%)         : 0
    Max power               : 20 dBm
    Preamble type            : Short
    Operational rate:
       Mandatory            : 1, 2, 5.5, 11 Mbps
       Multicast            : Auto
       Supported            : 6, 9, 12, 18, 24, 36, 48, 54 Mbps
       Disabled             : Not configured
    Distance                : 1 km
    ANI                     : Enabled
```

```
Fragmentation threshold   : 2346 bytes
Beacon interval          : 100 TU
Protection threshold      : 2346 bytes
Long retry threshold      : 4
Short retry threshold     : 7
Maximum rx duration       : 2000 ms
Noise Floor              : 0 dBm
Smart antenna            : Enabled
Smart antenna policy      : Auto
Protection mode          : rts-cts
Continuous mode          : N/A
HT protection mode        : No protection
```

表 1-2 コマンド出力

フィールド	説明
Stete	APの現在の状態を以下のように表示します。 ● **Idle**－アイドル ● **Join**－ジョイン ● **JoinAck**－ジョイン確認 ● **Image**－APがバージョンをダウンロードしています。 ● **Config**－APが初期設定をダウンロードしています。 ● **Data Check**－APがデータをチェックしています。 ● **Run**－APが動作しています。これは、APとACがCAPWAPトンネルを正常に確立したことを示します。 ● **R/M**－マスタCAPWAPトンネルが動作しています。これは、APとマスタACがCAPWAPトンネルを正常に確立したことを示します。 ● **R/B**－バックアップCAPWAPトンネルが動作しています。これは、APとバックアップACがCAPWAPトンネルを正常に確立したことを示します。 ● **M**－APはマスタACに接続されています。 ● **B**－APはバックアップACに接続されています。
Backup type	CAPWAPトンネルタイプです。 ● **Idle**－APはACとCAPWAPトンネルを確立していません。 ● **Master**－APとマスタAC間に確立されたCAPWAPトンネルです。 ● **Backup**－APとバックアップAC間に確立されたCAPWAPトンネルです。
Region code lock	● Enable ● Disable

フィールド	説明
Serial ID	APのシリアルIDです。APのシリアルIDが設定されていない場合、このフィールドには**Not configured**が表示されます。
MAC address	APのMACアドレスです。MACアドレスが設定されていない場合、このフィールドには**Not configured**が表示されます。
UDP control port number	CAPWAPコントロールトンネルを確立するためにAPによって使用されるポート番号です。
UDP data port number	CAPWAPデータトンネルを確立するためにAPによって使用されるポート番号です。
H/W version	APのハードウェアバージョンです。
S/W version	APのソフトウェアバージョンです。
USB state	USB 状態: ● Enabled. ● Disabled. USB状態の情報がない場合、このフィールドには**N/A**が表示されます。
Power Level	このフィールドは現在のソフトウェアバージョンではサポートされていません。 電力レベル: ● Low. ● Middle. ● High. 電力レベルが不明の場合、このフィールドには**N/A**が表示されます。
PowerInfo	電源情報
PoE status	このフィールドは現在のソフトウェアバージョンではサポートされていません。 各PIのPoE電源状態: ● Enabled. ● Disabled.
Description	APの説明です。説明が設定されていない場合、このフィールドには**Not configured**が表示されます。
Priority	ACに対するAP接続優先度です。
Fragment size (data)	CAPWAPデータパケットの最大フラグメントサイズです。
Fragment size (control)	CAPWAP制御パケットの最大フラグメントサイズです。
MAC type	AP-AC接続のMACタイプです。

フィールド	説明
	• **Local MAC**－APはACにフレームを送信する前に802.3形式でカプセル化します。 • **Split MAC**－APはACにフレームを送信する前に802.11形式でカプセル化します。 • **Local & Split MAC**－APをACはフレームに送信する前に、フレームを802.3形式または802.11形式でカプセル化します。
Tunnel mode	サポートされているAPのトンネルモードです。 • **Local Bridging**－APはローカルブリッジングをサポートし、データをACに転送しません。 • **802.3 Frame**－APはフレームを802.3形式でカプセル化してACに送信します。 • **Native Frame**－APはフレームを802.11形式でカプセル化してACに送信します。 • **Local Bridging & 802.3 Frame**－APは、ローカルブリッジングモードと802.3フレームモードをサポートしています。 • **802.3 Frame & Native Frame**－APは、802.3フレームモードとネイティブフレームモードをサポートしています。 • **Local Bridging & Native Frame**－APはローカルブリッジモードとネイティブフレームモードをサポートしています。
Discovery type	APの検出タイプです。 • **Static Configuration**－APは手動で設定されたACのIPv4アドレスを使用します。 • **DHCP**－APはDHCPを介してACのIPアドレスを取得します。 • **DNS**－APはDNSを介してACのIPアドレスを取得します。 • **Unknown.**
Retransmission count	AC要求の再送試行回数です。
Retransmission interval	AC要求を再伝送する間隔です。
Firmware upgrade	APソフトウェアアップグレードです。 • Enable • Disable
Sent control packet	ACが**Run**状態となった後に送信されたパケットの数です。**Change State Event Response**パケットが含まれています。
Received control Packets	ACが**Run**状態となった後に受信したパケット数です。**Change State Event Response**パケットが含まれています。

フィールド	説明
Echo requests	実行状態でAPによって送信されたエコー要求の数です。
Lost echo responses	実行状態でAPによって受信されなかったエコー応答の数です。
Average echo delay	平均エコー遅延（ミリ秒）です。
Last reboot reason	APの最後の再起動理由： • 電源投入 • ハードリブート • ウォッチドッグによる再起動 • 不明な再起動 • ユーザによるソフトリブート • カーネル例外ソフトリブート • カーネルデッドループソフトリブート • 自動アップデートによるソフトリブート • 不明なソフトリブート • メモリ枯渇 • その他
Latest IP address	APによって最近使用されたIPアドレスです。
Tunnel down reason	CAPWAPトンネルがダウンする原因: • タイマの作成に失敗しました。 • 隣接デッドタイマが切れました。 • 要求待ちタイマの有効期限が切れました。 • データチェックタイマーの有効期限が切れました。 • データチャネルキープアライブメッセージの処理に失敗しました。 • 要求を処理できませんでした。 • APがリセットされました。 • APが削除されました。 • オンラインにできませんでした。 • シリアル番号が変更されました。 • MACアドレスが変更されました。 • APの数が上限を超えました。 • 実行状態中に結合要求されました。 • APコンテキストの作成に失敗しました。 • 失敗結果コードを受信しました。 • メッセージの再送信に失敗しました。

フィールド	説明
	● 画像ファイルのダウンロードに失敗しました。 ● イメージファイルが正常にダウンロードされました。 ● ファイル操作タイマの有効期限が切れました。 ● トンネルを追加できませんでした。 ● APからWTPトンネルダウンイベントを受信しました。 ● バックアップACがバックアップトンネルを閉じました。 ● マスタとバックアップトンネルの切り替えです。 ● 設定を継承できませんでした。 ● AP認証に失敗しました。 CAPWAPトンネルがダウンしなかった場合、このフィールドには**N/A**が表示されます。
Connection count	APがACに接続した回数です。次のいずれかの場合にクリアされます。 ● ACの再起動 ● APのシリアルIDの変更 **reset wlan ap**コマンドでは、接続した回数はクリアされません。
Backup Ipv4	バックアップACのIPv4アドレスです。バックアップACが指定されていない場合、このフィールドには**Not configured**が表示されます。
Backup ipv6	バックアップACのIPv6アドレスです。バックアップACが指定されていない場合、このフィールドには**Not configured**が表示されます。
Tunnel encryption	● Enable ● Disable
LED mode	LED点灯モードです。 ● **quiet**－すべてのLEDがオフです。 ● **awake**－すべてのLEDを1分毎に点灯します。 ● **always-on**－すべてのLEDは常にオンです。 ● **normal**－本モードでのLED点灯の仕方は、APモデルによって変わります。
Remote configuration	● Enabled. ● Disabled.
Basic BSSID	無線のMACアドレスです。APがACとのCAPWAPトンネルを確立していない場合、このフィールドにはN/Aが表示されます。
Admin state	無線の状態です。 ● Up ● Down

フィールド	説明

Radio type	ワイヤレスモードです。
	• 2.4 GHz
	  • 802.11b
	  • 802.11g
	  • 802.11n(2.4GHz)
	• 5 GHz
	  • 802.11a
	  • 802.11n(5GHz)
	  • 802.11ac
	  • 80.211ax

Client dot11ac-only	• **Enable**－802.11a/b/g/n/acクライアントを無線と関連付けることができます。 • **Disable**－802.11acクライアントだけを無線に関連付けることができます。
Client dot11n-only	• **Enable**－802.11a/b/g/n/ac/axクライアントを無線と関連付けることができます。 • **Disable**－802.11nまたは802.11ac/axクライアントだけを無線に関連付けることができます。
Client dot11ax-only	• **Enable**－802.11a/b/g/n/axクライアントを無線と関連付けることができます。 • **Disable**－802.11axクライアントだけを無線に関連付けることができます。
Channel band-width	チャネル帯域幅です。 • 20 MHz • 20 or 40 MHz • 20/40/80/160 MHz
Active band-width	実行中の無線帯域幅です。
Secondary channel offset	802.11nおよび802.11ac/ax無線モードのセカンダリチャネル情報です。 • **SCA(Second Channel Above)**－APは40 MHz帯域幅モードで動作し、セカンダリチャネルはプライマリチャネルよりも上にあります。 • **SCB(Second Channel Below)**－APは40 MHz帯域幅モードで動作し、セカンダリチャネルはプライマリチャネルよりも下にあります。 • **SCN**－APは40 MHz帯域幅モードでは動作しません。

フィールド	説明
Short GI for 20MHz	20 MHzモードで動作するときに無線がShort GIをサポートするかどうかを示します。
Short GI for 40MHz	40 MHzモードで動作するときに無線がShort GIをサポートするかどうかを示します。
Short GI for 80MHz	80 MHzモードで動作するときに無線がShort GIをサポートするかどうかを示します。
Short GI for 160MHz	160 MHzモードで動作するときに無線がShort GIをサポートするかどうかを示します。
A-MSDU	• Enable • Disable
A-MPDU	• Enable • Disable
LDPC	• Supported • Not Supported
STBC	• Supported • Not Supported
Operational VHT MCS Set	• **Supported**－サポートVHT MCSセット • **Mandatory**－必須VHT MCSセット • **Multicast**－マルチキャストVHT MCSセット
Operational HT MCS Set	• **Supported**－サポートMCSセット • **Mandatory**－必須MCSセット • **Multicast**－マルチキャストMCSセット
Operational HE MCS Set	• **Supported**－サポートHE MCSセット • **Mandatory**－必須HE MCSセット • **Multicast**－マルチキャストHE MCSセット
Channel	• 現在のチャネルがAPによって自動的に選択された最適なチャネルである場合、このフィールドには*Number*<auto>が表示されます。 • 現在のチャネルが手動で設定されている場合、このフィールドには*Number*が表示されます。 • 現在のチャネルがレーダー信号を避けるためにAPによって自動的に選択されたチャネルである場合、このフィールドには*Number*<avoid radar>と表示されます。
Max power	無線の最大送信電力です。
Preamble type	プリアンブルタイプです。 • Short

フィールド	説明
	• Long
Operational rate	• Mandatory • Supported • Multicast • Disable • Not configured
Distance	無線信号が到達できる最大距離です。
ANI	• Enable • Disable
Protection threshold	保護メカニズムを起動するために必要なフレーム長のしきい値です。
Long retry threshold	長さがRTSしきい値を超えたフレームの最大再送試行回数です。
Short retry threshold	長さがRTSしきい値を超えないフレームの最大再送試行回数です。
Maximum rx duration	フレームの最大バッファ持続時間です。
Smart antenna	• Enable • Disable
Smart antenna policy	• Auto • High availability • High throughput
Protection mode	競合回避モード: • cts-to-self. • rts-cts.
Continuous mode	連続モード設定： • Transmission rate. • MCS index. • NSS index. • VHT-MCS index. 連続モードが設定されていない場合、このフィールドには**N/A**が表示されます。
HT protection mode	802.11n保護モード: • No protection • APに関連付けられたクライアントと近接の無線装置は802.11nモードで動作しています。APに関連付けら

フィールド	説明
	れたクライアントは40MHz帯で動作しています。 • APに関連付けられたクライアントは802.11nモードで動作しています。APに関連付けられたクライアントは40MHz帯で動作しています。 • Non-member protection すべてのAPに関連付けられたクライアントは802.11nモードで動作しています。近接の無線装置は非802.11nモードで動作しています。 • 20 MHz protection APの無線は40MHz帯を使用します。APに関連付けられたクライアントと近接の無線装置は802.11nモードで動作しています。20MHzの帯域幅を持つ最低 1 つのクライアントがAPの無線と関連付けられています。 • Non-HT mixed 上記のいずれのモードにもあてはまらないときに使用するモードです。
MU-TxBF	• Enabled. • Disabled. このフィールドのサポートは、APモデルによって異なります。
SU-TxBF	• Enabled. • Disabled. このフィールドのサポートは、APモデルによって異なります。

1.1.11 display wlan ap address

Syntax

display wlan ap { **all** | **name** *ap-name* } **address**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

説明

display wlan ap address コマンドは AP アドレス情報を表示します。

例

すべての AP のアドレス情報を表示します。

<AC> display wlan ap all address

```
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of inside APs: 0
AP name                      IP address                MAC address
ap1                          1.1.1.5                   0afb-428f-fc6a
```

表 1-3 コマンド出力

フィールド	説明
AP name	APの名前です。
IP address	APのIPアドレスです。 オフラインAPの場合、このフィールドには N/A が表示されます。
MAC address	APのMACアドレスです。 オフラインAPの場合、このフィールドには N/A が表示されます。

1.1.12 display wlan ap all feature capwap

Syntax

display wlan ap all feature capwap

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan ap all feature capwap コマンドはCAPWAP機能の設定状態を表示します。

例

CAPWAP 機能の設定状態を表示します。

<AC> display wlan ap all feature capwap

```
AP name                  Upgrade   Encryption  Control-address   Switch-back
ap1                      Disabled Both         Disabled          Horizontal
```

表 1-4 コマンド出力

フィールド	説明
Upgrade	APソフトウェアアップグレードです。 ● Enabled ● Disabled
Encryption	CAPWAPトンネルの暗号化です。 ● **Control**—制御トンネルの暗号化が有効です。 ● **Data**—データトンネルの暗号化が有効です。 ● **Both**—制御、データの両方のトンネルの暗号化が有効です。 ● **Disabled**—制御、データの両方のトンネルの暗号化が無効です。
Control-address	ACの再検出です。 ● Enabled. ● Disabled.

1.1.13 display wlan ap connection

🕮 **メモ**:

このコマンドの書式は、ソフトウェアバージョンにより異なります。

Syntax

ソフトウェアバージョン 7.1.13 を含む以前のソフトウェア：

display wlan ap connection record { **all** | **name** *ap-name* }

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェア：

display wlan ap { **all** | **name** *ap-name* } **connection-record**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

説明

display wlan ap connection コマンドは AC 上に AP 接続レコードを表示します。

例

AC 上のすべての AP 接続レコードを表示します。

<AC> display wlan ap connection record all

```
AP name                    IP address    State     Time
ap1                        2001::3       Run       05-06 09:47:44
ap2                        2001::5       Run       05-06 09:50:38
```

表 1-5 コマンド出力

フィールド	説明
State	APの現在の状態: ● Idle－アイドル状態です。 ● Run－CAPWAPトンネルが動作しています。これは、APとACがCAPWAPトンネルを正常に確立したことを示します。
Time	APがACとCAPWAPトンネルを確立した直近の時間です。

1.1.14 display wlan ap diagnostic-information

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.52 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan ap name *ap-name* **diagnostic-information**

View

すべての view

定義済みユーザロール

network-admin

パラメータ

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan ap diagnostic-information コマンドは、AC で管理している AP の診断情報を取得します。

取得した診断情報のファイルは、”apdiag_(apname).tar.gz”として、”apdiag”ディレクトリに保存されます。このコマンドを複数回実行した場合、”apdiag”ディレクトリ内の診断情報ファイルは、最後に実行した際のファイルに上書きされます。

例

AP **ap1** のダイアグ情報を取得します。

<AC> display wlan ap name ap1 diagnostic-information

```
begin to collect apdiag_ap1.tar.gz
save to cfa0:/apdiag/apdiag_ap1.tar.gz successfully.
```

1.1.15 display wlan ap files

> 🕮 **メモ：**
> このコマンドの書式は、ソフトウェアバージョンにより異なります。

Syntax

ソフトウェアバージョン 7.1.13 を含む以前のソフトウェア：

display wlan ap files name *ap-name*

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェア：

display wlan ap name *ap-name* **files**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

説明

display wlan ap files コマンドは AP 上のファイルおよびファイルフォルダに関する情報を表示します。

例

AP **ap1** のファイルとファイルフォルダに関する情報を表示します。

<AC> display wlan ap files name ap1

```
Directory of cfa0:
  0   13638656  wa4300-system.bin
```

```
  1   2573312   wa4300-boot.bin
131072 KB total (114208 KB free)
```

表 1-6 コマンド出力

フィールド	説明
0 13638656 xx.xx	ファイルまたはファイルのフォルダ情報: • 0－シリアル番号です。システムによって自動的に割り当てられます。 • 13638656－ファイルサイズ（バイト）です。ハイフン（-）はファイルフォルダを示します。 • xx.xx–ファイルまたはファイルフォルダの名前です。

関連コマンド

- **delete file**
- **download file**

1.1.16 display wlan ap group-name

🕮 **メモ**:

このコマンドは、ソフトウェアバージョン 7.2.79 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan ap group-name *ap-group-name*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap-group-name: AP グループ名を指定します。

説明

display wlan ap group-name コマンドは AP グループ内の AP に関する情報を表示します。

例

AP グループ **group1** のすべての AP に関する情報を表示します。

<AC> display wlan ap group-name default-group

```
Total number of APs: 2
Total number of online APs: 2

                          AP information
 State : I = Idle,      J  = Join,       JA = JoinAck,    IL = ImageLoad
        C = Config,    DC = DataCheck,  R  = Run,   M = Master,  B = Backup
 Online time : Day:Hour:Minute:Second

AP name  APID State  Model    Serial ID           Group name      Online time
Clients Mode  IP address
ap1      1    R/M    QX-W1110 219801A3DG8221E13131 default-group  0:15:31:36
  0      Fit   1.1.1.1
ap2      1    R/M    QX-W1120 219801A2EJ8218E01234 default-group  0:15:50:36
  0      Fit   1.1.1.2
```

表 1-7 コマンド出力

フィールド	説明
Total number of APs	FITまたはAnchor-FIT APの総数です。
Total number of online APs	オンラインのFITまたはAnchor-FIT APの合計数です。
APID	AC上のAPを一意に識別するためのIDです。
AP name	AP名です。

フィールド	説明
State	APの現在の状態を以下のように表示します。 ● Iーアイドル ● Jージョイン ● JAージョイン確認 ● ILーAPがバージョンをダウンロードしています。 ● Cー APが初期設定をダウンロードしています。 ● DCー APがデータをチェックしています。 ● Rー APが動作しています。これは、APとACがCAPWAPトンネルを正常に確立したことを示します。 ● R/Mーマスタ CAPWAPトンネルが動作しています。これは、APとマスタACがCAPWAPトンネルを正常に確立したことを示します。 ● R/Bーバックアップ CAPWAPトンネルが動作しています。これは、APとバックアップACがCAPWAPトンネルを正常に確立したことを示します。 ● Mー APはマスタACに接続されています。 ● Bー APはバックアップACに接続されています。 APのシリアルIDです。APのシリアルIDが設定されていない場合、このフィールドにはNot configuredが表示されます。
Model	APモデル名です。
Serial ID	APのシリアルIDです。APのシリアルIDが設定されていない場合、このフィールドには**Not configured**が表示されます。
Group Name	APグループ名です。
Online Time	APのオンライン期間です。
Clients	クライアント数です。
Mode	APモードです。
IP address	APのIPアドレスです。

1.1.17 display wlan ap online-time

🕮 メモ：

このコマンドの書式は、ソフトウェアバージョンにより異なります。

Syntax

ソフトウェアバージョン 7.1.13 を含む以前のソフトウェア：

display wlan ap online-time { **all** | **name** *ap-name* }

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェア：

display wlan ap { **all** | **name** *ap-name* } **online-time**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP を名前で指定します。大文字、小文字を区別しない 1～64 文字です。文字列には、文字、数字、アンダースコア（_）、ドット（.）、左カッコ（[）、右カッコ（]）、スラッシュ（/）、ハイフン（-）を使用できます。

説明

display wlan ap online-time コマンドは AP のオンライン期間を表示します。

例

すべての AP のオンライン期間を表示します。

<AC> display wlan ap online-time all

```
AP name          IP address            Time
ap1              1.1.1.2               0 days 0 hours 2 minutes 6 seconds
ap2              1.1.1.1               0 days 0 hours 5 minutes 6 seconds
ap3              1.1.1.6               0 days 0 hours 2 minutes 1 seconds
```

表 1-8 コマンド出力

フィールド	説明
IP address	APのIPアドレスです。

フィールド	説明
Time	APがオンラインになってからのAPのリアルタイムアソシエーション期間です。

1.1.18 display wlan ap reboot-log

🕮 **メモ：**

このコマンドの書式は、ソフトウェアバージョンにより異なります。

Syntax

ソフトウェアバージョン 7.1.13 を含む以前のソフトウェア：

display wlan ap reboot-log name *ap-name*

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェア：

display wlan ap name *ap-name* **reboot-log**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

説明

display wlan ap reboot-log コマンドは AP の再起動のログを表示します。

AP でシステムクラッシュが発生した場合、このコマンドを使用してクラッシュに関する詳細情報を表示できます。

このコマンドを使用するには、指定した AP が **Run** 状態であることを確認してください。

例

AP ap1 の再起動のログを表示します。

<AC> display wlan ap reboot-log name ap1

```
Debugging information is not available on the AC.
Downloading debugging data from AP. Continue? [Y/N]:y
Downloading debugging data. Please wait...
Please enter the same command again to view the log messages.
```

関連コマンド

reset wlan ap reboot-log

1.1.19 display wlan ap reboot-record

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.49 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan ap { **all** | **name** *ap-name* } **reboot-record**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan ap reboot-record コマンドは管理している AP の再起動履歴を表示します。

このコマンドは、オンライン状態の AP から再起動履歴を取得し、AC 上で表示できます。オンライン状態の AP から再起動履歴を取得するには、数分かかります。再起動履歴を

再度表示するには、AC が AP から再起動履歴を取得し終えるのを待ってから、再度 **display wlan ap reboot-record** コマンドを実行してください。

AP の再起動履歴は、直近で最大 10 件まで表示されます。

AP が AC から切断されると、AC は AP の再起動履歴を削除します。

デュアルリンクバックアップを使用した環境では、マスタ AC からのみ AP の再起動履歴を表示できます。

このコマンドを使用するには､指定したAPが**Run**状態であることを確認してください。

例

AP ap1 の再起動履歴を表示します。

<AC> dis wlan ap name ap1 reboot-record

```
******************************************************************************
AP Name : ap1
PowerOn BootTimes   : 76
Watchdog BootTimes  : 0
Software BootTimes  : 4781
Hardware BootTimes  : 1
MotherBoard BootTimes: 0
Backup BootTimes    : 0
SlotOut BootTimes   : 0
Current Boot Type   : Software-boot
Current Running Time: 120(s)
Running Time        : 77(d)12(h)
*** Boot History(Startup Time and Reason) ***
2021-12-08 15:36:46 User soft reboot
2021-01-10 06:22:04 User soft reboot(Stayed in idle state for a long time)
2021-01-10 06:12:00 User soft reboot(Stayed in idle state for a long time)
2021-01-10 06:01:56 User soft reboot(Stayed in idle state for a long time)
```

全ての AP の再起動履歴を表示します。

<AC> display wlan ap all reboot-record

```
******************************************************************************
Number of Online APs Supporting Displaying Reboot Records: 2
Number of APs from Which Reboot Records Have Been Obtained: 2
******************************************************************************
AP Name   : ap1
PowerOn BootTimes   : 70
Watchdog BootTimes  : 7
Software BootTimes   : 2939
Hardware BootTimes  : 0
MotherBoard BootTimes   : 0
Backup BootTimes  : 0
```

```
SlotOut BootTimes   : 0
Current Boot Type  : Poweron-boot
Current Running Time   : 480(s)
Running Time  : 90(d)7(h)
*** Boot History(Startup Time and Reason) ***
2021-09-10 20:46:36 Power on
2021-09-10 20:46:30 Power on
2021-09-10 20:46:51 Power on
2021-09-10 20:46:51 User soft reboot
2021-09-10 20:46:51 Power on
2021-09-10 20:46:51 User soft reboot(Stayed in idle state for a long time)
2021-09-10 20:46:51 Power on
2021-09-10 20:46:51 User soft reboot(Stayed in idle state for a long time)
2021-09-10 20:46:51 User soft reboot(Stayed in idle state for a long time)
2021-09-10 20:46:51 User soft reboot(Stayed in idle state for a long time)
**************************************************************************
AP Name   : ap2
PowerOn BootTimes   : 140
Watchdog BootTimes  : 6
Software BootTimes   : 2039
Hardware BootTimes  : 0
MotherBoard BootTimes   : 0
Backup BootTimes  : 0
SlotOut BootTimes   : 0
Current Boot Type  : Poweron-boot
Current Running Time   : 240(s)
Running Time  : 70(d)5(h)
*** Boot History(Startup Time and Reason) ***
2021-09-10 20:46:36 Power on
2021-09-10 20:46:30 Power on
2021-09-10 20:46:51 Power on
2021-09-10 20:46:51 User soft reboot
2021-09-10 20:46:51 Power on
2021-09-10 20:46:51 User soft reboot(Stayed in idle state for a long time)
2021-09-10 20:46:51 Power on
2021-09-10 20:46:51 User soft reboot(Stayed in idle state for a long time)
2021-09-10 20:46:51 User soft reboot(Stayed in idle state for a long time)
2021-09-10 20:46:51 User soft reboot(Stayed in idle state for a long time)
```

表 1-9 コマンド出力

フィールド	説明
Number of Online APs Supporting Displaying Reboot Records	再起動履歴の表示をサポートしているオンラインのAPの数です。
Number of APs from Which Reboot Records Have Been Obtained	再起動履歴の取得を終えたAPの数です。
AP Name	再起動履歴を取得したAP名です。
PowerOn BootTimes	Power onが原因で再起動した合計回数です。
Watchdog BootTimes	Watchdog rebootが原因で再起動した合計回数です。
Software BootTimes	soft rebootが原因で再起動した合計回数です。
Hardware BootTimes	Hard rebootが原因で再起動した合計回数です。
MotherBoard BootTimes	Master slotの合計再起動回数です。
Backup BootTimes	Standby slotの合計再起動回数です。
SlotOut BootTimes	Stanby slotが外れた合計回数です。
Current Boot Type	現在のBootタイプ。 • Unknown • Poweron-boot • Software-boot • Watchdog-boot • Hardware-boot • MotherBoard-boot • ExtendWatchdog-boot • Backup-boot • ExtendedModuleRemoved-boot
Current Running Time	直近のBootの動作時間です。
Running Time	合計の動作時間です。

フィールド	説明
Boot History	下記が表示されます。 原因： ● Power on ● Hard reboot ● Watchdog reboot ● User soft reboot ● Kernel exception soft reboot ● Kernel deadloop soft reboot ● DevHandShake soft reboot ● Lic overTime soft reboot ● Slave switch soft reboot ● IRF mergesoft reboot ● Auto update soft reboot ● Memory-exhausted reboot ● -Crypto self-test failed reboot

フィールド	説明
	サブカテゴリ： ● Reset by admin ● Image was downloaded successfully ● Stayed in idle state for a long time ● WTU reboot because of offline WT ● AP reset from Cloud ● Anomaly detected ● Inconsistent BSS states on AC and AP ● Inconsistent BSS states on AP and in drive ● Inconsistent radio states on AC and AP ● Inconsistent radio modes on AC and AP ● Inconsistent radio rates on AC and AP ● Inconsistent radio channels on AC and AP ● Inconsistent radio bandwidth on AC and AP ● Inconsistent radio interface states on AC and AP ● Inconsistent radio states on AP and in drive ● Inconsistent radio modes on AP and in drive ● Inconsistent radio channels on AP and in drive ● Inconsistent radio bandwidth on AP and in drive ● Anchor AC detected another anchor AC with smaller MAC address and switched its role to AP ● Anchor AC received a discovery response and switched its role to AP ● Anchor AP failed to detect other anchor ACs or ACs and switched its role to AC ● Anchor AC detected another anchor AC with higher priority and switched its role to AP ● Configure the anchor device as an AC ● Configure the anchor device as an AP ● Manually configure the AP to act as a fit AP ● Manually configure the AP to act as a fat AP ● Manually configure the inside AP to act as a fat AP ● Local AC image download ● Device role changed from common to local

フィールド	説明
	• Device role changed from local to common • Device role changed from common to central • Device role changed from central to common • WT version changed • Cannot process subslot insert event • Cannot send subslot insert event to next step for processing

1.1.20 display wlan ap running-configuration

🕮 **メモ**:

このコマンドの書式は、ソフトウェアバージョンにより異なります。

Syntax

ソフトウェアバージョン 7.1.13 を含む以前のソフトウェア：

display wlan ap running-configuration { **all** | **name** *ap-name* } [**verbose**]

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェア：

display wlan ap { **all** | **name** *ap-name* } **running-configuration** [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

verbose: 詳細情報を表示します。

説明

display wlan ap running-configuration コマンドは指定した AP またはすべての AP のランニングコンフィグレーションを表示します。

例

#すべての AP の詳細なランニングコンフィグレーションを表示します。

<AC> display wlan ap running-configuration all verbose

```
(i) -- Inherited from AP group
(g) -- Inherited from AP global-configuration

#
wlan ap ap1 model QX-W1020 id 5
  ap group name 1
  serial-id 210235A1BSC123000050
  region code 156
  echo interval 10 (i)
  retransmission count 3 (i)
  retransmission interval 5 (i)
  statistics interval 50 (i)
  jumbo frame 1500 (i)
  firmware update 1
  priority 4 (i)
…

  radio 1
    radio type 802.11ac (i)
    radio disable (i)
    channel auto<64> (i)
    channel unlock (i)
    max-power 11 (i)
    power unlock (i)
    distance 1 kilometer (i)
    ANI Enabled (i)
…

  radio 2
    radio type 802.11n(2.4GHz) (i)
    radio disable (i)
    channel auto<11> (i)
    channel unlock (i)
    max-power 15 (i)
    power unlock (i)
```

```
    distance 1 kilometer (i)
    ANI Enabled (i)
…

#
wlan ap ap2 model QX-W1020 id 6
  ap group name 2
  serialid
  region code 156
  echo interval 10 (i)
  retransmission count 3 (i)
  retransmission interval 5 (i)
  statistics interval 50 (i)
  jumbo frame 1500 (i)
  firmware update 1
  priority 4 (i)
…

  radio 1
    radio type 802.11ac (i)
    radio disable (i)
    channel auto<60> (i)
    channel unlock (i)
    max-power 11 (i)
    power unlock (i)
    distance 1 kilometer (i)
    ANI Enabled (i)
…

  radio 2
    radio type 802.11n(2.4GHz) (i)
    radio disable (i)
    channel auto<13> (i)
    channel unlock (i)
    max-power 15 (i)
    power unlock (i)
    distance 1 kilometer (i)
    ANI Enabled (i)
…
```

1.1.21 display wlan ap statistics association-failure-record

Syntax

display wlan ap statistics association-failure-record

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan ap statistics association-failure-record コマンドは AP の関連付けに失敗した記録を表示します。

例

AP の関連付けに失敗した記録を表示します。

<AC> display wlan ap statistics association-failure-record

```
MAC address    AP ID   failed at          Reason
9a48-45ed-0300  12312   07-07/15:56:25      AP authentication failed
```

表 1-10 コマンド出力

フィールド	説明
MAC address	APのMACアドレスです。
AP ID	AC上のAPを一意的に識別するAPのIDです。
Last failure at	APがACと関連付けられた最後の時間です。フォーマットはdate/hh:mm:ssです。

フィールド	説明
Reason	関連づけに失敗した理由です。 • メモリが十分でありません。 • APが存在しません。 • APのライセンスが足りません。 • MACアドレスが使用されています。 • APLBの追加に失敗しました。 • APが別のACを選択しました。 • ACでAPの最大数に到達しました。 • Run状態の加入要求を受信しました。 • APLBチェックに失敗しました。 • HA smoothのAPアクセスに拒否されました。 • AP認証に失敗しました。 • Auto APの作成に失敗しました。 • 手動APオンラインinfoチェックに失敗しました。 • インデックスの追加に失敗しました。 • APとACのバージョンがあっていません。 • 待ち要求タイマが終了しました。 • 失敗リザルトコードを受信しました。 • トンネルの追加に失敗しました。 • APの設定が見つかりません。 • AP IDが一致していません。 • APの基本ランニングデータの追加に失敗しました。

1.1.22 display wlan ap statistics image-download

Syntax

display wlan ap statistics image-download [failed | in-progress | succeeded]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

failed: イメージのダウンロードに失敗した AP を表示します。

in-progress: イメージをダウンロード中の AP を表示します。

succeeded: イメージのダウンロードが成功した AP を表示します。

説明

display wlan ap statistics image-download コマンドは AP イメージのダウンロード情報を表示します。

パラメータを指定しない場合、AP イメージのダウンロードに関する簡易情報を表示します。

例

#AP イメージのダウンロードに関する簡易情報を表示します。

<AC> display wlan ap statistics image-download

```
Completed : 50%
Time consumed : xxd hh:mm:ss
AP count:
 Total to download : 300
 Succeeded : 152
 In-progress : 140
 Failed : 8
```

表 1-11 コマンド出力

フィールド	説明
Completed	イメージのダウンロードが完了したAPの割合です。
Time consumed	イメージのダウンロードにかかった時間です。
Total to download	ソフトウェアを更新する必要があるAPの合計数です。
Succeeded	イメージのダウンロードに成功したAPの数です。
In-progress	イメージをダウンロード中のAPの数です。
Failed	イメージのダウンロードに失敗したAPの数。

#AP イメージをダウンロード中の AP を表示します。

<AC> display wlan ap statistics image-download in-progress

```
AP name                    Time consumed
ap6                            xxd 00:45:11
ap7                            N/A
ap8                            xxd 00:14:05
ap9                            xxd 01:16:09
....
------More----
```

表 1-12 コマンド出力

フィールド	説明
Time consumed	イメージのダウンロードにかかった時間です。 イメージをダウンロードしていない場合、このフィールドにはN/Aと表示されます。

#AP イメージのダウンロードに失敗した AP を表示します。

<AC> display wlan ap statistics image-download in-progress

```
AP name                  Failure reason
ap1                      Tunnel down
ap2                      AP memory not enough
ap3                      Image file does not exist
ap5                      Others
....
------More----
```

表 1-13 コマンド出力

フィールド	説明
Failure reason	イメージのダウンロードに失敗した理由: ● トンネルがダウンしました。 ● APのメモリが不足しています。 ● イメージファイルが存在しません。 ● 再送信に失敗しました。 ● その他。

#AP イメージのダウンロードが成功した AP を表示します。

<AC> display wlan ap statistics image-download succeeded

```
AP name                  Version              Download at
ap1                      7.2.59               11-25 01:10:15
ap2                      7.2.59               11-25 01:12:34
ap3                      7.2.59               11-25 01:14:21
ap5                      7.2.59               11-25 01:16:45
....
------More----
```

表 1-14 コマンド出力

フィールド	説明
Version	APイメージのソフトウェアバージョンです。

フィールド	説明
Download at	APイメージのダウンロードが成功した日時です。

1.1.23 display wlan ap statistics online-record

Syntax

display wlan ap statistics online-record [**datetime** *date time*] [**count** *count*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

time *date time*: オンライン AP を記録する時間を指定します。*date* パラメータは YYYY/MM/DD あるいは MM/DD/YYYY のフォーマットです。YYYY パラメータの設定範囲は 2000～2035 です。MM パラメータの設定範囲は 1～12 です。DD パラメータは月を記載します。time パラメータは hh:mm のフォーマットです。hh パラメータの設定範囲は 0～23 です。mm パラメータの設定範囲は 0～59 です。パラメータを指定しない場合、降順で最近の 7 日のオンライン AP 数についての統計情報を表示します。

count *count*: オンライン AP 数を指定します。設定範囲は 1～256 です。指定しない場合、10 のオンライン AP 数の記録を表示します。

説明

display wlan ap statistics online-record コマンドはオンライン AP 数の記録を表示します。

オンライン AP 数の記録は 1 分の間隔で 1 つずつ表示されます。コマンドは最近の 7 日で生成された記録を表示します。*time* パラメータを指定した場合、指定した時間から生成された記録を表示します。

例

2017/10/11 10:25 後に生成されたオンライン AP 数の記録を 11 表示します。

<AC> display wlan ap statistics online-record time 2017/10/11 10:16:11 count 11

```
Time                 Manual APs      Auto APs       Total       Total delta
2017-10-11 10:16:00    20              10            30          -2
2017-10-11 10:17:00    22              10            32          +6
2017-10-11 10:18:00    16              10            26          0
2017-10-11 10:19:00    16              10            26          0
```

```
2017-10-11 10:20:00    16            10            26          0
2017-10-11 10:21:00    16            10            26          0
2017-10-11 10:22:00    16            10            26          0
2017-10-11 10:23:00    16            10            26          0
2017-10-11 10:24:00    16            10            26          0
2017-10-11 10:25:00    16            10            26          0
2017-10-11 10:26:00    16            10            26          0
```

表 1-15 コマンド出力

フィールド	説明
Time	記録が生成された日時です。
Manual APs	オンライン手動AP数です。
Auto APs	オンラインauto AP数です。
Total	オンラインAPの総数です。
Total delta	最後の1分での数の差分です。

1.1.24 display wlan ap tunnel-down-record

Syntax

display wlan ap tunnel-down-record

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan ap tunnel-down-record コマンドは CAPWAP トンネルダウンレコードを表示します。

例

CAPWAP トンネルダウンレコードを表示します。

<AC> display wlan ap tunnel-down-record

```
AP ID   AP name        Tunnel down at       Tunnel down reason
12321  9a48-45ed-0300   2017-07-07/15:56:25   Processed join request in Run state
```

表 1-16 コマンド出力

フィールド	説明
AP ID	AC上のAPを一意的に識別するAPのIDです。
AP name	APの名前です。
Tunnel down at	APとAC間のCAPWAPトンネルがダウンした時刻です。形式は、date / hh：mm：ssです。
Tunnel down reason	CAPWAPトンネルダウン理由: • タイマの作成に失敗しました。 • 近隣デッドタイマが期限切れになりました。 • 要求待ちタイマの有効期限が切れました。 • データチェックタイマーの有効期限が切れました。 • キープアライブメッセージの処理に失敗しました。 • 要求の処理に失敗しました。 • APはadminによってリセットされました。 • APはCloudTunnelによってリセットされました。 • APが削除されました。 • オンラインにできませんでした。 • シリアル番号が変更されました。 • MACアドレスが変更されました。 • AC最大能力を超過しました。 • 実行状態中に結合要求されました。 • APコンテキストの作成に失敗しました。 • 失敗結果コードを受信しました。 • メッセージの再送信に失敗しました。 • イメージファイルのダウンロードに失敗しました。 • イメージファイルが正常にダウンロードされました。 • ファイル操作タイマの有効期限が切れました。 • トンネルの追加に失敗しました。 • APからのWTPトンネルダウンイベントを受信しました。 • バックアップACがバックアップトンネルを閉じました。 • マスタとバックアップトンネルの切り替えです。 • 設定を継承できませんでした。 • AP認証に失敗しました。 • バックアップAPのアップグレードに失敗しました。 • ボードはアクティブではありません。 • APライセンスの欠如です。

1.1.25 display wlan ap-distribution

Syntax

display wlan ap-distribution all

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan ap-distribution コマンドは AC 用に接続された AP の配信情報を表示します。

例

AP の配信情報を表示します。

<AC> display wlan ap-distribution

```
Total number of APs: 1
                          AP information
 State : I = Idle,     J  = Join,      JA = JoinAck,    IL = ImageLoad
 C = Config,    DC = DataCheck,   R = Run,   M = Master,   B = Backup

AP name           APID   State   Model          Serial ID
722a-d561-0300      4     R/M    QX-W1020       210235A1BSC123000050
```

表 1-17 コマンド出力

フィールド	説明
APID	AC上のAPを一意的に識別するためのAPのIDです。
State	APの現在の状態: • I－Idle • J－Join • JA－Join acknowledge • IL－APがソフトウェアイメージバージョンをダウンロードしています。 • C－APが初期設定をダウンロードしています。 • DC－APがデータをチェックしています。 • R－CAPWAPトンネルが動作しています。これは、APとACがCAPWAPトンネルを正常に確立したことを示します。

フィールド	説明
	• R / Mーマスタ CAPWAP トンネルが動作しています。これは、APとマスタACがCAPWAPトンネルを正常に確立したことを示します。 • R / Bーバックアップ CAPWAP トンネルが動作しています。これは、APとバックアップACがCAPWAPトンネルを正常に確立したことを示します。 • Mー APがマスタACに接続されています。 • Bー APがバックアップACに接続されています。
Model	APモデル情報です。
Serial ID	APのシリアルIDです。APのシリアルIDが設定されていない場合、このフィールドには**Not configured**が表示されます。

1.1.26 display wlan ap-distribution ap-name

Syntax

display wlan ap-distribution ap-name *ap-name*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap-name: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

説明

display wlan ap-distribution ap-name コマンドは AP の接続位置を表示します。

例

AP **ap1** の接続位置の場所を表示します。

<AC> display wlan ap-distribution ap-name ap1

```
The AP is not in run state.
```

1.1.27 display wlan ap-group

Syntax

display wlan ap-group [**brief** | **name** *group-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

brief: すべての AP group に関する簡易情報を表示します。

name *group-name*: 指定した AP group に関する詳細情報を表示します。*group-name* 引数は、1～31 文字の大文字小文字を区別しない AP group の名前を表します。

説明

display wlan ap-group コマンドはすべての AP group または指定した AP group に関する情報を表示します。

パラメータを指定しない場合、このコマンドはすべての AP group に関する詳細情報を表示します。

例

すべての AP group に関する詳細情報を表示します。

[AC] display wlan ap-group

```
Total number of AP groups: 2
AP group name      : default-group
Description        : Not configured
AP model           : Not configured
APs                : Not configured

AP group name      : group1
Description        : abcd
AP model           : QX-W1020
AP grouping rules:
  AP name          : ap1, ap2
  Serial ID        : 219801A0CNC138011454
  MAC address      : 0AFB-423B-893C
```

```
  IPv4 address     : Not configured
  IPv6 address     : Not configured
APs              : ap1 (AP name)
```

AP group **group1** に関する詳細情報を表示します。

[AC] display wlan ap-group group1

```
AP group name      : group1
Description        : Not configured
AP model           : QX-W1020
AP grouping rules:
  AP name          : ap1, ap2
  Serial ID        : 219801A0CNC138011454
  MAC address      : 0AFB-423B-893C
  IPv4 address     : Not configured
  IPv6 address     : Not configured
APs              : ap1 (AP name)
```

すべての AP group に関する簡易情報を表示します。

<AC> display wlan ap-group brief

```
Total number of AP groups: 4
AP group name              Group ID  Member APs   Online APs
default-group              1         1            0
group1                     2         2006         1986
group2                     3         10           10
group3                     4         4            4
```

関連コマンド

wlan ap-group

1.1.28 display wlan ap-model

Syntax

display wlan ap-model { **all** | **name** *model-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP モデルを指定します。

name *model-name*: AP モデルの名前を指定します。

説明

display wlan ap-model コマンドは AP モデル情報を表示します。

例

AP モデル **QX-W1020** に関する情報を表示します。

<AC> display wlan ap-model name QX-W1020

```
AP model       : QX-W1020
Alias          : QX-W1020
Vendor name    : NEC
Vendor ID      : 25506
License weight  : 100
Radio count    : 2
 Radio 1:
  Mode         : 802.11a, 802.11an, 802.11ac
  Default mode  : 802.11ac
  BSS count    : 16
 Radio 2:
  Mode         : 802.11b, 802.11g, 802.11gn
  Default mode  : 802.11gn
  BSS count    : 16
Version Support List :
 Hardware Version Ver.A:
  Software Version        : 7.1.0
  Default Software Version : 7.1.0
  Image Name              : qx-w1000-fit.ipe
 Hardware Version Ver.B:
  Software Version        : 7.1.0
  Default Software Version : 7.1.0
  Image Name              : qx-w1000-fit.ipe
 Hardware Version Ver.C:
  Software Version        : 7.1.0
  Default Software Version : 7.1.0
  Image Name              : qx-w1000-fit.ipe
 Hardware Version Ver.D:
  Software Version        : 7.1.0
  Default Software Version : 7.1.0
  Image Name              : qx-w1000-fit.ipe
 Hardware Version Ver.E:
```

```
  Software Version        : 7.1.0
  Default Software Version : 7.1.0
  Image Name              : qx-w1000-fit.ipe
Hardware Version Ver.F:
  Software Version        : 7.1.0
  Default Software Version : 7.1.0
  Image Name              : qx-w1000-fit.ipe
```

表 1-18 コマンド出力

フィールド	説明
AP model	APモデル名です。
Alias	APモデルのエイリアスです。
License weight	APライセンスを使用したAPモデルの重み（パーセンテージ）です。
Radio count	無線の数です。
Mode	サポートされている無線タイプです。
Default mode	デフォルトの無線タイプです。
BSS count	無線がサポートするBSSの最大数です。
Software Version	APによって報告されたソフトウェアバージョンと比較するために使用されるAPのソフトウェアバージョンです。
Default Software Version	デフォルト値は、APDBに格納されているAPソフトウェアのバージョンです。
Image Name	APDBに格納されているAPソフトウェアのバージョンです。

1.1.29 display wlan tunnel latency ap name

🕮 **メモ：**

このコマンドの書式は、ソフトウェアバージョンにより異なります。

Syntax

ソフトウェアバージョン 7.1.13 を含む以前のソフトウェア：

display wlan tunnel latency ap name *ap-name*

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェア：

display wlan ap name *ap-name* **tunnel latency**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap-name: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

説明

display wlan tunnel latency ap name コマンドは AP のトンネル待ち時間情報を表示します。

このコマンドを実行する前に、CAPWAP トンネル待ち時間検出が開始されていることを確認してください。

例

AP **ap1** のトンネル待ち時間情報を表示します。

<AC> display wlan tunnel latency ap name ap1

```
AP name                          : ap1
Tunnel latency                    : Enabled
Control link delay:
  Current delay                   : 1ms
  Maximum delay                   : 1ms
  Minimum delay                   : 1ms
Data link delay:
  Current delay                   : 1ms
  Maximum delay                   : 1ms
  Minimum delay                   : 1ms
```

表 1-19 コマンド出力

フィールド	説明
Tunnel latency	• Disable • Enable
Current delay	最新の遅延です。

関連コマンド

- **reset wlan tunnel latency ap**
- **tunnel latency-detect**

1.1.30 dns domain

Syntax

dns domain *domain-name*

undo dns domain

デフォルト

AP provision view では、AP は AP group provision view で設定を使用します。

AP group provision view では、AP にドメイン名が指定されていません。

View

AP provision view

AP group provision view

定義済みユーザロール

network-admin

パラメータ

domain-name: ドットで区切られた 1～253 文字の大文字と小文字を区別しないドメイン名を指定します。文字列には、文字、数字、ハイフン（-）、アンダースコア（_）を使用できます。

説明

dns domain コマンドは AP のドメイン名を指定します。

undo dns domain コマンドはデフォルトに戻します。

AP provision view の設定は、対象の AP にのみ有効です。AP group provision view の設定は、AP group 内のすべての AP で有効になります。

AP provision view の設定は、AP group provision view の設定よりも優先されます。

例

AP **ap1** のドメイン名を **com** に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] provision

[AC-wlan-ap-ap1-prvs] dns domain com

AP group **group1** の AP のドメイン名を **com** に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] provision

[AC-wlan-ap-group-group-prvs] dns domain com

関連コマンド

dns server

1.1.31 dns server

Syntax

dns server ip *ipv4-address*

undo dns server ip

デフォルト

AP provision view では、AP は AP group provision view で設定を使用します。

AP group provision view では、AP に DNS サーバが指定されていません。

View

AP provision view

AP group provision view

定義済みユーザロール

network-admin

パラメータ

ip *ipv4-address*: DNS サーバを IPv4 アドレスで指定します。有効な IP アドレスを指定してください。無効な IP アドレスには、ループバック IP アドレス、ダイレクトブロードキャストアドレス、クラス D IP アドレス、クラス E IP アドレス、IP アドレス 255.255.255.255、0.X.X.X 形式の IP アドレスが含まれます。

説明

dns server コマンドは AP の DNS サーバを指定します。

undo dns server コマンドはデフォルトに戻します。

各 view では、1 つの IPv4 アドレスしか指定できません。

AP provision view の設定は、対象の AP にのみ有効です。AP group provision view の設定は、AP group 内のすべての AP で有効になります。

AP provision view の設定は、AP group provision view の設定よりも優先されます。

例

AP **ap1** の DNS サーバの IP アドレスを **192.168.100.123** に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] provision

[AC-wlan-ap-ap1-prvs] dns server ip 192.168.100.123

AP group **group1** の AP の DNS サーバの IP アドレスを **192.168.100.123** に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] provision

[AC-wlan-ap-group-group-prvs] dns server ip 192.168.100.123

関連コマンド

dns domain

1.1.32 download file

Syntax

download file *filename*

View

AP view

定義済みユーザロール

network-admin

パラメータ

filename: イメージファイル名を 1～255 文字で指定します。

説明

download file コマンドはイメージファイルを AP にダウンロードします。

この機能は、デュアルリンクバックアップ環境では、マスタ AC でのみ実行可能です。デュアルリンクバックアップの詳細については、オペレーションマニュアルのセクション 2 *WLAN “デュアルリンクバックアップの設定”*を参照してください。

例

#イメージファイル **main.ipe** を AP **ap1** にダウンロードします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan‑ap-ap1] download file main.ipe

1.1.33 echo-count

Syntax

echo-count *count*

undo echo-count

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、エコー要求の送信試行の最大回数は 3 回です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

count: エコー要求の送信試行の最大回数を 3～60 の範囲で指定します。

説明

echo-count コマンドはエコー要求の送信試行の最大回数を設定します。

undo echo-interval コマンドはデフォルトに戻します。

AP は、指定されたエコーインターバルでエコー要求を AC に送信し、CAPWAP 制御トンネルが正しく動作しているかどうかを識別します。AC は、エコー応答を送信することによって応答します。AP がキープアライブ時間内にエコー応答を受信しない場合、AP は接続を終了します。AC がキープアライブ時間内にエコー要求を受信しない場合、AC は接続を終了します。キープアライブ時間は、エコー間隔にエコー要求の送信試行の最大回数を掛けたものです。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap3** のエコー要求送信試行の最大回数を 5 に設定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1020

[AC-wlan-ap-ap3] echo-count 5

AP group **group1** のエコー要求送信試行の最大回数を 5 に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] echo-count 5

1.1.34 echo-interval

Syntax

echo-interval *interval*

undo echo-interval

デフォルト

AP view は、AP group view の設定を使用します。

AP group view では、エコー要求を送信する間隔は 10 秒です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

interval: エコー要求を送信する間隔を 5～80 秒の範囲で指定します。

説明

echo-interval コマンドは AP が AC にエコー要求を送信する間隔を設定します。

undo echo-interval コマンドはデフォルトに戻します。

AP は、指定されたエコー間隔でエコー要求を AC に送信し、CAPWAP 制御トンネルが正しく動作しているかどうかを識別します。AC は、エコー応答を送信することによって応答します。AP から keepalive 時間内にエコー要求を受信しない場合、AC は接続を終了します。AP が keepalive 時間内にエコー応答を受信しない場合、AP は接続を終了します。keepalive 時間は、echo 間隔に **echo-count** *count* コマンドを使用して設定されたエコー要求送信の最大回数を掛けたエコー間隔です。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap3** のエコー間隔を 15 秒に設定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1020

[AC-wlan-ap-ap3] echo-interval 15

AP group **group1** の AP のエコー間隔を 15 秒に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] echo-interval 15

1.1.35 firmware-upgrade

Syntax

firmware-upgrade { **disable** | **enable** }

undo firmware-upgrade

デフォルト

AP view は、AP group view の設定を使用します。

AP group view は、global configuration view の設定を使用します。

global configuration view は、ソフトウェア更新機能が有効になっています。

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

disable: ソフトウェア更新機能を無効にします。

enable: ソフトウェア更新機能を有効にします。

説明

firmware-upgrade enable コマンドはソフトウェア更新機能を有効にします。

firmware-upgrade disable コマンドはソフトウェア更新機能を無効にします。

undo firmware-upgrade コマンドはデフォルトに戻します。

この機能により、AC は AP のソフトウェアバージョンが、CAPWAP トンネル確立中に AC に格納されているハードウェアバージョンおよびソフトウェアバージョンマッピングと一致するかどうかを調べることができます。

- 一致が見つかった場合、AC は AP との CAPWAP トンネルを確立します。

- 一致するものが見つからない場合、CAPWAP トンネルの設定は次のように行われます。

a) ACはAPにソフトウェアのバージョンの不一致を通知します。

b) 通知を受信した後、APはソフトウェアバージョンをACから要求し、次にソフトウェアをアップグレードしてACとCAPWAPトンネルを確立します。

この機能が無効の場合、AC は AP のソフトウェアバージョンを調べず、AP と CAPWAP トンネルを直接確立します。

AP view の設定は、AP group view の設定よりも優先されます。AP group view の設定は、グローバル設定 view の設定よりも優先されます。

例

AP **ap3** のソフトウェア更新機能を有効にします。

<AC> system-view

[AC] wlan ap ap3 model QX-W1020

[AC-wlan-ap-ap3] firmware-upgrade enable

AP group **group1** の AP のソフトウェア更新機能を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] firmware-upgrade enable

#ソフトウェア更新機能をグローバルに有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] firmware-upgrade enable

関連コマンド

wlan apdb

1.1.36 fragment-size

Syntax

fragment-size { **control** *control-size* | **data** *data-size* }

undo fragment-size { **control** | **data** }

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、CAPWAP 制御パケットとデータパケットの最大フラグメントサイズは、それぞれ 1450 バイトと 1500 バイトです。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

control *control-size*: CAPWAP 制御パケットの最大フラグメントサイズをバイト単位で指定します。*control-size* 引数の値の範囲は 1000～1450 です。

data *data-size*: CAPWAP データパケットの最大フラグメントサイズをバイト単位で指定します。*control-size* 引数の値の範囲は 1000～1748 です。

説明

fragment-size コマンドは CAPWAP 制御またはデータパケットの最大フラグメントサイズを設定します。

undo fragment-size コマンドは構成を削除します。

このコマンドは、AP がインターネット経由で AC に接続する場合、中間装置が AC と AP 間でパケットをドロップすることを防ぎます。

フラグメントサイズの最大変更は、オンライン AP で直ちに有効になります。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **AP1** の CAPWAP データパケットの最大フラグメントサイズを 1500 バイトに設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-ap-ap1] fragment-size data 1500

AP group **group1** の CAPWAP データパケットの最大フラグメントサイズを 1500 バイトに設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] fragment-size data 1500

1.1.37 gateway

Syntax

gateway ip *ipv4-address*

undo gateway ip

デフォルト

AP にゲートウェイが指定されていません。

View

AP provision view

定義済みユーザロール

network-admin

パラメータ

ip *ipv4-address*: ゲートウェイを IPv4 アドレスで指定します。有効な IP アドレスを指定してください。無効な IP アドレスには、ループバック IP アドレス、ダイレクトブロードキャストアドレス、クラス D IP アドレス、クラス E IP アドレス、IP アドレス 255.255.255.255、0.X.X.X 形式の IP アドレスが含まれます。

説明

gateway コマンドは AP のゲートウェイを指定します。

undo gateway コマンドはデフォルトに戻します。

1 つの IPv4 アドレスしか設定できません。

例

AP **ap1** のゲートウェイ IP アドレスを **192.168.100.1** に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] provision

[AC-wlan-ap-ap1-prvs] gateway ip 192.168.100.1

1.1.38 gigabitethernet

🕮 **メモ**:

このコマンドのサポートは、AP モデルによって異なります。

Syntax

gigabitethernet *interface-number*

View

AP view

AP group's AP model view

定義済みユーザロール

network-admin

パラメータ

interface-number: インタフェース番号を指定します。値の範囲は、AP モデルによって異なります。

説明

gigabitethernet コマンドは AP の GigabitEthernet interface view に移行します。

例

AP view から GigabitEthernet 1 の interface view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1]

AP group1 の AP モデル view から GigabitEthernet 1 の interface view に移行します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] gigabitethernet 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-gigabitethernet-1]

1.1.39 hybrid-remote-ap

Syntax

hybrid-remote-ap { **disable** | **enable** }

undo hybrid-remote-ap

デフォルト

AP view は、AP group view の設定を使用します。

AP group view では、リモート AP は無効です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: リモート AP 機能を無効にします。

enable: リモート AP 機能を有効にします。

説明

hybrid-remote-ap enable コマンドはリモート AP 機能を有効にします。

hybrid-remote-ap disable コマンドはリモート AP 機能を無効にします。

undo hybrid-remote-ap コマンドはデフォルトに戻します。

デフォルトでは、AP と AC 間のトンネルが切断された場合、AP はサービスの提供を停止します。この機能を有効にすると、AP はリモート AP として機能し、引き続きサービスを提供できます。

このコマンドは、ローカル転送モードで動作する AP でのみ有効です。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1** のリモート AP を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] hybrid-remote-ap enable

AP group **group1** 内の AP に対してリモート AP を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] hybrid-remote-ap enable

1.1.40 if-match ip

Syntax

if-match ip *ip-address* { *mask-length* | *mask* }

undo if-match ip [*ip-address* { *mask-length* | *mask* }]

デフォルト

IPv4 アドレスによる AP グループルールは設定されていません。

View

AP group view

定義済みユーザロール

network-admin

パラメータ

ip-address: ドット付き 10 進表記で IPv4 アドレスを指定します。

mask-length: マスクの長さを 1～31 の範囲で指定します。

mask: ドット付き 10 進表記でマスクを指定します。

説明

if-match ip コマンドは IPv4 アドレスによる AP グループルールを作成します。

undo if-match ip コマンドは IPv4 アドレスによる AP グループルールを削除します。

デフォルトの AP group view でこのコマンドを実行することはできません。

AP グループまたは異なる AP グループの IPv4 アドレスによる AP グループルールは、互いに重複することはできません。

AP グループに設定できる IPv4 アドレスによる AP グループルールの設定可能数はソフトウェアバージョンにより異なります。

ソフトウェアバージョン 7.2.85a を含む以前のソフトウェアでは、AP グループに最大 32 個ルールを設定できます。

ソフトウェアバージョン 7.2.89 を含む以降のソフトウェアでは、AP グループに最大 64 個のルールを設定できます。

AP 名、シリアル ID、MAC アドレス、IPv4 アドレスによる AP グループルールの優先度は降順になっています。AP グループルールと一致しない AP は、デフォルトの AP グループに追加されます。

undo if-match ip コマンドを IPv4 アドレス未指定で実行すると、AP グループに設定設定されている IPv4 アドレスによる AP グループルールをすべて削除します。

例

IP アドレスが **192.168.0.0/16** に属する AP を AP group **group1** に追加します。

<AC> system-view

[AC] wlan ap-group group1

[AC-ap-group-group1] if-match ip 192.168.0.0 16

1.1.41 ip address

Syntax

ip address *ip-address* { *mask* | *mask-length* }

undo ip address

デフォルト

AP の管理 VLAN インタフェースには IP アドレスが指定されていません。

View

AP provision view

定義済みユーザロール

network-admin

パラメータ

ip-address: ドット付き 10 進表記で IPv4 アドレスを指定します。

mask: ドット付き 10 進表記でマスクを指定します。

mask-length: マスクの長さを 1～31 の範囲で指定します。

説明

ip address コマンドは AP の管理 VLAN インタフェースの IPv4 アドレスを指定します。

undo ip address コマンドはデフォルトに戻します。

有効な IP アドレスを指定してください。無効な IP アドレスには、ループバック IP アドレス、ダイレクトブロードキャストアドレス、クラス D IP アドレス、クラス E IP アドレス、IP アドレス 255.255.255.255、0.X.X.X 形式の IP アドレスが含まれます。

AP の管理 VLAN インタフェースの IP アドレスは、次の IP アドレスと異なる必要があります。

- 別の AP の管理 VLAN インタフェースの IP アドレス
- 任意の AP の provision view で指定された AC IP アドレス

例

AP **ap1** の管理 VLAN インタフェースの IP アドレスを **10.1.1.1/24** に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] provision

[AC-wlan-ap-ap1-prvs] ip address 10.1.1.1 24

1.1.42 keepalive-interval

Syntax

keepalive-interval *interval*

undo keepalive-interval

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、データトンネルキープアライブ間隔は 10 秒です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

interval: AP が CAPWAP データトンネルを介してキープアライブパケットを送信する間隔を指定します。値の範囲は 1～255 秒です。

説明

keepalive-interval コマンドはデータトンネルキープアライブ間隔を設定します。

undo keepalive-interval コマンドはデフォルトに戻します。

例

AP **ap1** のデータトンネルキープアライブ間隔を 15 秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] keepalive-interval 15

AP group **1** のデータトンネルキープアライブ間隔を 15 秒に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-ap-group-1] keepalive-interval 15

1.1.43 led-mode

Syntax

led-mode { **always-on** | **awake** | **normal** | **quiet** }

undo led-mode

デフォルト

AP view は、AP group view の設定を使用します。

AP group view は、LED 点灯モードは **normal** です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

always-on: すべての LED を常に点灯させます。このキーワードのサポートは、AP モデルによって異なります。

awake: すべての LED を 1 分毎に点灯させます。このキーワードのサポートは、AP モデルによって異なります。

normal: ノーマルモードでは AP の作動状況を識別します。このモードでの LED の点滅方法は、AP モデルによって異なります。

quiet: すべての LED を消灯します。

説明

led-mode コマンドは LED 点灯モードを設定します。

undo led-mode コマンドはデフォルトに戻します。

AP group view で LED 点灯モードを awake または always-on に設定すると、指定された LED 照明モードをサポートするメンバ AP に対してのみ設定が有効になります。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1** の LED 点灯モードを **normal** に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] led-mode normal

AP group **g1** の AP に対して LED 点灯モードを **awake** に設定します。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] led-mode awake

1.1.44 mac-address(AP group view)

Syntax

mac-address *mac-address*

undo mac-address *mac-address*

デフォルト

MAC アドレスによる AP group ルールは設定されていません。

View

AP group view

定義済みユーザロール

network-admin

パラメータ

mac-address: AP の MAC アドレスを指定します。

説明

mac-address コマンドは MAC アドレスによる AP group ルールを作成します。

undo mac-address コマンドは MAC アドレスによる AP group ルールを削除します。

このコマンドは、指定された AP が存在するかどうかを識別しません。

複数の AP group ルールを MAC アドレスで設定できます。

AP 名、シリアル ID、MAC アドレス、IP アドレスによる AP group ルールの優先度は降順になっています。AP が group ルールと一致しない場合、AP はデフォルトの AP group に追加されます。

AP group ルールがすでに AP group に存在する場合、このコマンドは AP group からルールを削除します。

デフォルトの AP group の view でこのコマンドを実行することはできません。

例

AP group **group1** の MAC アドレスで AP group ルールを作成します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] mac-address 0AC1-F9B2-B1C2

関連コマンド

wlan ap-group

1.1.45 mac-address(AP view)

Syntax

mac-address *mac-address*

undo mac-address

デフォルト

AP には MAC アドレスは指定されていません。

View

AP view

定義済みユーザロール

network-admin

パラメータ

mac-address: AP の MAC アドレスを H-H-H 形式で指定します。

説明

mac-address コマンドは AP の MAC アドレスを指定します。

undo mac-address コマンドはデフォルトに戻します。

AP が AC と CAPWAP トンネルを確立している場合、AP の MAC アドレスを変更または削除すると CAPWAP トンネルが終了します。その後、AP は AC と CAPWAP トンネルを再確立します。

例

AP **ap1** の MAC アドレスを **0001-0000-0000** に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] mac-address 0001-0000-0000

1.1.46 name

🕮 **メモ**:

このコマンドのサポートは、AP モデルによって異なります。

Syntax

name *text*

undo name

デフォルト

AP's VLAN view では、VLAN は AP group's VLAN view で設定を使用します。

AP group's VLAN view では、VLAN の名前は **VLAN** *vlan-id* です。*vlan-id* 引数には、VLAN ID を 4 桁の形式で指定します。VLAN ID が 4 桁未満の場合、先行ゼロが追加されます。たとえば、VLAN 100 の名前は **VLAN 0100** です。

View

AP's VLAN view

AP group's VLAN view

定義済みユーザロール

network-admin

パラメータ

text: VLAN 名を指定します。大文字と小文字が区別される 1～32 文字の文字列です。

説明

name コマンドは AP の VLAN に名前を割り当てます。

undo name コマンドはデフォルトに戻します。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP's VLAN view の設定は、AP group's VLAN view の設定よりも優先されます。

例

AP **ap1** の VLAN 2 の名前に **test vlan** を割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] vlan 2

[AC-wlan-ap-ap1-vlan2] name test vlan

AP group **1** のすべての AP の VLAN 2 の名前に **test vlan** を割り当てます。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] vlan 2

[AC-wlan-ap-group-1-vlan2] name test vlan

関連コマンド

remote-configuration

1.1.47 port access vlan

🕮 メモ：

このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

port access vlan *vlan-id*

undo port access vlan

デフォルト

AP の Ethernet interface view では、AP グループの Ethernet interface view の設定を使用します。

AP グループの Ethernet interface view では、AP 上のすべての access ポートが VLAN 1 に属します。

View

AP の Ethernet interface view

AP グループの Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: ID を 1～4094 の範囲で指定します。

説明

port access vlan コマンドは AP 上の access ポートを指定された VLAN に割り当てます。

undo port access vlan コマンドはデフォルトに戻します。

access ポートを VLAN に割り当てる前に、VLAN が作成されていることを確認してください。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP の Ethernet interface view の設定は、AP グループの Ethernet interface view の設定よりも優先されます。

例

AP **ap1** の Layer 2 Ethernet interface view で GigabitEthernet 1 を VLAN 3 に割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap3-gigabitethernet-1] port access vlan 3

AP グループ 1 のモデル **QX-W1020** の AP の Ethernet interface view で、GigabitEthernet 1 を VLAN 3 に割り当てます。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port access vlan 3

関連コマンド

remote-configuration

1.1.48 port hybrid pvid

🕮 **メモ**:

このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

デフォルト

AP の Ethernet interface view では、hybrid ポートは AP グループの Ethernet interface view の設定を使用します。

AP グループの Ethernet interface view では、hybrid ポートの PVID は、リンクタイプがアクセスされているときにポートが属する VLAN の ID です。

View

AP の Ethernet interface view

AP グループの Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: ID を 1～4094 の範囲で指定します。

説明

port hybrid pvid コマンドは AP 上の hybrid ポートの PVID を設定します。

undo port hybrid pvid コマンドは AP の hybrid ポートの PVID を 1 に設定します。

存在しない VLAN を hybrid ポートの PVID として使用できます。**undo vlan** コマンドを使用して hybrid ポートの PVID を削除すると、ポートの PVID 設定は変更されません。

パケットを正しく送信するには、AP の hybrid ポートと AP に接続されたスイッチの hybrid ポートに同じ PVID を設定します。

hybrid ポートが PVID からパケットを送信できるようにするには、**port hybrid vlan** コマンドを使用して、hybrid ポートを PVID に割り当てる必要があります。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP の Ethernet interface view の設定は、AP グループの Ethernet interface view の設定よりも優先されます。

例

GigabitEthernet 1 を hybrid ポートとして設定し、AP **ap1** の Layer 2 Ethernet interface view で PVID を VLAN 100 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] port link-type hybrid

[AC-wlan-ap-ap1-gigabitethernet-1] port hybrid pvid vlan 100

GigabitEthernet 1 を hybrid ポートとして設定し、AP グループ 1 のモデル **QX-W1020** の Layer 2 Ethernet interface view で PVID を VLAN 100 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port link-type hybrid

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port hybrid pvid vlan 100

関連コマンド

- **port hybrid vlan**
- **port link-type**
- **remote-configuration**

1.1.49 port hybrid vlan

> 🕮 メモ：
>
> このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

デフォルト

AP の Ethernet interface view では、hybrid ポートは AP グループの Ethernet interface view の設定を使用します。

AP グループの Ethernet interface view では、hybrid ポートは、そのリンクタイプがアクセスされているときにポートが属する VLAN のタグなしメンバです。

View

AP の Ethernet interface view

AP グループの Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: 最大 10 個の VLAN 項目をスペースで区切って指定します。各項目は、VLAN ID または VLAN ID の範囲を *vlan-id1*～*vlan-id2* の形式で指定します。VLAN ID の値の範囲は 1～4094 です。*vlan-id2* 引数の値は、*vlan-id1* 引数の値よりも小さくすることはできません。指定された VLAN は、装置上にすでに存在している必要があります。

tagged: 指定された VLAN のタグ付きメンバとしてポートを設定します。VLAN のタグ付きメンバは、VLAN タグを削除せずに VLAN からパケットを送信します。

untagged: ポートを、指定された VLAN のタグなしメンバとして設定します。VLAN のタグなしメンバは、VLAN タグを削除した後、VLAN からパケットを送信します。

説明

port hybrid vlan コマンドは特定の VLAN に hybrid ポートを割り当てます。

undo port hybrid vlan コマンドは指定された VLAN から hybrid ポートを削除します。

hybrid ポートは、複数の VLAN を許可できます。hybrid ポートでこのコマンドを複数回実行すると、hybrid ポートは指定されたすべての VLAN を許可します。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP の Ethernet interface view の設定は、AP グループの Ethernet interface view の設定よりも優先されます。

例

AP ap1 の Layer 2 Ethernet interface view で、以下の作業を実行します。

1) GigabitEthernet 1 を hybrid ポートとして設定します。
2) VLAN 100、タグ付きメンバとして VLAN 2、VLAN 4、および VLAN 50 に割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] port link-type hybrid

[AC-wlan-ap-ap1-gigabitethernet-1] port hybrid vlan 2 4 50 to 100 tagged

AP グループ 1 のモデル **QX-W1020** の AP の Layer 2 Ethernet interface view では、以下の作業を行います。

1) GigabitEthernet 1 を hybrid ポートとして設定します。
2) VLAN 100、タグ付きメンバとして VLAN 2、VLAN 4、および VLAN 50 に割り当てます。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port link-type hybrid

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port hybrid vlan 2 4 50 to 100 tagged

関連コマンド

- **port link-type**
- **remote-configuration**

1.1.50 port-isolate enable

メモ:

このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

port-isolate { **enable** | **disable** }

undo port-isolate

デフォルト

AP の Ethernet interface view では、AP は AP グループの Ethernet interface view の設定を使用します。

AP グループの Ethernet interface view では、ポートアイソレーションは有効です。

AP の aggregate interface view では、AP は AP グループの aggregate interface view の設定を使用します。

AP グループの aggregate interface view では、ポートアイソレーションは有効です。

View

AP の Ethernet interface view

AP group の Ethernet interface view

AP の aggregate interface view

AP グループの aggregate interface view

定義済みユーザロール

network-admin

パラメータ

disable: ポートアイソレーションを無効にします。

enable: ポートアイソレーションを有効にします。

説明

port-isolate enable コマンドはポートアイソレーションを有効にします。

port-isolate disable コマンドはポートアイソレーションを無効にします。

undo port-isolate コマンドはデフォルトに戻します。

Ethernet interface view での設定は、そのインタフェースにのみ適用されます。

aggregate interface view での設定は、アグリゲートインタフェースとアグリゲーションメンバポートに適用されます。装置がアグリゲートインタフェースへの設定の適用に失敗した場合、装置はどのアグリゲーションメンバポートもアイソレーショングループに割り当てません。設定の適用失敗がアグリゲーションメンバポートで起きた場合、装置は失敗が起きたポートをスキップし、別のアグリゲーションメンバポートをアイソレーショングループに割り当てます。

リモートコンフィグレーションシンクロナイゼーションを使用すると、オンラインのすべての AP に設定が同期されます。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 の GigabitEthernet 1 でポートアイソレーションを有効にします。

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap3-gigabitethernet-1] port-isolate enable

AP グループ 1 のモデル **QX-W1020** の GigabitEthernet 1 でポートアイソレーションを有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port-isolate enable

AP ap1 のアグリゲートインタフェース Bridge-Aggregation 1 に対してポートアイソレーションを有効にします。

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] bridge-aggregation 1

[AC-wlan-ap-ap1-bridge-aggregation-1] port-isolate enable

AP グループ 1 のモデル **QX-W1020** のアグリゲートインタフェース Bridge-Aggregation 1 でポートアイソレーションを有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] bridge-aggregation 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-bridge-aggregation-1] port-isolate enable

関連コマンド

- **remote-configuration**
- **remote-configuration synchronize**

1.1.51 port link-aggregation group

🕮 **メモ：**

このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

port link-aggregation group *group-id*

undo port link-aggregation

デフォルト

AP の Ethernet interface view では、AP は AP グループの Ethernet interface view の設定を使用します。

AP グループの Ethernet interface view では、インタフェースはアグリゲーショングループに所属していません。

View

AP の Ethernet interface view

AP グループの Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

group-id: アグリゲーションインタフェースの番号でアグリゲーショングループを指定します。番号の範囲は装置のモデルにより異なります。

説明

port link-aggregation group コマンドはアグリゲーショングループにインタフェースを割り当てます。

undo port link-aggregation group コマンドはアグリゲーショングループからインタフェースを除外します。

1 つのアグリゲーショングループに割り当てられるイーサネットインタフェースは 1 つだけです。

アグリゲーショングループに参加すると、インタフェースはグループに設定された設定を引き継ぎます。

port link-aggregation group コマンドを実行する前に、指定したアグリゲーショグループが既に存在し、AP がアグリゲートインタフェースをサポートしていることを確認してください。

リモートコンフィグレーションシンクロナイゼーションを使用すると、オンラインのすべての AP に設定が同期されます。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 の GigabitEthernet 1 をアグリゲーショングループ 1 に割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] port link-aggregation group 1

AP グループ 1 のモデル **QX-W1020** の GigabitEthernet 1 をアグリゲーショングループ 1 に割り当てます。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port link-aggregation group 1

関連コマンド

- **remote-configuration**
- **remote-configuration synchronize**

1.1.52 port link-type

🕮 **メモ**：

このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

port link-type { **access** | **hybrid** | **trunk** }

undo port link-type

デフォルト

AP の Ethernet interface view では、イーサネットポートは AP グループの Ethernet interface view で設定を使用します。

AP グループの Ethernet interface view では、各イーサネットポートは access ポートです。

View

AP の Ethernet interface view

AP グループの Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

access: ポートリンクタイプを access に設定します。

hybrid: ポートリンクタイプを hybrid に設定します。

trunk: ポートリンクタイプを trunk に設定します。

説明

port link-type コマンドは AP 上のイーサネットポートのリンクタイプを設定します。

undo port link-type コマンドはデフォルトに戻します。

イーサネットポートのリンクタイプを trunk から hybrid へ、またはその逆に変更するには、まずリンクタイプを access に設定します。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP の Ethernet interface view の設定は、AP グループの Ethernet interface view の設定よりも優先されます。

例

AP **ap1** の Layer 2 Ethernet interface view で、GigabitEthernet 1 を trunk ポートとして設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] port link-type trunk

AP グループ 1 のモデル **QX-W1020** の AP の Layer 2 Ethernet interface view で、GigabitEthernet 1 を trunk ポートとして設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port link-type trunk

関連コマンド

remote-configuration

1.1.53 port trunk permit vlan

> 🕮 メモ：
>
> このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

port trunk permit vlan { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

デフォルト

AP の Ethernet interface view では、trunk ポートは AP グループの Ethernet interface view の設定を使用します。

AP グループの Ethernet interface view では、trunk ポートは VLAN 1 からのパケットだけを通過させます。

View

AP の Ethernet interface view

AP グループの Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: 最大 10 個の VLAN 項目をスペースで区切って指定します。各項目は、VLAN ID または VLAN ID の範囲を *vlan-id1*～*vlan-id2* の形式で指定します。VLAN ID の値の範囲は 1～4094 です。*vlan-id2* 引数の値は、*vlan-id1* 引数の値よりも小さくすることはできません。

all: すべての VLAN を指定します。

説明

port trunk permit vlan コマンドは指定された VLAN に trunk ポートを割り当てます。

undo port trunk permit vlan コマンドは指定された VLAN から trunk ポートを削除します。

trunk ポートは、複数の VLAN を許可できます。このコマンドを trunk ポート上で複数回実行すると、trunk ポートは指定されたすべての VLAN を許可します。

trunk ポートでは、PVID からのパケットだけがタグなしを通過できます。

許可されていない VLAN ユーザがポートを介して制限されたリソースにアクセスするのを防ぐには、**port trunk permit vlan all** コマンドを慎重に使用してください。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP の Ethernet interface view の設定は、AP グループの Ethernet interface view の設定よりも優先されます。

例

GigabitEthernet 1 を trunk ポートとして設定し、AP **ap1** の Layer 2 Ethernet interface view で VLAN 100、VLAN 2、VLAN 4、および VLAN 50 に割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] port link-type trunk

[AC-wlan-ap-ap1-gigabitethernet-1] port trunk permit vlan 2 4 50 to 100

GigabitEthernet 1 を trunk ポートとして設定し、AP グループ 1 のモデル **QX-W1020** の AP の Ethernet interface view で VLAN 100、VLAN 2、VLAN 4、および VLAN 50 に割り当てます。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port link-type trunk

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port trunk permit vlan 2 4 50 to 100

関連コマンド

- **port link-type**
- **remote-configuration**

1.1.54 port trunk pvid

🕮 **メモ：**

このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

デフォルト

AP の Ethernet interface view では、trunk ポートは AP グループの Ethernet interface view の設定を使用します。

AP グループの Ethernet interface view では、trunk ポートの PVID は VLAN 1 です。

View

AP の Ethernet interface view

AP グループの Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: ID を 1～4094 の範囲で指定します。

説明

port trunk pvid コマンドは AP 上の trunk ポートの PVID を設定します。

undo port trunk pvid コマンドはデフォルトに戻します。

存在しない VLAN を trunk ポートの PVID として使用できます。**undo vlan** コマンドを使用して trunk ポートの PVID を削除すると、ポートの PVID 設定は変更されません。

パケットを正しく送信するには、AP の hybrid ポートと AP に接続されたスイッチの hybrid ポートに同じ PVID を設定します。

trunk ポートが PVID からパケットを送信できるようにするには、**port trunk permit vlan** コマンドを使用して、trunk ポートを PVID に割り当てる必要があります。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP の Ethernet interface view の設定は、AP グループの Ethernet interface view の設定よりも優先されます。

例

AP **ap1** の Layer 2 Ethernet interface view で、GigabitEthernet 1 を trunk ポートとして設定し、PVID を VLAN 100 に設定し、VLAN 100 に割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap3-gigabitethernet-1] port link-type trunk

[AC-wlan-ap-ap3-gigabitethernet-1] port trunk pvid vlan 100

[AC-wlan-ap-ap3-gigabitethernet-1] port trunk permit vlan 100

AP グループの Ethernet interface view で、GigabitEthernet 1 を trunk ポートとして設定し、PVID を VLAN 100 に設定し、VLAN 100 に割り当てます。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port link-type trunk

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port trunk pvid vlan 100

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port trunk permit vlan 100

関連コマンド

- **port link-type**
- **port trunk permit vlan**
- **remote-configuration**

1.1.55 power-level default

🕮 **メモ**:

- **power-level default** コマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。
- QX-W1210 と QX-W1230 はデフォルトの給電モード(High)の設定で 25W 以下の消費電力で動作します。

Syntax

power-level default

undo power-level default

デフォルト

AP view では、AP は AP group の AP model view の設定を使用します。

AP group の AP model view では AP の給電モードは High です。

View

AP view（QX-W1200 シリーズのみ）

AP group view（QX-W1200 シリーズのみ）

定義済みユーザロール

network-admin

パラメータ

high: 10G Ethernet インタフェースの最大リンク速度、USB インタフェース利用を制限しません。

middle: 10G Ethernet インタフェースの最大リンク速度を 5Gbps に制限し、USB インタフェースを使用不可にします。

low: 10G Ethernet インタフェースの最大リンク速度を 2.5Gbps に制限し、USB インタフェースを使用不可にします。

説明

power-level default コマンドは、AP の給電モードを指定します。

undo power-level default コマンドはデフォルトに戻します。

10G Ethernetインタフェースの最大リンク速度とUSBインタフェースの利用を制限することにより、消費電力を 25W 以下に制限し PoE+(802.3at)給電での動作を可能にします。

- PoE++(802.3bt)もしくは AC アダプタによる給電の場合は、**high** を設定します
- PoE+(802.3at)による給電の場合は、**middle** または **low** を設定します。

表 1-20 に AP の給電モード設定時の動作仕様を示します。

表 1-20 AP の給電モードの動作仕様

動作仕様 / AP の給電モード	装置の消費電力制限	10G Ethernet インタフェース最大リンク速度	USB インタフェース利用制限
high	制限なし	制限なし	制限なし (QX-W1230 は使用不可)
middle	25W	5Gbps	使用不可
low	25W	2.5Gbps	使用不可

🕮 **メモ**：

- 10G Ethernet インタフェースの通信速度が ”**10000**” または ”**5000**” の固定設定の場合、AP の給電モード設定 “**low**” を設定することはできません。
- 10G Ethernet インタフェースの通信速度が ”**10000**” の固定設定の場合、AP の給電モード設定 “**middle**” と “**low**” を設定することはできません。
- AP の給電モード設定 ”**middle**” または ”**low**” が設定されている場合、10G Ethernet インタフェースの通信速度、通信モードを変更することはできません。
- AP の給電モード設定による USB インタフェースの利用制限は ”**usb enable**” コマンドの設定よりも優先されます。
- AP の給電モードを異なるモードに変更する場合、AutoNegotiation をやり直すため 10G Ethernet インタフェースがリンクダウンします。

例

AP **ap1**（QX-W1240）の給電モードを **middle** に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1240

[AC-wlan-ap-ap1] power-level default middle

AP グループ 1 のモデル **QX-W1240** の AP の給電モードを **low** に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1240

[AC-wlan-ap-group-1-ap-model-QX-W1240] power-level default low

関連コマンド

usb

1.1.56 priority

Syntax

priority *priority*

undo priority

デフォルト

AP view は、AP group view の設定を使用します。

AP group view は、AC の AP 接続優先度は 4 です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

priority: AC の AP 接続優先度を 0～7 の範囲で指定します。値が大きいほど接続優先度が高くなります。

説明

priority コマンドは AC の AP 接続優先度を設定します。

undo priority コマンドはデフォルトに戻します。

AP は、より高い接続優先度を有する AC と CAPWAP トンネルを優先して確立します。

AP 接続優先度は、AC ディスカバリ中にのみ有効です。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap3** の AP 接続優先度を 7 に設定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1020

[AC-wlan-ap-ap3] priority 7

AP group **group1** の、AP 接続優先度を 7 に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] priority 7

1.1.57 provision

Syntax

provision

undo provision

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、AP の事前プロビジョニングが無効になっています。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

priority: AC の AP 接続優先度を 0～7 の範囲で指定します。値が大きいほど接続優先度が高くなります。

説明

provision コマンドは AP の事前プロビジョニングを有効にし、AP provision view に移行します。

undo provision コマンドは AP の事前プロビジョニングを無効にします。

AP の事前プロビジョニングでは、AC 上の AP のネットワーク設定を構成できます。AC は自動的にこれらの設定を AP に割り当てます。

AP の事前プロビジョニングを無効にすると、AC 上で設定されたネットワーク設定が削除されます。ただし、この操作は、すでに AP に割り当てられているネットワーク設定には影響しません。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP の事前プロビジョニングを有効にし、AP **ap1** の AP provision view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] provision

[AC-wlan-ap-ap1-prvs]

AP の事前プロビジョニングを有効にし、AP group **group1** の AP group provision view に移行します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] provision

[AC-wlan-ap-group-group1-prvs]

1.1.58 provision auto-recovery

Syntax

provision auto-recovery { **disable** | **enable** }

undo provision auto-recovery

デフォルト

AP view は、AP group view の設定を使用します。

AP group view では、事前プロビジョニングされた設定の自動ロードが有効になっています。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: 事前プロビジョニングされた設定の自動ロードを無効にします。

enable: 事前プロビジョニングされた設定の自動ロードを有効にします。

説明

provision auto-recovery enable コマンドは事前プロビジョニングされた設定の自動ロードを有効にします。

provision auto-recovery disable コマンドは事前プロビジョニングされた設定の自動ロードを無効にします。

undo provision auto-recovery コマンドはデフォルトに戻します。

事前プロビジョニングされた設定の自動ロードにより、AP と AC の間で CAPWAP トンネルが正常に確立されます。AP は、この機能をイネーブルにすると、以下の手順で AC を検出します。

1) 事前プロビジョニングされた設定を使用して、AP の手動または自動 AP 設定を持つ AC を検出します。
2) AC 検出が失敗した場合に AC を検出するために、リブートして他の方法を使用します。
3) AP がまだターゲット AC を検出できない場合は、再プロビジョニングされた設定を再起動して使用して、AC を検出します。

この AC ディスカバリプロセスは、AP がターゲット AC を検出して CAPWAP トンネルを確立するまで繰り返されます。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1** の事前プロビジョニングされた設定の自動ロードを無効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-ap-ap1] provision auto-recovery disable

AP group **group1** の AP の事前プロビジョニングされた設定の自動ロードを無効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] provision auto-recovery disable

1.1.59 provision auto-update

Syntax

provision auto-update { **disable** | **enable** }

undo provision auto-update

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、事前プロビジョニングされた設定の自動割り当てが無効になっています。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: 事前プロビジョニングされた設定の自動割り当てを無効にします。

enable: 事前プロビジョニングされた設定の自動割り当てを有効にします。

説明

provision auto-update enable コマンドは事前プロビジョニングされた設定の自動割り当てを有効にします。

provision auto-update disable コマンドは事前プロビジョニングされた設定の自動割り当てを無効にします。

undo provision auto-update コマンドはデフォルトに戻します。

このコマンドを使用すると、AC は事前プロビジョニングされた設定を AP に自動的に割り当てて、AP が事前プロビジョニングされた設定をオンラインで使用できるようにします。

このコマンドは、オフライン AP にのみ適用されます。事前プロビジョニングされた設定をオンライン AP に展開するには、**save wlan ap provision** コマンドを使用します。

AP プロビジョニング view の事前プロビジョニングされた設定は、AP グループプロビジョニング view の事前プロビジョニングされた設定よりも優先されます。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1** の事前プロビジョニング設定の自動割り当てを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-ap-ap1] provision auto-update enable

APgroup **group1** の AP の事前プロビジョニングされた設定の自動割り当てを有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] provision auto-update enable

1.1.60 qos priority

🕮 **メモ**:

- このコマンドはソフトウェアバージョン 7.2.18 を含む以降のソフトウェアからサポートしています。
- このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

qos priority *priority-value*

undo qos priority

デフォルト

AP の Ethernet interface view では、AP グループの Ethernet interface view の設定を使用します。

AP グループの Ethernet interface view では、ポートプライオリティは 0 です。

AP の aggregate interface view では、AP グループの aggregate interface view の設定を使用します。

AP グループの aggregate interface view では、ポートプライオリティは 0 です。

View

AP の GigabitEthernet interface view

AP group view の GigabitEthernet interface view

AP の Layer 2 aggregate interface view

AP group view の Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

priority-value: ポートプライオリティを 0～7 の範囲で指定します。

説明

qos priority コマンドはポートプライオリティを設定します。

undo qos priority コマンドはデフォルトに戻します。

本設定は **remote-configuration synchronize** コマンドを実行したときにのみ、オンラインの AP に適用されます。

AP view の設定は AP group view の設定より優先されます。

例

AP の GigabitEthernet interface view でポートプライオリティを 2 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1010

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] qos priority 2

AP グループの GigabitEthernet interface view でポートプライオリティを 2 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1010

[AC-wlan-ap-group-1-ap-model-QX-W1010] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1010-gigabitethernet-1] qos priority 2

AP の Layer 2 aggregate interface view でポートプライオリティを 2 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1010

[AC-wlan-ap-ap1] interface bridge-aggregation 1

[AC-wlan-ap-ap1-Bridge-Aggregation1] qos priority 2

AP グループの Layer 2 aggregate interface view でポートプライオリティを 2 に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-1] ap-model QX-W1010

[AC-wlan-ap-group-1-ap-model-QX-W1010] interface bridge-aggregation 1

[AC-wlan-ap-group-1-ap-model-QX-W1010-Bridge-Aggregation1] qos priority 2

関連コマンド

remote-configuration synchronize

1.1.61 qos trust

🕮 **メモ**:

- このコマンドはソフトウェアバージョン 7.2.18 を含む以降のソフトウェアからサポートしています。
- このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

qos trust { **dot1p** | **dscp** }

undo qos trust

デフォルト

AP の Ethernet interface view では、AP グループの Ethernet interface view の設定を使用します。

AP グループの Ethernet interface view では、設定されていません。

AP の aggregate interface view では、AP グループの aggregate interface view の設定を使用します。

AP グループの aggregate interface view では、設定されていません。

View

AP の GigabitEthernet interface view

AP group view の GigabitEthernet interface view

AP の Layer 2 aggregate interface view

AP group view の Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

dot1p: 802.1p プライオリティをマッピングに使用します。

dscp: DSCP プライオリティをマッピングに使用します。

説明

qos trust コマンドはポートプライオリティを設定します。

undo qos trust コマンドはデフォルトに戻します。

本設定は **remote-configuration synchronize** コマンドを実行したときにのみ、オンラインの AP に適用されます。

AP view の設定は AP group view の設定より優先されます。

例

AP の GigabitEthernet interface view で信頼されたパケットプライオリティタイプを dot1p に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1010

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] qos trust dot1p

AP グループの GigabitEthernet interface view で信頼されたパケットプライオリティタイプを dot1p に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1010

[AC-wlan-ap-group-1-ap-model-QX-W1010] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1010-gigabitethernet-1] qos trust dot1p

AP の Layer 2 aggregate interface view で信頼されたパケットプライオリティタイプを dot1p に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1010

[AC-wlan-ap-ap1] interface bridge-aggregation 1

[AC-wlan-ap-ap1-Bridge-Aggregation1] qos trust dot1p

AP グループの Layer 2 aggregate interface view で信頼されたパケットプライオリティタイプを dot1p に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-1] ap-model QX-W1010

[AC-wlan-ap-group-1-ap-model-QX-W1010] interface bridge-aggregation 1

[AC-wlan-ap-group-1-ap-model-QX-W1010-Bridge-Aggregation1] qos trust dot1p

関連コマンド

remote-configuration synchronize

1.1.62 remote-configuration

🕮 **メモ：**

remote-configuration を有効にした場合、**remote-configuration** で設定可能なコマンドがデフォルト値として適用されます。**remote-configuration** で設定できないコマンドを設定したい場合に限り、**map-configuration** の併用をご検討ください。また、**remote-configuration** と **map-configuration** の両方に同じ機能を有するコマンド設定がある場合、AP へのコンフィグ適用が正常におこなわれません。

Syntax

remote-configuration { **disable** | **enable** }

undo remote-configuration enable

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、リモート設定の割り当てが無効になっています。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: リモート構成割り当て機能を無効にします。

enable: リモート構成割り当て機能を有効にします。

説明

🕮 **メモ**:

このコマンドのサポートは、AP モデルによって異なります。

remote-configuration enable コマンドはリモート構成割り当て機能を有効にします。

remote-configuration disable コマンドはリモート構成割り当て機能を無効にします。

undo remote-configuration コマンドはデフォルトに戻します。

AC は、リモート設定割り当て機能がイネーブルになっている場合にのみ、関連する VLAN 設定を AP に割り当てます。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1** のリモート設定割り当て機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] remote-configuration enable

APgroup **group1** のリモート設定割り当て機能を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] remote-configuration enable

1.1.63 remote-configuration synchronize

🕮 **メモ**:

remote-configuration synchronize コマンドを使用する前に、**remote-configuration enable** が設定されていることを確認してください。

Syntax

remote-configuration synchronize

デフォルト

AP view では、AP は AP group view の設定を使用します。

AP group view では、リモートコンフィグレーションシンクロナイゼーションは起動していません。

View

AP view

AP group view

定義済みユーザロール

network-admin

説明

⚠ **注意：**

- このコマンドは、オンラインの AP のすべての VLAN、リンクアグリゲーション、ポート設定（ポートアイソレーション設定を除く）を削除し、AC で設定した設定内容を AP に反映させます。使用の際はご注意ください。
- AP が AC に接続された状態で、AP の設定内容を AC 上で変更した場合、**remote-configuration synchronize** コマンドを実行するまで変更内容が AP に反映されません。

remote-configuration synchronize コマンドは AC の設定を AP に同期します。

AP のコンフィグレーションファイルを更新するには、**map-configuration** コマンドを使用してコンフィグレーションファイルを AP に展開することができます。しかし、コンフィグレーションファイルを AP に展開する前に、そのファイルにコマンドを記述しておく必要があります。この方法は、時間がかかり、AP が数多く存在するネットワークでは適用できません。

本機能により、AC は VLAN、リンクアグリゲーション、ポートアイソレーションといった設定を、オンラインの AP に対して直接同期させることができます。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1** に対してリモートコンフィグレーションシンクロナイゼーションを起動します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] remote-configuration synchronize

AP グループ **group1** の AP に対してリモートコンフィグレーションシンクロナイゼーションを起動します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] remote-configuration synchronize

関連コマンド

remote-configuration

1.1.64 reset wlan ap

Syntax

reset wlan ap { **all** | **name** *ap-name* | **model** *model-name* | **ap-group** *group-name* }

View

ユーザ view

定義済みユーザロール

network-admin

パラメータ

all: AC に接続されているすべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

model *model-name*: モデル名で AP モデルを指定します。

ap-group *group-name*: AP group を名前で指定します。大文字と小文字を区別しない 1～31 文字です。

説明

reset wlan ap コマンドはすべての AP または指定した AP をリセットします。このコマンドは、AP と AC 間の CAPWAP トンネルを終了し、AP に関するすべての接続情報を削除します。

例

AP **ap1** をリセットします。

<AC> reset wlan ap name ap1

```
Reset the AP that has established or is to establish a primary tunnel with the
AC. Continue? [Y/N]:
```

1.1.65 reset wlan ap provision

Syntax

reset wlan ap provision { **all** | **name** *ap-name* }

View

すべての view

定義済みユーザロール

network-admin

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

説明

reset wlan ap provision コマンドはすべての AP または指定された AP から設定ファイル wlan_ap_prvs.xml を削除します。

このコマンドは、マスタ AC との CAPWAP トンネルを確立し、Run 状態にある AP でのみ有効です。

例

AP **ap1** の設定ファイル **wlan_ap_prvs.xml** を削除します。

<AC> reset wlan ap provision name ap1

1.1.66 reset wlan ap reboot-log

Syntax

reset wlan ap reboot-log { **all** | **name** *ap-name* }

View

ユーザ view

定義済みユーザロール

network-admin

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

説明

reset wlan ap reboot-log コマンドはすべての AP または指定された AP の再起動ログを消去します。

例

AP **ap1** の再起動ログを削除します。

<AC> reset wlan ap reboot-log name ap1

関連コマンド

display wlan ap reboot-log

1.1.67 reset wlan tunnel latency ap

Syntax

reset wlan tunnel latency ap { **all** | **name** *ap-name* }

View

ユーザ view

定義済みユーザロール

network-admin

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

説明

reset wlan tunnel latency ap コマンドはすべての AP または指定された AP のトンネル待ち時間情報を消去します。

このコマンドは、マスタ AC とのトンネルを確立し、Run 状態の AP でのみ有効です。

例

AP **ap1** のトンネル待ち時間情報を削除します。

<AC> reset wlan tunnel latency ap name ap1

関連コマンド

- **display wlan tunnel latency ap name**
- **tunnel latency-detect**

1.1.68 retransmit-count

Syntax

retransmit-count *value*

undo retransmit-count

デフォルト

AP view は、AP group view の設定を使用します。

AP group view は、AC 要求再送信の最大試行回数は 3 回です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

value: AC 要求再送信の最大試行回数を 2～5 の範囲で指定します。

説明

retransmit-count コマンドは AC 要求の再送信の最大試行回数を設定します。

undo retransmit-count コマンドはデフォルトに戻します。

AC は、要求再送の最大試行回数に達するか応答が受信されるまで、再送信間隔で AP に送信された要求を送信します。

AC から AP に送信される要求には、次のタイプがあります。

- イメージデータ要求
- 設定更新要求
- リセット要求
- データ転送要求
- IEEE 802.11 WLAN 設定要求
- ステーション設定要求

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap3** の AC 要求の再送信の最大試行回数を 4 に設定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1020

[AC-wlan-ap-ap3] retransmit-count 4

AP group **group1** の AP の AC 要求再送信の最大試行数を 4 に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] retransmit-count 4

関連コマンド

retransmit-interval

1.1.69 retransmit-interval

Syntax

retransmit-interval *interval*

undo retransmit-interval

デフォルト

AP view は、AP group view の設定を使用します。

AP group view は、要求の再送信間隔は 5 秒です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

interval: 要求の再送信間隔を 3～8 秒の範囲で指定します。

説明

retransmit-interval コマンドは AC が AP への要求を再送信する間隔を設定します。

undo retransmit-interval コマンドはデフォルトに戻します。

AC から AP に送信される要求には、次のタイプがあります。

- イメージデータ要求
- 設定更新要求
- リセット要求
- データ転送要求
- IEEE 802.11 WLAN 設定要求
- ステーション設定要求

AP view の設定は、AP group view の設定よりも優先されます。

例

AC が AP **ap3** に要求を送信する際の、要求の再送信間隔を 6 秒に設定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1020

[AC-wlan-ap-ap3] retransmit-interval 6

AC が AP group **group1** 内の AP に要求を送信際の、要求の再送信間隔を 6 秒に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] retransmit-interval 6

関連コマンド

retransmit-count

1.1.70 save wlan ap provision

Syntax

save wlan ap provision { **all** | **name** *ap-name* }

View

すべての view

定義済みユーザロール

network-admin

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

説明

save wlan ap provision コマンドはすべての AP または指定された AP に事前プロビジョニング設定を保存します。

このコマンドは、追加または変更された事前プロビジョニングされた設定を構成ファイル wlan_ap_prvs.xml に保存します。

このコマンドは、マスタ AC とのトンネルを確立したオンライン AP でのみ有効です。このコマンドは、AP の事前プロビジョニングされた設定が存在しない場合、**reset wlan ap provision** コマンドと同じ効果があります。

provision view での事前プロビジョニング設定は、**save wlan ap provision** コマンドを実行するとすぐに有効になります。

provision view での事前プロビジョニング設定のキャンセルは、**save wlan ap provision** コマンドを実行しても有効になりません。キャンセルを AP で有効にするには、AP を再起動します。

例

AP **ap1** の設定ファイル **wlan_ap_prvs.xml** に AP provision view の設定を保存します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] provision

[AC-wlan-ap-ap1-prvs] ac ip 192.168.0.1

[AC-wlan-ap-ap1-prvs] save wlan ap provision name ap1

1.1.71 serial-id (AP group view)

Syntax

serial-id *serial-id*

undo serial-id *serial-id*

デフォルト

シリアル ID による AP group ルールは設定されていません。

View

AP group view

定義済みユーザロール

network-admin

パラメータ

serial-id: AP のシリアル ID を、大文字と小文字を区別しない 1～63 文字で指定します。

説明

serial-id コマンドはシリアル ID で AP group ルールを作成します。

undo serial-id コマンドはシリアル ID で AP group ルールを削除します。

このコマンドは、指定された AP が存在するかどうかを識別しません。

シリアル ID で複数の AP group ルールを設定できます。

AP 名、シリアル ID、MAC アドレス、IP アドレスによる AP group ルールの優先度は、降順になっています。AP が group ルールと一致しない場合、AP はデフォルトの AP group に追加されます。

AP group ルールがすでに AP group に存在する場合、このコマンドは AP group からルールを削除します。

デフォルトの AP group の view でこのコマンドを実行することはできません。

例

AP group **group1** のシリアル ID で AP group ルールを作成します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] serial-id 210235A1BSC123000037

関連コマンド

wlan ap-group

1.1.72 serial-id (AP view)

Syntax

serial-id *serial-id*

undo serial-id *serial-id*

デフォルト

AP にシリアル ID は指定されていません。

View

AP view

定義済みユーザロール

network-admin

パラメータ

serial-id: AP のシリアル ID を、大文字と小文字を区別しない 1～63 文字で指定します。

説明

serial-id コマンドは AP のシリアル ID を指定します。

undo serial-id コマンドはデフォルトに戻します。

AP が AC との CAPWAP トンネルを確立している際に、AP のシリアル ID を変更または削除すると、CAPWAP トンネルが終了します。その後、AP は AC と CAPWAP トンネルを再確立します。

例

AP **ap1** のシリアル ID を **210235A1BSC123000050** に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-ap-ap1] serial-id 210235A1BSC123000050

1.1.73 smartrate-ethernet

Syntax

smartrate-ethernet *interface-number*

View

AP view

AP group's AP model view

定義済みユーザロール

network-admin

パラメータ

interface-number: インタフェース番号を指定します。値の範囲は、AP モデルによって異なります。

説明

🕮 **メモ：**

このコマンドのサポートは、AP モデルによって異なります。

smartrate-ethernet コマンドは AP の 2.5 GigabitEthernet interface view に移行します。

例

AP view から Smartrate-Ethernet 1 の interface view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] smartrate-ethernet 1

[AC-wlan-ap-ap3-smartrate-ethernet-1]

AP group **group1** の AP model view から Smartrate-Ethernet 1 の interface view に移行します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] smartrate-ethernet 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-smartrate-ethernet-1]

1.1.74 snmp-agent trap enable wlan ap

Syntax

snmp-agent trap enable wlan ap

undo snmp-agent trap enable wlan ap

デフォルト

AP 管理の SNMP 通知は無効になっています。

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan ap コマンドは AP 管理の SNMP 通知を有効にします。

undo snmp-agent trap enable wlan ap コマンドはデフォルトに戻します。

重要な AP 管理イベントを NMS に報告するには、AP 管理の SNMP 通知を有効にします。AP 管理イベント通知が正しく送信されるようにするには、オペレーションマニュアルのセクション 11 *システム管理 "SNMP"* の説明に従って SNMP も設定する必要があります。

例

AP 管理の SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan ap

1.1.75 snmp-agent trap enable wlan capwap

Syntax

snmp-agent trap enable wlan capwap

undo snmp-agent trap enable wlan capwap

デフォルト

CAPWAP の SNMP 通知は無効になっています。

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan capwap コマンドは CAPWAP の SNMP 通知を有効にします。

undo snmp-agent trap enable wlan capwap コマンドはデフォルトに戻します。

重要な CAPWAP イベントを NMS に報告するには、CAPWAP の SNMP 通知を有効にします。CAPWAP イベント通知が正しく送信されるようにするには、オペレーションマニュアルのセクション 11 *システム管理 “SNMP”* の説明に従って SNMP も設定する必要があります。

例

CAPWAP の SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan capwap

1.1.76 statistics-interval

Syntax

statistics-interval *interval*

undo statistics-interval

デフォルト

AP view は、AP group view の設定を使用します。

AP group view は、統計値報告間隔は 50 秒です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

interval: 統計値報告間隔を 0～240 秒の範囲で指定します。AP の統計値報告を無効にするには、統計値報告間隔を 0 に設定します。

説明

statistics-interval コマンドは AP が統計値報告を AC に送信する間隔を設定します。

undo statistics-interval コマンドはデフォルトに戻します。

このコマンドを実行すると、AP が統計情報を報告する間隔を変更できます。これらの統計情報を使用して、AP 上の無線の動作ステータスを監視できます。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1** の統計値報告間隔を 10 秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] statistics-interval 10

AP group **group1** の AP の統計値報告間隔を 10 秒に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] statistics-interval 10

1.1.77 tunnel encryption

Syntax

tunnel encryption { **disable** | **enable** }

undo tunnel encryption enable

デフォルト

AP view：AP group view の設定を使用

AP group view：無効

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: CAPWAP 制御トンネル暗号化を無効にします。

enable: CAPWAP 制御トンネル暗号化を有効にします。

説明

tunnel encryption enable コマンドは CAPWAP 制御トンネル暗号化を有効にします。

tunnel encryption disable コマンドは CAPWAP 制御トンネルを無効にします。

undo tunnel encryption enable コマンドはデフォルトに戻します。

本コマンド適用時、CAPWAP トンネルが再接続されます。

本機能を有効にすると、AP は AC から暗号化フラッグがついた検出応答を受信したとき、AC と CAPWAP トンネルを確立します。CAPWAP トンネル確立されると、DTLS ハンドシェークのあとに AC と AP は CAPWAP 制御トンネル内で転送された制御パケットを暗号化します。

AP view の設定は AP group view の設定より優先されます。

例

AP **ap1** に対して CAPWAP 制御トンネル暗号化を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] tunnel encryption enable

```
This operation will restart the AP. Continue? [Y/N]
```

APgroup **group1** に CAPWAP 制御トンネル暗号化を設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] tunnel encryption enable

```
This operation will restart member APs that are not enabled with CAPWAP control
tunnel encryption. Continue? [Y/N]
```

1.1.78 tunnel latency-detect

Syntax

tunnel latency-detect { **start** | **stop** }

デフォルト

CAPWAP トンネル待ち時間検出は開始されません。

View

AP view

定義済みユーザロール

network-admin

パラメータ

start: CAPWAP トンネル待ち時間検出は開始します。

stop: CAPWAP トンネル待ち時間検出は停止します。

説明

tunnel latency-detect コマンドは CAPWAP トンネル待ち時間検出を設定します。

CAPWAP トンネル待ち時間検出により、CAPWAP 制御フレームもしくは AP から AC へのデータフレームおよびその逆方向通信の送信待ち時間を検出できます。

AP がオフラインのとき、CAPWAP トンネル待ち時間検出は自動的に停止します。AP が再びオンラインになると、**tunnel latency-detect start** コマンドを実行して、CAPWAP トンネル待ち時間検出を再始動させる必要があります。

tunnel latency-detect start コマンドは、マスタ AC との CAPWAP トンネルを確立し、Run 状態にある AP でのみ有効です。

例

AP **ap1** の CAPWAP トンネル待ち時間検出を開始します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] tunnel latency-detect start

関連コマンド

- **display wlan tunnel latency ap name**
- **reset wlan tunnel latency ap**

1.1.79 usb

Syntax

usb { **disable** | **enable** }

undo usb

デフォルト

AP view では、AP は AP group's AP model view で設定を使用します。

AP group's AP model view では、USB インタフェースが無効になっています。

View

AP view

AP group's AP model view

定義済みユーザロール

network-admin

パラメータ

disable: AP 上の USB インタフェースを無効にします。

enable: AP 上の USB インタフェースを有効にします。

説明

🕮 **メモ：**

このコマンドのサポートは、AP モデルによって異なります。

usb enable コマンドは AP 上の USB インタフェースを有効にします。

usb disable コマンドは AP 上の USB インタフェースを無効にします。

undo usb コマンドはデフォルトに戻します。

このコマンドは、次のいずれかの要件が満たされている場合にのみ、AP で有効になります。

- AP の電力レベルが高い。
- AP の電力レベルは中程度で、MIMO モードは 1×1 です。

AP view の設定は、AP group's AP model view の設定よりも優先されます。

例

AP view で USB インタフェースを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] usb enable

AP group **g1** の AP model view で USB インタフェースを有効にします。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] ap-model QX-W1020

[AC-wlan-ap-group-g1-ap-model-QX-W1020] usb enable

関連コマンド

power-level default

1.1.80 vlan

🕮 **メモ：**

このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

undo vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、VLAN 1（デフォルト VLAN）が AP に存在します。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

vlan-id1: VLAN ID を 1～4094 の範囲で指定します。

vlan-id1 **to** *vlan-id2*: VLAN 範囲を指定します。*vlan-id1* および *vlan-id2* 引数は VLAN ID を指定します。2 つの引数の値の範囲は 1～4094 です。*vlan-id2* 引数の値は、*vlan-id1* 引数の値よりも小さくすることはできません。

all: 予約済み VLAN を除くすべての VLAN を指定します。このキーワードは、AP で作成できる VLAN の最大数が 4094 未満の場合はサポートされません。このキーワードのサポートは、AP モデルによって異なります。

説明

🕮 **メモ：**

このコマンドのサポートは、AP モデルによって異なります。

---

vlan *vlan-id* コマンドは AP の VLAN を作成し、AP の VLAN view に移行します。

vlan *vlan-id1* **to** *vlan-id2* コマンドは予約済み VLAN を除き、AP の VLAN *vlan-id1*～*vlan-id2* を作成します。

vlan all コマンドは AP の VLAN 1～4094 を作成します。

undo vlan コマンドは AP の指定された VLAN を削除します。

VLAN 1（デフォルト VLAN）または予約済み VLAN を作成または削除することはできません。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1** の VLAN 2 を作成し、VLAN の VLAN view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] vlan 2

[AC-wlan-ap-ap1-vlan2]

APgroup **group1** の VLAN 2 を作成し、VLAN の VLAN view に移行します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] vlan 2

[AC-wlan-ap-group-1-vlan2]

関連コマンド

remote-configuration

1.1.81 wlan ap

Syntax

wlan ap *ap-name* { **model** *model-name* }

undo wlan ap *ap-name*

デフォルト

手動 AP は存在しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

ap-name: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

model *model-name*: AP のモデル名を指定します。AP を作成するときは、モデル名を指定する必要があります。

QX-W1010：QX-W1010 を指定します。

QX-W1020：QX-W1020 を指定します。

QX-W1030：QX-W1030 を指定します。

QX-W1110：QX-W1110 を指定します。

QX-W1120：QX-W1120 を指定します。

QX-W1130：QX-W1130 を指定します。

QX-W1210：QX-W1210 を指定します。

QX-W1230：QX-W1230 を指定します。

QX-W1240：QX-W1240 を指定します。

🕮 **メモ：**

QX-W1010 はソフトウェアバージョン 7.1.11 を含む以降のソフトウェアからサポートしています。
QX-W1130 はソフトウェアバージョン 7.2.27 を含む以降のソフトウェアからサポートしています。
QX-W1120 はソフトウェアバージョン 7.2.46 を含む以降のソフトウェアからサポートしています。
QX-W1110 はソフトウェアバージョン 7.2.55 を含む以降のソフトウェアからサポートしています。
QX-W1240 はソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。
QX-W1210 と QX-W1230 はソフトウェアバージョン 7.2.89 を含む以降のソフトウェアからサポートしています。

説明

wlan ap コマンドは AP を作成し AP view へ移行します。

undo wlan ap コマンドは AP を削除します。

指定された AP がすでに存在する場合、AP view に入ります。

指定された AP が CAPWAP トンネルを確立している場合、**undo wlan ap** コマンドはトンネルも終了します。

例

QX-W1020 モデルで AP **ap1** を作成します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1]

1.1.82 wlan apdb

Syntax

wlan apdb *model-name hardware-version software-version*

undo wlan apdb *model-name hardware-version*

デフォルト

AP モデルのハードウェアバージョンに対するソフトウェアバージョンは、APDB ユーザスクリプト内に記憶されているソフトウェアバージョンです。

View

System view

定義済みユーザロール

network-admin

パラメータ

model-name: APDB の AP モデル名を指定します。

hardware-version: APDB のハードウェアバージョンを指定します。

software-version: AP ソフトウェアバージョンを大文字と小文字を区別しない 1～31 文字で指定します。

説明

注意：

CAPWAP トンネルの確立に失敗しないようにするには、NEC サポートの案内に従ってこのコマンドを使用してください。

wlan apdb コマンドは AP モデルのソフトウェアバージョンとハードウェアバージョン間のマッピングを設定します。

undo wlan apdb コマンドはデフォルトに戻します。

APDB には、AP モデルのハードウェアバージョンに対するソフトウェアバージョンのマッピングが記憶されています。このコマンドを使用して、ソフトウェア更新用の AP モデルのハードウェアバージョンに対するソフトウェアバージョンを再指定することができます。ソフトウェア更新機能は、AP がオンラインになったときに、このコマンドで指定されたソフトウェアバージョンにソフトウェアを更新します。

例

APDB 内の AP モデル QX-W1020 のハードウェアバージョン **Ver.C** に対するソフトウェアバージョンを E2108 に指定します。

<AC> system-view

[AC] wlan apdb QX-W1020 Ver.C E2108

関連コマンド

firmware-upgrade

1.1.83 wlan apdb file

Syntax

wlan apdb file *user.apdb*

undo wlan apdb file

デフォルト

APDB ユーザスクリプトはロードされません。

View

System view

定義済みユーザロール

network-admin

パラメータ

user.apdb: APDB ユーザープロファイルを名前で指定します。大文字と小文字が区別される 1～63 文字です。apdb はファイル名の拡張子です。

説明

wlan apdb file コマンドは APDB ユーザスクリプトをロードします。

undo wlan apdb file コマンドは APDB ユーザスクリプトを削除します。

このコマンドは、ユーザスクリプト内の AP モデル情報を APDB に追加します。

AC 上で複数のユーザスクリプトをロードする場合、直近でロードされたユーザスクリプトは、古いユーザスクリプトを上書きします。

以下の状況下で新たなユーザスクリプトをロードするために、各状況に応じて以下の操作のいずれかを実行します。

- 手動 AP または、古いユーザスクリプト内にモデルが記載されているオンラインの自動 AC が存在するとき、AC 上で一致する AP モデル情報を削除します。
- AP がすでに AP group に追加されている場合、古いユーザスクリプト内にモデルが記載されている AP を、AP group から取り除きます。
- 古いユーザスクリプトが、ソフトウェアバージョンがすでに設定された AP モデルを含む場合、元のソフトウェアバージョンを復元するために **wlan apdb** コマンドを使用します。

ファイルシステム内のユーザスクリプトを修正または削除する場合、AC は再起動後ユーザスクリプト内の AP モデルの設定を失います。

例

#ユーザスクリプト **user.apdb** をロードします。

<AC> system-view

[AC] wlan apdb file user.apdb

関連コマンド

wlan apdb

1.1.84 wlan ap-group

Syntax

wlan ap-group *group-name*

undo wlan ap-group *group-name*

デフォルト

デフォルトの AP group **default-group** が存在します。

View

System view

定義済みユーザロール

network-admin

パラメータ

group-name: AP group を名前で指定します。大文字と小文字を区別しない 1～31 文字です。

説明

wlan ap-group コマンドは AP group を作成します。

undo wlan ap-group コマンドは AP group を削除します。

指定された AP group が存在する場合、AP group view に移行します。

デフォルトの AP group は削除できません。

例

group1 という名前の AP group を作成します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1]

関連コマンド

display wlan ap-group

1.1.85 wlan ap-image-deploy

メモ:

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

wlan ap-image-deploy { **all** | **name** *ap-name* | **ap-group** *group-name* }

View

System view

定義済みユーザロール

network-admin

パラメータ

all: AC に接続されているすべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

ap-group *group-name*: AP group を名前で指定します。大文字と小文字を区別しない 1～31 文字です。

説明

wlan ap-image-deploy コマンドはオンライン状態の AP にイメージファイルを展開します。展開したソフトウェアを有効にするためには AP を再起動する必要があります。

このコマンドを実行する前に、AC のストレージメディアにイメージファイルをアップロードする必要があります。**wlan image-load filepath** コマンドを実行して、ストレージメディアを指定できます。

例

#すべてのオンライン状態の AP にイメージファイルを展開します。

<Sysname> system-view
[Sysname] wlan ap-image-deploy all

関連コマンド

wlan image-load filepath

1.1.86 wlan auto-ap enable

Syntax

wlan auto-ap enable

undo wlan auto-ap enable

デフォルト

自動 AP 機能は無効です。

View

System view

定義済みユーザロール

network-admin

説明

wlan auto-ap enable コマンドは自動 AP 機能を有効にします。

undo wlan auto-ap enable コマンドは自動 AP 機能を無効にします。

自動 AP 機能により、AP は手動 AP 設定なしで AC に接続可能となります。数多くの AP を WLAN 内に配置する際の設定が単純化されます。

自動 AP を設定するために、自動 AP を手動 AP に変換するための自動 AP パーシステンスを使用するか、もしくは AP group を通じてそれを設定しなければなりません。

例

#自動 AP 機能を有効にします。

<AC> system-view

[AC] wlan auto-ap enable

1.1.87 wlan auto-ap persistent

Syntax

wlan auto-ap persistent { **all** | **name** *auto-ap-name* [*new-ap-name*] }

View

System view

定義済みユーザロール

network-admin

パラメータ

all: すべてのオンライン自動 AP を指定します。このキーワードを指定すると、コマンドはすべてのオンライン自動 AP を名前が変更されていない手動 AP に変換します。

auto-ap-name: オンライン自動 AP を指定します。

new-ap-name: 新しい AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

説明

wlan auto-ap persistent コマンドはオンライン自動 AP を手動 AP に変換します。

例

MAC アドレスが 0afb-4212-cd36 の自動 AP を手動 AP **ap2** に変換します。

<AC> system-view

[AC] wlan auto-ap persistent name 0afb-4212-cd36 ap2

1.1.88 wlan auto-persistent enable

Syntax

wlan auto-persistent enable

undo wlan auto-persistent enable

デフォルト

自動 AP パーシステンスは無効です。

View

System view

定義済みユーザロール

network-admin

説明

wlan auto-persistent enable コマンドは自動 AP パーシステンスを有効しオンラインになった後に自動 AP を自動的に手動 AP に変換します。

undo wlan auto-persistent enable コマンドはデフォルトに戻します。

このコマンドは、コマンドを実行した後にオンラインになった自動 AP でのみ有効です。すでにオンラインになっている自動 AP の場合は、**wlan auto-ap persistent** コマンドを使用して、手動 AP に変換します。

例

#自動 AP パーシステンスを有効にします。

<AC> system-view

[AC] wlan auto-persistent enable

1.1.89 wlan capwap discovery-policy unicast

Syntax

wlan capwap discovery-policy unicast

undo wlan capwap discovery-policy

デフォルト

AC は、ユニキャスト、マルチキャスト、ブロードキャストの発見要求に応答できます。

View

System view

定義済みユーザロール

network-admin

説明

wlan capwap discovery-policy unicast コマンドは AC がユニキャスト発見要求にのみ応答するようにします。

undo wlan capwap discovery-policy コマンドはデフォルトに戻します。

例

AC がユニキャスト発見要求にのみ応答するようにします。

<AC> system-view

[AC] wlan capwap discovery-policy unicast

1.1.90 wlan detect-anomaly enable

Syntax

wlan detect-anomaly enable

undo wlan detect-anomaly enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

wlan detect-anomaly enable コマンドはサービス異常の検出を有効にします。

undo wlan detect-anomaly enable コマンドはサービス異常の検出を無効にします。

本コマンド有効時、IRF スタックを組んだ AC に規定台数以上の AP が接続した後、AP がすべてオフラインになると、AC は 10 分後に再起動します。IRF スタックの詳細は、オペレーションマニュアルのセクション 12 *IRF スタック “IRF スタックの設定”* を参照してください。

🕮 **メモ：**

規定台数はソフトウェアバージョンにより異なります。

- ソフトウェアバージョン 7.1.13 を含む以前のソフトウェア：1 台以上の AP が接続した場合。
- ソフトウェアバージョン 7.2.18 を含む以降のソフトウェア：50 台以上の AP が接続した場合。

例

サービス異常の検出を有効にします。

<AC> system-view

[AC] wlan detect-anomaly enable

1.1.91 wlan global-configuration

Syntax

wlan global-configuration

View

System view

定義済みユーザロール

network-admin

説明

wlan global-configuration コマンドは global configuration view へ移行します。

AP view、AP group view、global configuration view での AP の設定の優先度は降順です。1 つの view で設定が構成されていない場合、優先度の低い view の設定が使用されます。3 つの view の全てに設定がされていない場合、AP は最も優先度の低い view のデフォルト設定を使用します。

例

global configuration view へ移行します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration]

1.1.92 wlan image-load filepath

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

wlan image-load filepath { **local** | **ram** }

undo wlan image-load filepath

View

System view

定義済みユーザロール

network-admin

パラメータ

local:AP イメージファイルを優先して取得する場所としてローカルフォルダを指定します。ローカルフォルダに AP イメージファイルが含まれていない場合、AC は RAM から AP イメージファイルを取得します。RAM に AP イメージファイルが含まれていない場合、AC は AP イメージファイルを取得することはできません。

ram:AP イメージファイルを優先して取得する場所として RAM を指定します。RAM に AP イメージファイルが含まれていない場合、AC はローカルフォルダから AP イメージファイルを取得します。ローカルフォルダに AP イメージファイルが含まれていない場合、AC は AP イメージファイルを取得することはできません。

説明

AC のイメージファイルには AP イメージファイルが含まれています。AC は、起動時に AP イメージファイルを RAM に読み込みます。

local キーワードは、次の条件を満たす場合にだけ指定します。

- 必要な AP イメージファイルが AC のイメージファイルに含まれていない。
- AP がオンラインになるときに使用するソフトウェアバージョンが、wlan apdb コマンドを使用して指定されている。

local キーワードを指定する場合は、AC がデフォルトのファイルシステムとして CF またはフラッシュカードを使用し、AP イメージファイルが AC 上のファイルシステムのルートディレクトリに保存されていることを確認してください。

AC は、. ipe の AP イメージファイルのみを AP に割り当てることができます。

例

AP イメージファイルを優先して取得する場所として、AC のローカルフォルダを指定します。

<Sysname> system-view
[Sysname] wlan image-load filepath local

1.1.93 wlan re-group

Syntax

wlan re-group { **ap** *ap-name* | **ap-group** *old-group-name* | **mac-address** *mac-address* | **serial-id** *serial-id* } *group-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

ap *ap-name*: AP 名で AP group ルールを指定します。

ap-group *old-group-name*: 送信元 AP group を指定します。送信元 AP group をデフォルト AP group にすることはできません。

mac-address *mac-address*: MAC アドレスで AP group ルールを指定します。

serial-id *serial-id*: シリアル ID で AP group ルールを指定します。

group-name: 宛先 AP group を指定します。宛先 AP group をデフォルト AP group にすることはできません。

説明

wlan re-group コマンドは AP group ルールまたは AP group ルールのリストを指定された AP group に移動します。

例

AP group **group1** を作成し、ap1、ap2、ap3 という AP 名で AP group ルールを作成します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap ap1 ap2 ap3

[AC-wlan-ap-group-group1] quit

＃AP group **group2** を作成し、AP 名で AP group ルールを group2 に移動します。

[AC] wlan ap-group group2

[AC-wlan-ap-group-group2] quit

[AC] wlan re-group ap ap1 group2

1.1.94 wlan rename-ap

Syntax

wlan rename-ap *ap-name new-ap-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

ap-name: 手動 AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

new-ap-name:新しい AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

説明

wlan rename-ap コマンドは手動 AP の名前を変更します。

例

AP **ap1** の名前を **ap1-office** に変更します。

<AC> system-view

[AC] wlan rename-ap ap1 ap1-office

1.1.95 wlan save ap-configuration

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7. 2. 73 を含む以降のソフトウェアからサポートしています。

Syntax

wlan save ap-configuration { **all** | **ap-group** *group-name* | **name** *ap-name* }

View

System view

定義済みユーザロール

network-admin

パラメータ

all: AC に接続されているオンライン状態のすべての AP を指定します。

ap-group *group-name*: AP group 内のオンライン状態の AP を指定します。*group-name* は大文字と小文字を区別しない 1～31 文字です。

name *ap-name*: オンライン状態の AP を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列で、大文字と小文字を区別します。

説明

wlan save ap-configuration コマンドは、指定した AP、AP グループ、または全てのオンライン状態の AP を対象に、現在のコンフィグを AP 上に保存し、次回の起動に使用するスタートアップコンフィグレーションファイルとして設定します。

例

全てのオンライン状態の AP の現在のコンフィグを保存します

<AC> system-view

[AC] wlan save ap-configuration all

This operation will save the configuration of ap. Continue? [Y/N]: y

[AC]

1.1.96 wlan timezone-sync enable

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.46 を含む以降のソフトウェアからサポートしています。

Syntax

wlan timezone-sync enable

undo wlan timezone-sync enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

wlan timezone-sync enable コマンドはタイムゾーンの同期を有効にします。

undo wlan timezone-sync enable コマンドはデフォルトに戻します。

例

タイムゾーンの同期を有効にします。

<AC> system-view

[AC] wlan timezone-sync enable

1.1.97 wlan tcp mss

Syntax

wlan tcp mss value

undo wlan tcp mss

デフォルト

CAPWAP トンネルの TCP MSS のデフォルト値は、ソフトウェアバージョンにより異なります。

ソフトウェアバージョン 7.2.27a を含む以前のソフトウェアでは QX は MSS の書き換えを行いません。

ソフトウェアバージョン 7.2.42 を含む以降のソフトウェアでは 1360 バイトです。

View

System view

定義済みユーザロール

network-admin

パラメータ

value: 128～2048 の範囲のバイト単位の TCP MSS を指定します。

説明

wlan tcp mss コマンドは CAPWAP トンネルの最大 TCP セグメントサイズ（MSS）を設定します。

undo wlan tcp mss コマンドを設定すると、QX は MSS の書き換えを行いません。

TCP セッションは端末が設定した MSS で動作し、QX はパケットの分割を行いません。

このコマンドは、CAPWAP トンネルを介して送信される SYN パケットの MSS オプションの値を設定します。

MSS オプションは、送信者が受け入れることができる最大セグメントの受信者に通知します。各エンドは、TCP 接続の確立中に MSS をアナウンスします。TCP セグメントのサイズが受信側の MSS より小さいか等しい場合、TCP はフラグメンテーションなしで TCP セグメントを送信します。そうでない場合、TCP は受信者の MSS に基づいてセグメントを分割します。

例

CAPWAP トンネルの TCP MSS を 2000 バイトに設定します。

<AC> system-view

[AC] wlan tcp mss 2000

目次

このセクションのページは **2-x-x** です。

2 章 無線管理の設定 2-1
2.1 無線管理の設定コマンド 2-1
2.1.1 a-mpdu 2-1
2.1.2 a-msdu 2-2
2.1.3 ani 2-3
2.1.4 antenna type 2-4
2.1.5 auto-channel european-gap enable 2-5
2.1.6 beacon-interval 2-6
2.1.7 bss-color 2-7
2.1.8 channel 2-9
2.1.9 channel auto-select 2-10
2.1.10 channel band-width 2-12
2.1.11 channel-usage measure 2-13
2.1.12 channel-usage threshold 2-15
2.1.13 client dot11ac-only 2-15
2.1.14 client dot11ax-only 2-17
2.1.15 client dot11b-forbidden 2-18
2.1.16 client dot11n-only 2-19
2.1.17 client max-count 2-20
2.1.18 continuous-mode 2-21
2.1.19 custom antenna gain 2-22
2.1.20 display wlan ap continuous-mode 2-24
2.1.21 display wlan ap radio 2-25
2.1.22 display wlan ap radio channel 2-26
2.1.23 display wlan ap radio type 2-27
2.1.24 display wlan statistics ap radio 2-28
2.1.25 distance 2-43
2.1.26 dl-ofdma 2-44
2.1.27 dot11ac mandatory maximum-nss 2-46
2.1.28 dot11ax mandatory maximum-nss 2-47
2.1.29 dot11ac multicast-nss 2-48
2.1.30 dot11ax multicast-nss 2-50
2.1.31 dot11ac support maximum-nss 2-51
2.1.32 dot11ax support maximum-nss 2-52
2.1.33 dot11be mandatory maximum-nss 2-53
2.1.34 dot11be multicast-nss 2-54

2.1.35 dot11be support maximum-nss 2-55
2.1.36 dot11g protection 2-56
2.1.37 dot11n mandatory maximum-mcs 2-58
2.1.38 dot11n multicast-mcs 2-59
2.1.39 dot11n protection 2-60
2.1.40 dot11n support maximum-mcs 2-62
2.1.41 dtim 2-63
2.1.42 fragment-threshold 2-65
2.1.43 green-energy-management 2-66
2.1.44 ldpc 2-67
2.1.45 long-retry threshold 2-68
2.1.46 max-power 2-69
2.1.47 mru 2-72
2.1.48 mu-txbf 2-74
2.1.49 power-lock 2-76
2.1.50 preamble 2-78
2.1.51 pre-puncture static 2-79
2.1.52 protection-mode 2-80
2.1.53 protection-threshold 2-82
2.1.54 radar-channel-switchback disable 2-83
2.1.55 radio 2-84
2.1.56 radio { disable | enable } 2-85
2.1.57 radio-type 2.4g 2-86
2.1.58 radio-type 5g 2-87
2.1.59 rate 2-88
2.1.60 reset wlan statistics ap radio 2-90
2.1.61 short-gi 2-91
2.1.62 short-retry threshold 2-92
2.1.63 smart-antenna 2-93
2.1.64 smart-antenna policy 2-95
2.1.65 stbc 2-96
2.1.66 su-txbf 2-97
2.1.67 twt negotiate 2-99
2.1.68 type 2-101
2.1.69 ul-ofdma 2-103
2.1.70 wlan in-band 6g-discovery 2-105
2.1.71 wlan multiple-bssid enable 2-106
2.1.72 wlan out-band 6g-discovery 2-107
2.1.73 wlan radio 2-108

2章 無線管理の設定

2.1 無線管理の設定コマンド

2.1.1 a-mpdu

Syntax

a-mpdu { **disable** | **enable** }

undo a-mpdu

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、A-MPDU アグリゲーション手法は有効です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: A-MPDU アグリゲーション手法を無効にします。

enable: A-MPDU アグリゲーション手法を有効にします。

説明

a-mpdu enable コマンドは A-MPDU アグリゲーション手法を有効にします。

a-mpdu disable コマンドは A-MPDU アグリゲーション手法を無効にします。

undo a-mpdu コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax、802.11gac、802.11gax 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g に変更すると、コマンドが無効になります。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、A-MPDU アグリゲーション手法を無効化します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] a-mpdu disable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、A-MPDU アグリゲーションを無効化します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] a-mpdu disable

2.1.2 a-msdu

Syntax

a-msdu { **disable** | **enable** }

undo a-msdu

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、A-MSDU アグリゲーション手法は有効です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: A-MSDU アグリゲーション手法を無効にします。

enable: A-MSDU アグリゲーション手法を有効にします。

説明

a-msdu enable コマンドは A-MSDU アグリゲーション手法を有効にします。

a-msdu disable コマンドは A-MSDU アグリゲーション手法を無効にします。

undo a-msdu コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax、802.11gac、802.11gax 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g に変更すると、コマンドが無効になります。

装置は A-MSDU を受信することができますが、送信することはできません。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、A-MSDU アグリゲーション手法を無効化します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] a-msdu disable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、A-MPDU アグリゲーションを無効化します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] a-msdu disable

2.1.3 ani

Syntax

ani { **disable** | **enable** }

undo ani

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、ANI は有効です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: ANI（Adaptive Noise Immunity）を無効にします。

enable: ANI（Adaptive Noise Immunity）を有効にします。

説明

ani enable コマンドは ANI（Adaptive Noise Immunity）を有効にします。

ani disable コマンドは ANI を無効にします。

undo ani コマンドはデフォルトに戻します。

ANI は周辺環境からの干渉を減少させるために、環境に基づいた騒音防止レベルを調整できるようにします。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、ANI を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] ani enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、ANI を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] ani enable

2.1.4 antenna type

Syntax

antenna type *antenna-type*

undo antenna type

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、デフォルトのアンテナタイプは装置モデルにより異なります。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

antenna-type: 1～10 文字の文字列でアンテナタイプを指定します。AP によりサポートされるアンテナタイプは装置モデルにより異なります。

説明

antenna type コマンドは AP のアンテナタイプを設定します。

undo antenna type コマンドはデフォルトに戻します。

アンテナタイプを設定すると、送信電力が正しい範囲内に収まるよう、アンテナ利得が自動的に変化します。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** のアンテナタイプを設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] antenna type internal

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、アンテナタイプを設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] antenna type internal

2.1.5 auto-channel european-gap enable

Syntax

auto-channel european-gap enable

undo auto-channel european-gap enable

デフォルト

2.4GHz 無線ではヨーロッパ以外のチャネルギャップ 5 を使用して、チャネル 1,6,11 を自動的に選択します。

View

Global configuration view

定義済みユーザロール

network-admin

説明

auto-channel european-gap enable コマンドは 2.4GHz 無線を設定して、ヨーロッパのギャップを自動チャネル選択に使用します。

undo auto-channel european-gap enable コマンドはデフォルトに戻します。

2.4GHz 無線でヨーロッパチャネルギャップ 6 を使用してチャネル 1,7、および 13 を自動的に選択するには、このコマンドを設定します。

例

自動チャネル選択のためにヨーロッパのチャネルギャップを使用するように 2.4GHz 無線を設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] auto-channel european-gap enable

関連コマンド

channel

2.1.6 beacon-interval

Syntax

beacon-interval *interval*

undo beacon-interval

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、ビーコン間隔は 100TU(Time Unit)です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

interval: ビーコン間隔を 32TU から 8191TU の範囲で指定します。

説明

beacon-interval コマンドはビーコン間隔を設定します。

undo beacon-interval コマンドはデフォルトに戻します。

例

AP **ap1** のビーコン間隔を 1000TU に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] beacon-interval 1000

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、ビーコン間隔を 1000TU に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] beacon-interval 1000

2.1.7 bss-color

🕮 **メモ**:

- **bss-color** コマンドはソフトウェアバージョン 7.2.42 を含む以降のソフトウェアからサポートしています。
- **bss-color** コマンドは QX-W1100 シリーズおよび QX-W1200 シリーズでのみサポートしています。

Syntax

bss-color { **disable** | **enable** }

undo bss-color

デフォルト

radio view では、AP group radio view の設定を使用します。

AP group radio view では、ソフトウェアバージョンにより異なります。

ソフトウェアバージョン7.2.55 を含む以前のソフトウェアでは無効(コンフィグ上は非表示)です。

ソフトウェアバージョン7.2.56 を含む以降のソフトウェアでは有効(コンフィグ上は非表示)です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

説明

bss-color enable コマンドは BSS カラーリングを有効にします。

bss-color disable コマンドは BSS カラーリングを無効にします。

undo bss-color コマンドはデフォルトに戻します。

このコマンドは、802.11 ax および 802.11 gax でのみ有効です。無線タイプを 802.11 a/b/g/n/ac/gac に変更すると、設定が削除されます。

BSS カラーリングを使用すると、システムは各 BSS にカラーを割り当て、クライアントへのデータパケットにカラーID を含めることができます。データパケットにカラーID が含まれることで、クライアントは関連付いた AP からパケットが送信されたかどうかを識別できます。衝突を避けるために、関連付けられた BSS と同じカラーの 802.11 ax データパケットを検出したクライアントは送信を延期します。

高密度環境で BSS カラーリングを有効にすると、システムパフォーマンスとチャネル使用率が向上します。

Radio view の設定は AP group radio view の設定よりも優先されます。

例

AP **ap1** の Radio1 で BSS カラーリングを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ax

[AC-wlan-ap-ap1-radio-1] bss-color enable

AP グループ **apgroup1** の AP の Radio1 で BSS カラーリングを有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1]ap-model QX-W1130

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] type dot11ax

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] bss-color enable

関連コマンド

type dot11ax

2.1.8 channel

Syntax

channel { *channel-number* | **auto** { **lock** | **unlock** } }

undo channel [**auto**]

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、AP は無線チャネルを自動的に選択し、チャネルはロックされません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

channel-number: 数字でチャネルを指定します。この引数の値の範囲は、地域コードおよび無線モードにより異なります。

auto lock: AP が自動的に無線チャネルを選択し、チャネルをロックするよう設定します。

auto unlock: AP が自動的に無線チャネルを選択し、チャネルをロックしないよう設定します。

説明

channel コマンドは無線の動作チャネルを設定します。

undo channel コマンドはデフォルトに戻します。

無線の作動チャネル上でレーダ信号が検出されると、チャネルが手動で指定されているか自動的に割り当てられているかにかかわらず、無線は使用中のチャネルを変更します。30 分後、変更前に使用していたチャネルに戻り、静止タイマを起動します。静止時間内にレーダ信号が検出されなければ、無線はそのチャネルの使用を開始します。静止時間内にレーダ信号が検出されると、無線は再びチャネルを変更します。

例

AP **ap1** の動作チャネルを **48** に指定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] channel 48

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、動作チャネルを **48** に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] channel 48

2.1.9 channel auto-select

Syntax

channel auto-select { **blacklist** | **whitelist** } *channel-number*

undo channel auto-select { **blacklist** | **whitelist** } { **all** | *channel-number* }

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、チャネル選択のブラックリストまたはホワイトリストは存在しません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

blacklist: チャネル選択ブラックリストにチャネルを追加します。AP はブラックリストにあるチャネルを選択しません。

whitelist: チャネル選択ホワイトリストにチャネルを追加します。AP はホワイトリストにあるチャネルのみを選択します。

channel-number: チャネル番号によりチャネルを指定します。この引数の値の範囲は、地域コードおよび無線モードにより異なります。

all: チャネル選択ブラックリストまたはホワイトリストのすべてのチャネルを指定します。

説明

channel auto-select コマンドはチャネル選択のブラックリストまたはホワイトリストを設定します。

undo channel auto-select コマンドはブラックリストまたはホワイトリストから指定したチャネルを削除します。

同じ AP に対してブラックリストとホワイトリストの両方にチャネル選択を設定することはできません。

この機能は、AP が自動チャネル選択モードで作動する場合に限り有効になります。

例

AP **ap1** のチャネル選択ホワイトリストにチャネル 56、60、64 を追加します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] channel auto-select whitelist 56 60 64

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、チャネル選択ホワイトリストにチャネル 56、60、64 を追加します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] channel auto-select whitelist 56 60 64

関連コマンド

channel

2.1.10 channel band-width

🕮 **メモ：**

- QX-W1240 は、320MHz 帯域幅モードをサポートしていません。
- QX-W1210、QX-W1230 の 320MHz 帯域幅モードの設定は、ソフトウェアバージョン 7.2.89 を含む以降のソフトウェアからサポートしています。

Syntax

channel band-width { **20** | **40** [**auto-switch**] | **80** | **160 320** }

undo channel band-width

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、帯域幅モードは 802.11be/eax では 160MHz、802.11ac/ax/abe では 80MHz、802.11an では 40MHz、802.11gac/gax/gbe/gn では 20MHz です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

20: 帯域幅を 20 MHz に設定します。

40: 帯域幅を 40 MHz に設定します。

80: 帯域幅を 80 MHz に設定します。

160: 帯域幅を 160 MHz に設定します。

320: 帯域幅を 320 MHz に設定します。

🕮 **メモ：**

160MHz は QX-W1130 の Radio1、QX-W1200 シリーズのみでサポートします。

auto-switch: 無線が 20MHz から 40MHz の間で帯域幅モードを切り替えることを許可します。このキーワードは、802.11g、802.11gac、802.11gax にのみ適用されます。

説明

channel band-width コマンドは帯域幅モードを設定します。

undo channel band-width コマンドはデフォルトに戻します。

本コマンドは 802.11n、802.11ac、802.11ax、802.11gac、802.11gax 無線にのみ適用可能です。無線モードを変更すると、新しい無線モードでは、本コマンドのデフォルト設定に戻ります。

帯域幅モードが 40MHz の場合、ボンディングできる 2 つの隣接したチャネルが存在する場合は、無線は 40MHz の帯域を使用します。ボンディングできる隣接チャネルがない場合は、無線は 20MHz の帯域を使用します。

帯域幅モードが 80MHz の場合、ボンディングできる隣接したチャネルが存在する場合は、無線は 80MHz の帯域を使用します。80MHz にボンディングできる隣接チャネルはないが、40MHz チャネルにボンディングできる 2 つの隣接チャネルが存在する場合は、40MHz の帯域が使用されます。隣接するチャネルがない場合は、無線は 20MHz の帯域を使用します。

帯域幅モードが 160MHz の場合、ボンディングできる隣接したチャネルが存在する場合は、無線は 160MHz の帯域を使用します。160MHz にボンディングできる隣接チャネルはないが、80MHz チャネルにボンディングできる 2 つの隣接チャネルが存在する場合は、80MHz の帯域が使用されます。隣接するチャネルがない場合は、無線は 20MHz の帯域を使用します。

radio view の設定は、AP group radio view の設定に優先します。

例

AP ap1 の帯域幅モードを 40MHaz に設定します。

<AC> system-view

[AC] wlan ap **ap1** model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] channel band-width 40

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、帯域幅モードを 40MHz に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] channel band-width 40

2.1.11 channel-usage measure

Syntax

channel-usage measure

View

Radio view

定義済みユーザロール

network-admin

説明

channel-usage measure コマンドはオンデマンドチャネル使用量測定を実行します。

この機能により、AP はサポートされているチャネルをスキャンし、スキャン後にチャネルの使用状況を表示できます。チャネルをスキャンするのに約 1 秒かかります。

例

AP **ap1** の無線 2 でオンデマンドのチャネル使用状況測定を実行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] channel-usage measure

```
Please wait......Done.
Channel  Usage
1        63%
2        61%
3        55%
4        45%
5        64%
6        74%
7        66%
8        48%
9        35%
10       38%
11       54%
12       30%
13       72%
```

2.1.12 channel-usage threshold

メモ：

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

channel-usage threshold *threshold*

undo channel-usage threshold

デフォルト

90%

View

Radio view

定義済みユーザロール

network-admin

パラメータ

threshold:チャネル使用率アラームしきい値をパーセンテージで指定します。値の範囲は 5 から 100 です。

説明

channel-usage threshold コマンドはチャネル使用率アラームしきい値を設定します。

undo channel-usage threshold コマンドはデフォルトに戻します。

チャネル使用率がしきい値を超えると、装置は info-center にアラームを報告します。

例

AP **ap1** の Radio1 のチャネル使用率アラームしきい値を 20%に設定します。

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] channel-usage threshold 20

2.1.13 client dot11ac-only

Syntax

client dot11ac-only { **disable** | **enable** }

undo client dot11ac-only

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、無効。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 802.11ac クライアント限定アクセスを無効にします。

enable: 802.11ac クライアント限定アクセスを有効にします。

説明

client dot11ac-only enable コマンドは 802.11ac 無線で 802.11ac クライアントの接続のみを許可し、802.11ax 無線で 802.11ac/ax クライアントの接続のみを許可します。

client dot11ac-only disable コマンドは 802.11ac クライアントを無効にします。

undo client dot11ac-only コマンドはデフォルトに戻します。

本コマンドは 802.11ac/ax 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g、802.11n に変更すると、本コマンドは無効になります。

本コマンドを有効にすると、802.11ac/ax 以外のクライアントはログオフされます。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、802.11ac クライアントにのみアクセスを許可します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ac

[AC-wlan-ap-ap1-radio-1] client dot11ac-only enable

AP グループ apgroup1 の型番 **QX-W1020** の AP で、802.11ac クライアントにのみアクセスを許可します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] client dot11ac-only enable

関連コマンド

dot11ac mandatory maximum-nss

2.1.14 client dot11ax-only

Syntax

client dot11ax-only { **disable** | **enable** }

undo client dot11ax-only

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、無効。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 802.11ax クライアント限定アクセスを無効にします。

enable: 802.11ax クライアント限定アクセスを有効にします。

説明

client dot11ax-only enable コマンドは 802.11ax 無線で 802.11ax クライアントの接続のみを許可します。

client dot11ax-only disable コマンドは 802.11ax クライアント限定アクセスを無効にします。

undo client dot11ax-only コマンドはデフォルトに戻します。

本コマンドは 802.11ax 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g、802.11n、802.11ac に変更すると、コマンドは無効になります。

本コマンドを有効にすると、802.11ax 以外のクライアントはログオフされます。

radio view の設定は、AP group radio view の設定に優先します。

関連コマンド

dot11ax mandatory maximum-nss

2.1.15 client dot11b-forbidden

Syntax

client dot11b-forbidden { **disable** | **enable** }

undo client dot11b-forbidden

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、無効。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

mdc-admin

パラメータ

disable: 802.11b クライアント拒否を無効にします。

enable: 802.11b クライアント拒否を有効にします。

説明

client dot11b-forbidden enable コマンドは 802.11b クライアントの接続を拒否します。

client dot11b-forbidden disable コマンドは 802.11b クライアント拒否を無効にします。

undo client dot11b-forbidden コマンドはデフォルトに戻します。

802.11g または 802.11gn 無線で 802.11b クライアントを拒否することにより、低速な 802.11b クライアントの影響を減少させ、無線データ転送を高速化することができます。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、802.11b クライアントを拒否します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] client dot11b-forbidden enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、802.11b クライアントを拒否します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-model-QX-W1020-radio-1] client dot11b-forbidden enable

2.1.16 client dot11n-only

Syntax

client dot11n-only { **disable** | **enable** }

undo client dot11n-only

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、無効。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 802.11n/ac/ax クライアント限定アクセスを無効にします。

enable: 802.11n/ac/ax クライアント限定アクセスを有効にします。

説明

client dot11n-only enable コマンドは 802.11ac 無線で 802.11an/ac クライアントの接続のみを許可し、802.11ax 無線で 802.11an/ac/ax クライアントの接続のみを許可します。

client dot11n-only disable コマンドは 802.11n および 802.11ac/ax クライアントを無効にします。

undo client dot11n-only コマンドはデフォルトに戻します。

本コマンドは 802.11n、802.11ac、802.11ax 無線にのみ適用可能です。無線モードを 802.11a/b/g に変更することで、本機能は無効になります。

本コマンド有効にすると、802.11a/b/g クライアントはログオフされます。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、802.11n/ac/ax クライアント限定アクセスを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] client dot11n-only enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、802.11n/ac/ax クライアント限定アクセスを有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] client dot11n-only enable

2.1.17 client max-count

Syntax

client max-count *max-number*

undo client max-count

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、AP に接続できるクライアント数に制限はありません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

max-number: AP に接続できるクライアントの最大数を指定します。この引数の値の範囲は、AP モデルによって異なります。

説明

client max-count コマンドは AP に接続できるクライアントの最大数を設定します。

undo client max-count コマンドはデフォルトに戻します。

クライアント数が最大に達すると、AP は新しいクライアントの許可を停止します。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、AP に接続できるクライアントの最大数を 38 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] client max-count 38

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、AP に接続できるクライアントの最大数を 38 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] client max-count 38

2.1.18 continuous-mode

Syntax

continuous-mode { **mcs** *mcs-index* | **nss** *nss-index* **vht-mcs** *vhtmcs-index* | **rate** *rate-value* }

undo continuous-mode

デフォルト

無効

View

Radio view

定義済みユーザロール

network-admin

パラメータ

mcs *mcs-index*: 0〜76 の範囲の MCS インデックスを指定します。このオプションは、802.11n、802.11ac、および 802.11gac 無線にのみ適用されます。

nss *nss-index* **vht-mcs** *vhtmcs-index*: VHT-MCS インデックスを指定します。nss-index および vhtmcs-index 引数の値の範囲は、それぞれ 1〜8 および 0〜9 です。このオプションは、802.11ac および 802.11gac 無線にのみ適用されます。

rate *rate-value*: 送信レートを Mbps で指定します。このオプションは、すべての無線タイプに適用されます。

説明

continuous-mode コマンドは無線の連続モードを有効にします。

undo continuous-mode コマンドはデフォルトに戻します。

この機能はネットワークテストにのみ使用されます。それ以外の環境では使用しないでください。

指定されたレートで連続データパケット送信を可能にします。この機能が有効になっているときは、送信レートを変更する以外の操作は実行しないでください。

例

連続モードを有効にし、送信レートを 6 Mbps に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] continuous-mode rate 6

関連コマンド

display wlan ap continuous-mode

2.1.19 custom antenna gain

Syntax

custom-antenna gain *antenna-gain*

undo custom-antenna gain

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、アンテナゲインは 0dBi です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

antenna-gain: アンテナゲインを指定します。範囲は 0～20dBi です。

説明

重要：

本コマンドは、AP がサードパーティのアンテナを使用している場合のみ適用可能です。

custom antenna-gain コマンドはアンテナゲインを設定します。

undo antenna-gain コマンドはデフォルトに戻します。

AP がサードパーティーアンテナを使用する場合、AP が使用するアンテナのゲインに対し、アンテナゲインを設定しなければなりません。

効果的等方性放射電力（EIRP）は、アンテナの実質的な伝送電力であり、無線のアンテナゲインと最大伝送電力の合計です。設定したアンテナゲインが原因で EIRP がしきい値を超過した場合、アンテナゲインの設定に失敗します。

無線モードを変更すると、アンテナゲインが自動的に変更されます。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、アンテナゲインを 2dBi に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] custom-antenna gain 2

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、アンテナゲインを 2dBi に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] custom-antenna gain 2

2.1.20 display wlan ap continuous-mode

Syntax

display wlan ap { **all** | **name** *ap-name* } **continuous-mode**

View

Any view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

説明

display wlan ap continuous-mode コマンドは連続モードに関する情報を表示します。

例

AP **ap1** の無線の連続モードに関する情報を表示します。

<AC> display wlan ap name ap1 continuous-mode

```
AP name    Radio ID    Radio type      Rate    Mcs-Index   Nss   Vht-mcs
ap1        1           802.11a         6       N/A         N/A   N/A
```

表 2-1 コマンド出力

フィールド	説明
Mcs-Index	MCS index.
Nss	NSS index.
Vht-mcs	VHT-MCS index.

関連コマンド

continuous-mode

2.1.21 display wlan ap radio

Syntax

display wlan ap all radio [**frequency-band** { **5** | **2.4** }]

View

Any view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

frequency-band: 周波数帯を指定します。

5: 5GHz 周波数帯を指定します。

2.4: 2.4GHz 周波数帯を指定します。

説明

display wlan ap radio コマンドは AP 無線情報を表示します。

例

すべての AP の無線情報を表示します。

<AC> display wlan ap all radio

```
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 32
Remaining APs: 31
Total AP licenses: 20
Remaining AP licenses: 19

AP name              RID State Channel        Usage TxPower AntGain EIRP
```

```
                                                (%)   (dBm)   (dBi)   (dBm)
ap1                    1   Up    48(auto)       10     20      10      30
```

すべての AP の 2.4 GHz 無線情報を表示します。

<AC> display wlan ap all radio frequency-band 2.4

```
AP name                RID State Channel         Usage TxPower AntGain EIRP
                                                 (%)   (dBm)   (dBi)   (dBm)
ap1                    2   Up    104(auto)       15     20      10      30
```

表 2-2 コマンド出力

フィールド	説明
Total number of inside APs	内部APは、アンカーAPがACとして動作するときに無線管理のために自動的に作成される手動APです。内部APの名前とシリアルIDは、アンカーAPのMACアドレスとシリアルIDです。
Total number of connected WTUs	このフィールドは、将来の使用のために予約されています。
Maximum supported APs	AC上のサポートされているAPの最大数です。
Remaining APs	サポートされているAPの残りの数です。
Total AP licenses	APライセンスの総数です。
Remaining AP licenses	残りのAPライセンスの数です。
State	無線状態: • Up. • Down.
Usage	使用チャネルです。
TxPower (dBm)	送信電力です。デフォルトでは、サポートされる最大電力がパケットの送信に使用されます。
AntGain (dBi)	アンテナ利得です。
EIRP (dBm)	効果的な等方放射電力です。

2.1.22 display wlan ap radio channel

Syntax

display wlan ap { **all** | **name** *ap-name* } **radio channel**

View

Any view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

説明

display wlan ap radio channel コマンドは無線チャネル情報を表示します。

例

AP **ap3** の無線チャネル情報を表示します。

<AC> display wlan ap name ap3 radio channel

```
AP name                RID Channel         Band-width          CenterFreq
                                          (MHz)
ap3                    1  36(auto)         20/40/80/160/(80+80) 42/58
ap3                    2  120              20/40/80            155
```

表 2-3 コマンド出力

フィールド	説明
Band-width (MHz)	サポートされるチャネル帯域幅です。
CenterFreq	中央周波数です。このフィールドは、サポートされているチャネル帯域幅が80MHzに達した場合にのみ使用できます。このフィールドには、160MHzまたは80+80MHzの帯域幅がサポートされている場合のメインチャネルとセカンダリチャネルの中心周波数が表示されます。

2.1.23 display wlan ap radio type

Syntax

display wlan ap { **all** | **name** *ap-name* } **radio type**

View

Any view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

説明

display wlan ap radio type コマンドは無線タイプ情報を表示します。

例

AP **ap1** の無線タイプ情報を表示します。

<AC> display wlan ap name ap1 radio type

```
AP name               RID  AP state  Radio state  Radio type
ap1                   1    Up       Up          802.11n(5GHz)
ap1                   2    Up       Down        802.11n(2.4GHz)
```

表 2-4 コマンド出力

フィールド	説明
AP state	APの状態: ● **Up**–APはACとCAPWAPトンネルを確立しました。 ● **Down**–APはACとCAPWAPトンネルを確立していません。
Radio state	無線状態: ● Up. ● Down.

2.1.24 display wlan statistics ap radio

Syntax

display wlan statistics ap { **all** | **name** *ap-name* } **radio**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap: AP を指定します。

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan statistics ap radio コマンドは無線統計情報を表示します。

例

#AP ap1 の無線統計情報を表示します

```
<AC>display wlan statistics ap name ap1 radio
                        Radio statistics
--------------------------------------------------------------------------------
 AP name:ap1                                Radio ID:1
--------------------------------------------------------------------------------
Transmitted frame statistics:
  Total frames                        :176
  Total frame bytes                    :45205
  Unicast frames                      :31
  Unicast frame bytes                  :8085
  Broadcast/Multicast frames            :184
  Broadcast/Multicast frame bytes       :39664
  Other frames                        :18446744073709551577
  Other frame bytes                    :18446744073709549072

  Discarded frames                    :35
  Failed RTS frames                    :0
  Retransmissions                     :0
  Successful RTS frames                :0
  Retransmitted frames                 :0
  No-ACK frames                       :0
  Authentication frames                :1
  Association frames                   :1
```

```
 Packet statistics by size:
   Smaller than or equal to 128         :72
   Between 128 and 512 (inclusive)      :89
   Between 512 and 1024 (inclusive)     :0
   Larger than 1024                   :0

 Packet statistics by rate:
     1 Mbps  :0          2 Mbps  :0
   5.5 Mbps  :0          6 Mbps  :2
     9 Mbps  :0         11 Mbps  :0
    12 Mbps  :0         18 Mbps  :0
    24 Mbps  :0         36 Mbps  :0
    48 Mbps  :0         54 Mbps  :0

 Packet statistics based on data rate:
  6.5 Mbps  :0                      7.2 Mbps  :0
   13 Mbps  :0                     13.5 Mbps  :0
 14.4 Mbps  :0                       15 Mbps  :0
 19.5 Mbps  :0                     21.7 Mbps  :0
   26 Mbps  :0                       27 Mbps  :0
 28.9 Mbps  :0                     29.3 Mbps  :0
   30 Mbps  :0                     32.5 Mbps  :0
   39 Mbps  :0                     40.5 Mbps  :0
 43.3 Mbps  :0                       45 Mbps  :0
   52 Mbps  :0                       54 Mbps  :0
 57.8 Mbps  :0                     58.5 Mbps  :0
   60 Mbps  :0                       65 Mbps  :0
 72.2 Mbps  :0                       78 Mbps  :0
   81 Mbps  :0                     86.5 Mbps  :0
 86.7 Mbps  :0                     87.8 Mbps  :0
   90 Mbps  :0                       96 Mbps  :0
 97.5 Mbps  :0                      104 Mbps  :0
  108 Mbps  :0                    115.6 Mbps  :0
  117 Mbps  :0                      120 Mbps  :0
121.5 Mbps  :0                      130 Mbps  :0
  135 Mbps  :0                    144.4 Mbps  :0
  150 Mbps  :0                      156 Mbps  :0
  162 Mbps  :0                      173 Mbps  :0
173.3 Mbps  :0                    175.5 Mbps  :0
  180 Mbps  :0                      192 Mbps  :0
  195 Mbps  :0                      200 Mbps  :0
  208 Mbps  :0                      216 Mbps  :0
```

```
 216.7 Mbps  :0                    231.1 Mbps  :0
   234 Mbps  :0                      240 Mbps  :0
   243 Mbps  :0                      260 Mbps  :0
   263 Mbps  :0                    263.3 Mbps  :0
   270 Mbps  :0                    288.9 Mbps  :0
 292.5 Mbps  :0                      300 Mbps  :0
   312 Mbps  :0                      324 Mbps  :0
   325 Mbps  :0                      344 Mbps  :0
 346.7 Mbps  :0                      351 Mbps  :0
   360 Mbps  :0                    364.5 Mbps  :0
   390 Mbps  :0                      400 Mbps  :0
   405 Mbps  :0                      432 Mbps  :0
 433.3 Mbps  :0                      450 Mbps  :0
   468 Mbps  :0                      480 Mbps  :0
   486 Mbps  :0                      520 Mbps  :0
 526.5 Mbps  :0                      540 Mbps  :0
   585 Mbps  :0                      600 Mbps  :0
   648 Mbps  :0                      650 Mbps  :0
   702 Mbps  :0                      720 Mbps  :0
   780 Mbps  :0                    789.9 Mbps  :0
   800 Mbps  :0                    866.7 Mbps  :0
 877.5 Mbps  :0                      936 Mbps  :0
   975 Mbps  :0                     1040 Mbps  :0
  1053 Mbps  :0                     1170 Mbps  :0
  1300 Mbps  :0                     1404 Mbps  :0
  1560 Mbps  :0                    1733.3 Mbps  :0
-------------------------------------------------------------------------------
Received frame statistics:
   Total frames                          :4232
   Total frame bytes                      :1011302
   Unicast frames                        :861
   Unicast frame bytes                    :185001
   Broadcast/Multicast frames              :3371
   Broadcast/Multicast frame bytes         :821056
   Fragmented frames                     :0
   Duplicate frames                      :0
   FCS failures                          :0
   Decryption errors                      :0
   Authentication frames                  :0
   Association frames                    :0

   Packet statistics by size:
     Smaller than or equal to 128        :322
```

```
    Between 128 and 512 (inclusive)      :3910
    Between 512 and 1024 (inclusive)     :0
    Larger than 1024                  :0

  Packet statistics by rate:
     1 Mbps  :0          2 Mbps  :0
   5.5 Mbps  :0          6 Mbps  :5
     9 Mbps  :0         11 Mbps  :0
    12 Mbps  :0         18 Mbps  :0
    24 Mbps  :0         36 Mbps  :0
    48 Mbps  :0         54 Mbps  :19

  Packet statistics based on data rate:
   6.5 Mbps  :0                      7.2 Mbps  :0
    13 Mbps  :0                     13.5 Mbps  :0
  14.4 Mbps  :0                       15 Mbps  :0
  19.5 Mbps  :0                     21.7 Mbps  :0
    26 Mbps  :0                       27 Mbps  :0
  28.9 Mbps  :0                     29.3 Mbps  :0
    30 Mbps  :0                     32.5 Mbps  :0
    39 Mbps  :0                     40.5 Mbps  :0
  43.3 Mbps  :0                       45 Mbps  :0
    52 Mbps  :0                       54 Mbps  :19
  57.8 Mbps  :0                     58.5 Mbps  :0
    60 Mbps  :0                       65 Mbps  :0
  72.2 Mbps  :0                       78 Mbps  :0
    81 Mbps  :0                     86.5 Mbps  :0
  86.7 Mbps  :0                     87.8 Mbps  :0
    90 Mbps  :0                       96 Mbps  :0
  97.5 Mbps  :0                      104 Mbps  :0
   108 Mbps  :0                    115.6 Mbps  :0
   117 Mbps  :8                      120 Mbps  :0
 121.5 Mbps  :0                      130 Mbps  :0
   135 Mbps  :0                    144.4 Mbps  :0
   150 Mbps  :0                      156 Mbps  :0
   162 Mbps  :0                      173 Mbps  :0
 173.3 Mbps  :0                    175.5 Mbps  :4
   180 Mbps  :0                      192 Mbps  :0
   195 Mbps  :0                      200 Mbps  :0
   208 Mbps  :0                      216 Mbps  :0
 216.7 Mbps  :0                    231.1 Mbps  :0
   234 Mbps  :0                      240 Mbps  :0
   243 Mbps  :0                      260 Mbps  :0
```

```
  263 Mbps  :0                    263.3 Mbps  :0
  270 Mbps  :0                    288.9 Mbps  :0
292.5 Mbps  :0                      300 Mbps  :0
  312 Mbps  :0                      324 Mbps  :0
  325 Mbps  :0                      344 Mbps  :0
346.7 Mbps  :0                      351 Mbps  :0
  360 Mbps  :0                    364.5 Mbps  :0
  390 Mbps  :0                      400 Mbps  :0
  405 Mbps  :0                      432 Mbps  :0
433.3 Mbps  :0                      450 Mbps  :0
  468 Mbps  :0                      480 Mbps  :0
  486 Mbps  :0                      520 Mbps  :0
526.5 Mbps  :0                      540 Mbps  :0
  585 Mbps  :0                      600 Mbps  :0
  648 Mbps  :0                      650 Mbps  :0
  702 Mbps  :0                      720 Mbps  :0
  780 Mbps  :0                    789.9 Mbps  :0
  800 Mbps  :0                    866.7 Mbps  :0
877.5 Mbps  :0                      936 Mbps  :0
  975 Mbps  :0                     1040 Mbps  :0
 1053 Mbps  :0                     1170 Mbps  :0
 1300 Mbps  :0                     1404 Mbps  :0
 1560 Mbps  :0                   1733.3 Mbps  :0
--------------------------------------------------------------------------------
                         Radio statistics
--------------------------------------------------------------------------------
 AP name:ap1                                Radio ID:2
--------------------------------------------------------------------------------
Transmitted frame statistics:
   Total frames                        :0
   Total frame bytes                    :0
   Unicast frames                      :0
   Unicast frame bytes                  :0
   Broadcast/Multicast frames            :0
   Broadcast/Multicast frame bytes       :0
   Other frames                        :0
   Other frame bytes                    :0

   Discarded frames                    :0
   Failed RTS frames                    :0
   Retransmissions                     :0
   Successful RTS frames                :0
   Retransmitted frames                 :0
```

```
No-ACK frames                        :0
Authentication frames                 :0
Association frames                   :0

Packet statistics by size:
  Smaller than or equal to 128        :0
  Between 128 and 512 (inclusive)     :0
  Between 512 and 1024 (inclusive)    :0
  Larger than 1024                   :0

Packet statistics by rate:
    1 Mbps  :0          2 Mbps  :0
  5.5 Mbps  :0          6 Mbps  :0
    9 Mbps  :0         11 Mbps  :0
   12 Mbps  :0         18 Mbps  :0
   24 Mbps  :0         36 Mbps  :0
   48 Mbps  :0         54 Mbps  :0

Packet statistics based on data rate:
 6.5 Mbps  :0                       7.2 Mbps  :0
  13 Mbps  :0                      13.5 Mbps  :0
14.4 Mbps  :0                        15 Mbps  :0
19.5 Mbps  :0                      21.7 Mbps  :0
  26 Mbps  :0                        27 Mbps  :0
28.9 Mbps  :0                      29.3 Mbps  :0
  30 Mbps  :0                      32.5 Mbps  :0
  39 Mbps  :0                      40.5 Mbps  :0
43.3 Mbps  :0                        45 Mbps  :0
  52 Mbps  :0                        54 Mbps  :0
57.8 Mbps  :0                      58.5 Mbps  :0
  60 Mbps  :0                        65 Mbps  :0
72.2 Mbps  :0                        78 Mbps  :0
  81 Mbps  :0                      86.5 Mbps  :0
86.7 Mbps  :0                      87.8 Mbps  :0
  90 Mbps  :0                        96 Mbps  :0
97.5 Mbps  :0                       104 Mbps  :0
 108 Mbps  :0                     115.6 Mbps  :0
 117 Mbps  :0                       120 Mbps  :0
121.5 Mbps  :0                      130 Mbps  :0
 135 Mbps  :0                     144.4 Mbps  :0
 150 Mbps  :0                       156 Mbps  :0
 162 Mbps  :0                       173 Mbps  :0
173.3 Mbps  :0                    175.5 Mbps  :0
```

```
   180 Mbps  :0                      192 Mbps  :0
   195 Mbps  :0                      200 Mbps  :0
   208 Mbps  :0                      216 Mbps  :0
 216.7 Mbps  :0                    231.1 Mbps  :0
   234 Mbps  :0                      240 Mbps  :0
   243 Mbps  :0                      260 Mbps  :0
   263 Mbps  :0                    263.3 Mbps  :0
   270 Mbps  :0                    288.9 Mbps  :0
 292.5 Mbps  :0                      300 Mbps  :0
   312 Mbps  :0                      324 Mbps  :0
   325 Mbps  :0                      344 Mbps  :0
 346.7 Mbps  :0                      351 Mbps  :0
   360 Mbps  :0                    364.5 Mbps  :0
   390 Mbps  :0                      400 Mbps  :0
   405 Mbps  :0                      432 Mbps  :0
 433.3 Mbps  :0                      450 Mbps  :0
   468 Mbps  :0                      480 Mbps  :0
   486 Mbps  :0                      520 Mbps  :0
 526.5 Mbps  :0                      540 Mbps  :0
   585 Mbps  :0                      600 Mbps  :0
   648 Mbps  :0                      650 Mbps  :0
   702 Mbps  :0                      720 Mbps  :0
   780 Mbps  :0                    789.9 Mbps  :0
   800 Mbps  :0                    866.7 Mbps  :0
 877.5 Mbps  :0                      936 Mbps  :0
   975 Mbps  :0                     1040 Mbps  :0
  1053 Mbps  :0                     1170 Mbps  :0
  1300 Mbps  :0                     1404 Mbps  :0
  1560 Mbps  :0                   1733.3 Mbps  :0
-------------------------------------------------------------------------------
--
Received frame statistics:
   Total frames                        :0
   Total frame bytes                    :0
   Unicast frames                      :0
   Unicast frame bytes                  :0
   Broadcast/Multicast frames            :0
   Broadcast/Multicast frame bytes        :0
   Fragmented frames                   :0
   Duplicate frames                    :0
   FCS failures                        :0
   Decryption errors                    :0
   Authentication frames                :0
```

```
 Association frames                  :0

 Packet statistics by size:
   Smaller than or equal to 128        :0
   Between 128 and 512 (inclusive)     :0
   Between 512 and 1024 (inclusive)    :0
   Larger than 1024                  :0

 Packet statistics by rate:
     1 Mbps  :0          2 Mbps  :0
   5.5 Mbps  :0          6 Mbps  :0
     9 Mbps  :0         11 Mbps  :0
    12 Mbps  :0         18 Mbps  :0
    24 Mbps  :0         36 Mbps  :0
    48 Mbps  :0         54 Mbps  :0

 Packet statistics based on data rate:
  6.5 Mbps  :0                      7.2 Mbps  :0
   13 Mbps  :0                     13.5 Mbps  :0
 14.4 Mbps  :0                       15 Mbps  :0
 19.5 Mbps  :0                     21.7 Mbps  :0
   26 Mbps  :0                       27 Mbps  :0
 28.9 Mbps  :0                     29.3 Mbps  :0
   30 Mbps  :0                     32.5 Mbps  :0
   39 Mbps  :0                     40.5 Mbps  :0
 43.3 Mbps  :0                       45 Mbps  :0
   52 Mbps  :0                       54 Mbps  :0
 57.8 Mbps  :0                     58.5 Mbps  :0
   60 Mbps  :0                       65 Mbps  :0
 72.2 Mbps  :0                       78 Mbps  :0
   81 Mbps  :0                     86.5 Mbps  :0
 86.7 Mbps  :0                     87.8 Mbps  :0
   90 Mbps  :0                       96 Mbps  :0
 97.5 Mbps  :0                      104 Mbps  :0
  108 Mbps  :0                    115.6 Mbps  :0
  117 Mbps  :0                      120 Mbps  :0
121.5 Mbps  :0                      130 Mbps  :0
  135 Mbps  :0                    144.4 Mbps  :0
  150 Mbps  :0                      156 Mbps  :0
  162 Mbps  :0                      173 Mbps  :0
173.3 Mbps  :0                    175.5 Mbps  :0
  180 Mbps  :0                      192 Mbps  :0
  195 Mbps  :0                      200 Mbps  :0
```

```
  208 Mbps  :0                    216 Mbps  :0
 216.7 Mbps  :0                   231.1 Mbps  :0
  234 Mbps  :0                    240 Mbps  :0
  243 Mbps  :0                    260 Mbps  :0
  263 Mbps  :0                   263.3 Mbps  :0
  270 Mbps  :0                   288.9 Mbps  :0
 292.5 Mbps  :0                   300 Mbps  :0
  312 Mbps  :0                    324 Mbps  :0
  325 Mbps  :0                    344 Mbps  :0
 346.7 Mbps  :0                   351 Mbps  :0
  360 Mbps  :0                   364.5 Mbps  :0
  390 Mbps  :0                    400 Mbps  :0
  405 Mbps  :0                    432 Mbps  :0
 433.3 Mbps  :0                   450 Mbps  :0
  468 Mbps  :0                    480 Mbps  :0
  486 Mbps  :0                    520 Mbps  :0
 526.5 Mbps  :0                   540 Mbps  :0
  585 Mbps  :0                    600 Mbps  :0
  648 Mbps  :0                    650 Mbps  :0
  702 Mbps  :0                    720 Mbps  :0
  780 Mbps  :0                   789.9 Mbps  :0
  800 Mbps  :0                   866.7 Mbps  :0
 877.5 Mbps  :0                   936 Mbps  :0
  975 Mbps  :0                   1040 Mbps  :0
 1053 Mbps  :0                   1170 Mbps  :0
 1300 Mbps  :0                   1404 Mbps  :0
 1560 Mbps  :0                  1733.3 Mbps  :0
--------------------------------------------------------------------------------
                        Radio statistics
--------------------------------------------------------------------------------
 AP name:ap1                                Radio ID:3
--------------------------------------------------------------------------------
Transmitted frame statistics:
   Total frames                        :0
   Total frame bytes                    :0
   Unicast frames                      :0
   Unicast frame bytes                  :0
   Broadcast/Multicast frames            :0
   Broadcast/Multicast frame bytes        :0
   Other frames                        :0
   Other frame bytes                    :0

   Discarded frames                     :0
```

```
 Failed RTS frames                    :0
 Retransmissions                      :0
 Successful RTS frames                :0
 Retransmitted frames                 :0
 No-ACK frames                        :0
 Authentication frames                :0
 Association frames                   :0

 Packet statistics by size:
   Smaller than or equal to 128       :0
   Between 128 and 512 (inclusive)    :0
   Between 512 and 1024 (inclusive)   :0
   Larger than 1024                   :0

 Packet statistics by rate:
     1 Mbps  :0          2 Mbps  :0
   5.5 Mbps  :0          6 Mbps  :0
     9 Mbps  :0         11 Mbps  :0
    12 Mbps  :0         18 Mbps  :0
    24 Mbps  :0         36 Mbps  :0
    48 Mbps  :0         54 Mbps  :0

 Packet statistics based on data rate:
  6.5 Mbps  :0                      7.2 Mbps  :0
   13 Mbps  :0                     13.5 Mbps  :0
 14.4 Mbps  :0                       15 Mbps  :0
 19.5 Mbps  :0                     21.7 Mbps  :0
   26 Mbps  :0                       27 Mbps  :0
 28.9 Mbps  :0                     29.3 Mbps  :0
   30 Mbps  :0                     32.5 Mbps  :0
   39 Mbps  :0                     40.5 Mbps  :0
 43.3 Mbps  :0                       45 Mbps  :0
   52 Mbps  :0                       54 Mbps  :0
 57.8 Mbps  :0                     58.5 Mbps  :0
   60 Mbps  :0                       65 Mbps  :0
 72.2 Mbps  :0                       78 Mbps  :0
   81 Mbps  :0                     86.5 Mbps  :0
 86.7 Mbps  :0                     87.8 Mbps  :0
   90 Mbps  :0                       96 Mbps  :0
 97.5 Mbps  :0                      104 Mbps  :0
  108 Mbps  :0                    115.6 Mbps  :0
  117 Mbps  :0                      120 Mbps  :0
121.5 Mbps  :0                      130 Mbps  :0
```

```
   135 Mbps  :0                    144.4 Mbps  :0
   150 Mbps  :0                     156 Mbps  :0
   162 Mbps  :0                     173 Mbps  :0
 173.3 Mbps  :0                   175.5 Mbps  :0
   180 Mbps  :0                     192 Mbps  :0
   195 Mbps  :0                     200 Mbps  :0
   208 Mbps  :0                     216 Mbps  :0
 216.7 Mbps  :0                   231.1 Mbps  :0
   234 Mbps  :0                     240 Mbps  :0
   243 Mbps  :0                     260 Mbps  :0
   263 Mbps  :0                   263.3 Mbps  :0
   270 Mbps  :0                   288.9 Mbps  :0
 292.5 Mbps  :0                     300 Mbps  :0
   312 Mbps  :0                     324 Mbps  :0
   325 Mbps  :0                     344 Mbps  :0
 346.7 Mbps  :0                     351 Mbps  :0
   360 Mbps  :0                   364.5 Mbps  :0
   390 Mbps  :0                     400 Mbps  :0
   405 Mbps  :0                     432 Mbps  :0
 433.3 Mbps  :0                     450 Mbps  :0
   468 Mbps  :0                     480 Mbps  :0
   486 Mbps  :0                     520 Mbps  :0
 526.5 Mbps  :0                     540 Mbps  :0
   585 Mbps  :0                     600 Mbps  :0
   648 Mbps  :0                     650 Mbps  :0
   702 Mbps  :0                     720 Mbps  :0
   780 Mbps  :0                   789.9 Mbps  :0
   800 Mbps  :0                   866.7 Mbps  :0
 877.5 Mbps  :0                     936 Mbps  :0
   975 Mbps  :0                    1040 Mbps  :0
  1053 Mbps  :0                    1170 Mbps  :0
  1300 Mbps  :0                    1404 Mbps  :0
  1560 Mbps  :0                   1733.3 Mbps  :0
-------------------------------------------------------------------------------
Received frame statistics:
   Total frames                        :0
   Total frame bytes                    :0
   Unicast frames                      :0
   Unicast frame bytes                  :0
   Broadcast/Multicast frames            :0
   Broadcast/Multicast frame bytes       :0
   Fragmented frames                   :0
   Duplicate frames                    :0
```

```
 FCS failures                          :0
 Decryption errors                     :0
 Authentication frames                 :0
 Association frames                    :0

 Packet statistics by size:
   Smaller than or equal to 128        :0
   Between 128 and 512 (inclusive)     :0
   Between 512 and 1024 (inclusive)    :0
   Larger than 1024                    :0

 Packet statistics by rate:
     1 Mbps  :0          2 Mbps  :0
   5.5 Mbps  :0          6 Mbps  :0
     9 Mbps  :0         11 Mbps  :0
    12 Mbps  :0         18 Mbps  :0
    24 Mbps  :0         36 Mbps  :0
    48 Mbps  :0         54 Mbps  :0

 Packet statistics based on data rate:
  6.5 Mbps  :0                       7.2 Mbps  :0
   13 Mbps  :0                      13.5 Mbps  :0
 14.4 Mbps  :0                        15 Mbps  :0
 19.5 Mbps  :0                      21.7 Mbps  :0
   26 Mbps  :0                        27 Mbps  :0
 28.9 Mbps  :0                      29.3 Mbps  :0
   30 Mbps  :0                      32.5 Mbps  :0
   39 Mbps  :0                      40.5 Mbps  :0
 43.3 Mbps  :0                        45 Mbps  :0
   52 Mbps  :0                        54 Mbps  :0
 57.8 Mbps  :0                      58.5 Mbps  :0
   60 Mbps  :0                        65 Mbps  :0
 72.2 Mbps  :0                        78 Mbps  :0
   81 Mbps  :0                      86.5 Mbps  :0
 86.7 Mbps  :0                      87.8 Mbps  :0
   90 Mbps  :0                        96 Mbps  :0
 97.5 Mbps  :0                       104 Mbps  :0
  108 Mbps  :0                     115.6 Mbps  :0
  117 Mbps  :0                       120 Mbps  :0
121.5 Mbps  :0                       130 Mbps  :0
  135 Mbps  :0                     144.4 Mbps  :0
  150 Mbps  :0                       156 Mbps  :0
  162 Mbps  :0                       173 Mbps  :0
```

```
173.3 Mbps  :0                  175.5 Mbps  :0
  180 Mbps  :0                    192 Mbps  :0
  195 Mbps  :0                    200 Mbps  :0
  208 Mbps  :0                    216 Mbps  :0
216.7 Mbps  :0                  231.1 Mbps  :0
  234 Mbps  :0                    240 Mbps  :0
  243 Mbps  :0                    260 Mbps  :0
  263 Mbps  :0                  263.3 Mbps  :0
  270 Mbps  :0                  288.9 Mbps  :0
292.5 Mbps  :0                    300 Mbps  :0
  312 Mbps  :0                    324 Mbps  :0
  325 Mbps  :0                    344 Mbps  :0
346.7 Mbps  :0                    351 Mbps  :0
  360 Mbps  :0                  364.5 Mbps  :0
  390 Mbps  :0                    400 Mbps  :0
  405 Mbps  :0                    432 Mbps  :0
433.3 Mbps  :0                    450 Mbps  :0
  468 Mbps  :0                    480 Mbps  :0
  486 Mbps  :0                    520 Mbps  :0
526.5 Mbps  :0                    540 Mbps  :0
  585 Mbps  :0                    600 Mbps  :0
  648 Mbps  :0                    650 Mbps  :0
  702 Mbps  :0                    720 Mbps  :0
  780 Mbps  :0                  789.9 Mbps  :0
  800 Mbps  :0                  866.7 Mbps  :0
877.5 Mbps  :0                    936 Mbps  :0
  975 Mbps  :0                   1040 Mbps  :0
 1053 Mbps  :0                   1170 Mbps  :0
 1300 Mbps  :0                   1404 Mbps  :0
 1560 Mbps  :0                  1733.3 Mbps  :0
```

表 2-5 コマンド出力

フィールド	説明
送信フレーム統計情報	
Total frames	プローブ応答とビーコンフレームを含む、送信されたフレームの合計数。
Total frame bytes	プローブ応答とビーコンフレームを含む、送信されたフレームの合計バイト数。
Unicast frames	送信されたユニキャストフレームの総数 (プローブ応答を除く)。
Unicast frame bytes	送信されたユニキャストフレームの合計バイト数 (プローブ応答を除く)。

フィールド	説明
Broadcast/Multicast frames	送信されたブロードキャストおよびマルチキャストフレームの総数（ビーコンフレームを除く）。
Broadcast/Multicast frame bytes	送信されたブロードキャストフレームとマルチキャストフレームの合計バイト数（ビーコンフレームを除く）。
Others frames	他の送信フレームの合計数。
Others frame bytes	他の送信フレームの合計バイト数。
Discarded frames	破棄されたフレームの合計数。
Failed RTS frames	失敗したRTSフレームの合計数。
Retransmissions	再送された回数。
Successful RTS frames	成功したRTSフレームの合計数。
Retransmitted frames	再送されたフレームの合計数。
No-ACK frames	No-ACKフレームの合計数。
Authentication frames	Authenticationフレームの合計数。
Association frames	Associationフレームの合計数
Packet statistics by size	パケットサイズによって分類されたパケットの総数。 Smaller than or equal to 128 ：128バイト以下のパケット数 Between 128 and 512 (inclusive)：129～512バイトのパケット数 Between 512 and 1024 (inclusive)：513～1024バイトのパケット数 Larger than 1024：1024バイトを超えるパケット数
Packet statistics by rate	802.11 a/b/gレートによって分類されたパケットの総数。
Packet statistics based on data rate	802.11 nレートによって分類されたパケットの総数。デバイスが802.11 nをサポートしていない場合、このフィールドは使用できません。
受信フレーム統計情報	
Total frames	受信したフレームの総数。
Total frame bytes	受信したフレームの合計バイト数。
Unicast frames	受信したユニキャストフレームの総数。
Unicast frame bytes	受信したユニキャストフレームの合計バイト数。
Broadcast/Multicast frames	受信したブロードキャストフレームとマルチキャストフレームの総数。

フィールド	説明
Broadcast/Multicast frame bytes	受信したブロードキャストフレームとマルチキャストフレームの合計バイト数。
Fragmented frames	受信したフラグメント化されたフレームの総数。
Duplicate frames	重複受信したフレームの総数
FCS failures	FCSエラーが発生した受信パケットの総数。
Decryption errors	復号化エラーのある受信パケットの合計数。
Authentication frames	受信したAuthenticationフレームの合計数。
Association frames	受信したAssociationフレームの合計数
Packet statistics by size	パケットサイズによって分類された受信パケットの総数。 Smaller than or equal to 128 ：128バイト以下のパケット数 Between 128 and 512 (inclusive)：129～512バイトのパケット数 Between 512 and 1024 (inclusive)：513～1024バイトのパケット数 Larger than 1024：1024バイトを超えるパケット数
Packet statistics by rate	802.11 a/b/gレートによって分類された受信パケットの総数。
Packet statistics based on data rate	802.11 nレートによって分類された受信パケットの総数。デバイスが802.11 nをサポートしていない場合、このフィールドは使用できません。

2.1.25 distance

Syntax

distance *distance*

undo distance

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、最大伝送距離は 1km です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

distance: 最大伝送距離を指定します。範囲は 1～40km です。

説明

distance コマンドは最大伝送距離を設定します。

undo distance コマンドはデフォルトに戻します。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、最大伝送距離を 5km に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] distance 5

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、最大伝送距離を 5km に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] distance 5

2.1.26 dl-ofdma

🕮 **メモ**:

- **dl-ofdma** コマンドはソフトウェアバージョン 7.2.42 を含む以降のソフトウェアからサポートしています。
- **dl-ofdma** コマンドは QX-W1100 シリーズおよび QX-W1200 シリーズでのみサポートしています。

Syntax

dl-ofdma { **disable** | **enable** }

undo dl-ofdma

デフォルト

radio view では、AP group radio view の設定を使用します。

AP group radio view では、ソフトウェアバージョンにより異なります。

ソフトウェアバージョン7.2.55 を含む以前のソフトウェアでは無効(コンフィグ上は非表示)です。

ソフトウェアバージョン7.2.56 を含む以降のソフトウェアでは有効(コンフィグ上は非表示)です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

説明

dl-ofdma enable コマンドはダウンリンク OFDMA を有効にします。

dl-ofdma disable コマンドはダウンリンク OFDMA を無効にします。

undo dl-ofdma コマンドはデフォルトに戻します。

このコマンドは、802.11 ax および 802.11 gax でのみ有効です。無線タイプを 802.11 a/b/g/n/ac/gac に変更すると、設定が削除されます。

Radio view の設定は AP group radio view の設定よりも優先されます。

OFDMA は、小さなデータパケットが送信される高密度環境で有効にすると、次の利点があります。

- 複数ユーザへの同時通信
- 無線使用率の向上
- 転送遅延の短縮
- 衝突バックオフの削減

例

AP ap1 の Radio1 でダウンリンク OFDMA を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ax

[AC-wlan-ap-ap1-radio-1] dl-ofdma enable

AP グループ apgroup1 の AP の Radio1 でダウンリンク OFDMA を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1]ap-model QX-W1130

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] type dot11ax

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] dl-ofdma enable

関連コマンド

type dot11ax

2.1.27 dot11ac mandatory maximum-nss

Syntax

dot11ac mandatory maximum-nss *nss-number*

undo dot11ac mandatory maximum-nss

デフォルト

radio view でのデフォルト設定は以下の通りです。

- 最大サポート NSS が設定されている場合、最大必須 NSS は設定されていません。
- 最大サポート NSS が設定されていない場合、無線は AP group radio view の設定を使用します。

AP group radio view では、最大必須 NSS は設定されていません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

nss-number: 最大必須 NSS を指定します。範囲は 1～8 です。

説明

dot11ac mandatory maximum-nss コマンドは最大必須 NSS を設定します。

undo dot11ac mandatory maximum-nss コマンドはデフォルトに戻します。

本コマンドは、802.11ac、および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g、または 802.11n に変更すると、コマンドが無効になります。

最大必須 NSS は、最大サポート NSS より大きくすることはできません。

最大必須 NSS の変更後、無線に接続している、変更された NSS をサポートしないクライアントの接続が解除されます。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、最大必須 NSS を 7 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ac

[AC-wlan-ap-ap1-radio-1] dot11ac mandatory maximum-nss 7

AP グループ 1 の型番 **QX-W1020** の AP で、最大必須 NSS を 7 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] type dot11ac

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] dot11ac mandatory maximum-nss 7

関連コマンド

dot11ac support maximum-nss

2.1.28 dot11ax mandatory maximum-nss

Syntax

dot11ax mandatory maximum-nss *nss-number*

undo dot11ax mandatory maximum-nss

デフォルト

radio view でのデフォルト設定は以下の通りです。

- 最大サポート NSS が設定されている場合、最大必須 NSS は設定されていません。
- 最大サポート NSS が設定されていない場合、無線は AP group radio view の設定を使用します。

AP group radio view では、最大必須 NSS は設定されていません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

nss-number: 最大必須 NSS を指定します。範囲は 1～8 です。

説明

dot11ax mandatory maximum-nss コマンドは最大必須 NSS を設定します。

undo dot11ax mandatory maximum-nss コマンドはデフォルトに戻します。

本コマンドは、802.11ax、および 802.11gax 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g、または 802.11n に変更すると、コマンドが無効になります。

最大必須 NSS は、最大サポート NSS より大きくすることはできません。

最大必須 NSS の変更後、無線に接続している、変更された NSS をサポートしないクライアントの接続が解除されます。

radio view の設定は、AP group radio view の設定に優先します。

関連コマンド

dot11ax support maximum-nss

2.1.29 dot11ac multicast-nss

Syntax

dot11ac multicast-nss *nss-number* **vht-mcs** *index*

undo dot11ac multicast-nss

デフォルト

radio view でのデフォルト設定は以下の通りです。

- 最大サポート NSS か最大必須 NSS が設定されている場合、マルチキャスト NSS は設定されていません。
- 最大サポート NSS と最大必須 NSS のいずれも設定されていない場合、無線は AP group radio view の設定を使用します。

AP group radio view では、マルチキャスト NSS は設定されていません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

nss-number: マルチキャスト NSS を指定します。範囲は 1〜8 です。

index: VHT-MCS インデックスを指定します。範囲は 0〜9 です。

説明

dot11ac multicast-nss コマンドはマルチキャスト NSS と VHT-MCS インデックスを設定します。

undo dot11ac multicast-nss コマンドはデフォルトに戻します。

本コマンドは、802.11ac、および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g、または 802.11n に変更すると、コマンドが無効になります。

本コマンドを設定する前に、**dot11ac mandatory maximum-nss** コマンドを設定しなければいけません。

マルチキャスト NSS は、最大必須 NSS より大きくすることはできません。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、最大必須 MSS を 2 に、マルチキャスト NSS を 2 に、VHT-MCS インデックスを 2 にそれぞれ設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ac

[AC-wlan-ap-ap1-radio-1] dot11ac mandatory maximum-nss 2

[AC-wlan-ap-ap1-radio-1] dot11ac multicast-nss 2 vht-mcs 2

AP グループ 1 の型番 **QX-W1020** の AP で、最大必須 MSS を 2 に、マルチキャスト NSS を 2 に、VHT-MCS インデックスを 2 にそれぞれ設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] dot11ac mandatory maximum-nss 2

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] dot11ac multicast-nss 2 vht-mcs 2

関連コマンド

dot11ac mandatory maximum-nss

2.1.30 dot11ax multicast-nss

Syntax

dot11ax multicast-nss *nss-number* **he-mcs** *index*

undo dot11ax multicast-nss

デフォルト

radio view でのデフォルト設定は以下の通りです。

- 最大サポート NSS か最大必須 NSS が設定されている場合、マルチキャスト NSS は設定されていません。
- 最大サポート NSS と最大必須 NSS のいずれも設定されていない場合、無線は AP group radio view の設定を使用します。

AP group radio view では、マルチキャスト NSS は設定されていません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

nss-number: マルチキャスト NSS を指定します。範囲は 1～8 です。

index: he-mcs インデックスを指定します。範囲は 0～11 です。

説明

dot11ax multicast-nss コマンドはマルチキャスト NSS と he-mcs インデックスを設定します。

undo dot11ax multicast-nss コマンドはデフォルトに戻します。

本コマンドは、802.11ax、および 802.11gax 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g、または 802.11n に変更すると、コマンドが無効になります。

本コマンドを設定する前に、**dot11ax mandatory maximum-nss** コマンドを設定しなければいけません。

マルチキャスト NSS は、最大必須 NSS より大きくすることはできません。

radio view の設定は、AP group radio view の設定に優先します。

関連コマンド

dot11ax mandatory maximum-nss

2.1.31 dot11ac support maximum-nss

Syntax

dot11ac support maximum-nss *nss-number*

undo dot11ac support maximum-nss

デフォルト

radio view でのデフォルト設定は以下の通りです。

- 最大必須 NSS が設定されている場合、最大サポート NSS は 8 となります。
- 最大必須 NSS が設定されていない場合、無線は AP group radio view の設定を使用します。

AP group radio view では、最大サポート NSS は 8 となります。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

nss-number: 最大サポート NSS を指定します。範囲は 1～8 です。

説明

dot11ac support maximum-nss コマンドは最大サポート NSS を設定します。

undo dot11ac support maximum-nss コマンドはデフォルトに戻します。

本コマンドは、802.11ac、および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g、または 802.11n に変更すると、コマンドが無効になります。

最大サポート NSS は、最大必須 NSS より小さくすることはできません。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、最大サポート NSS を 7 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ac

[AC-wlan-ap-ap1-radio-1] dot11ac support maximum-nss 7

AP グループ 1 の型番 **QX-W1020** の AP で、最大サポート NSS を 7 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] type dot11ac

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] dot11ac support maximum-nss 7

関連コマンド

dot11ac mandatory maximum-nss

2.1.32 dot11ax support maximum-nss

Syntax

dot11ax support maximum-nss *nss-number*

undo dot11ax support maximum-nss

デフォルト

radio view でのデフォルト設定は以下の通りです。

- 最大必須 NSS が設定されている場合、最大サポート NSS は 8 となります。
- 最大必須 NSS が設定されていない場合、無線は AP group radio view の設定を使用します。

AP group radio view では、最大サポート NSS は 8 となります。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

nss-number: 最大サポート NSS を指定します。範囲は 1～8 です。

説明

dot11ax support maximum-nss コマンドは最大サポート NSS を設定します。

undo dot11ax support maximum-nss コマンドはデフォルトに戻します。

本コマンドは、802.11ax、および 802.11gax 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g、または 802.11n に変更すると、コマンドが無効になります。

最大サポート NSS は、最大必須 NSS より小さくすることはできません。

radio view の設定は、AP group radio view の設定に優先します。

関連コマンド

dot11ax mandatory maximum-nss

2.1.33 dot11be mandatory maximum-nss

🕮 **メモ：**

dot11be mandatory maximum-nss コマンドはソフトウェアバージョン7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

dot11be mandatory maximum-nss *nss-number*

undo dot11be mandatory maximum-nss

デフォルト

設定なし

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

Nss-number: 最大必須 NSS を指定します。範囲は 1～8 です。

説明

dot11be mandatory maximum-nss コマンドは最大必須 NSS を設定します。

undo dot11n mandatory maximum-nss コマンドはデフォルトに戻します。

このコマンドで 802.11be に対して指定される最大必須 NSS は、802.11be の dot11be support max-nss コマンドで設定された最大必須 NSS を超えることはできません。

このコマンドは Radio type が 802.11be、802.11gbe、および 802.11abe の無線でのみ使用することができます。Radio type が 802.11be、802.11gbe、802.11abe 以外のモードに切り替わると、このコマンドは無効になります。

例

最大必須 NSS を 8 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1240

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11be

[AC-wlan-ap-ap1-radio-1] dot11be mandatory maximum-nss 8

2.1.34 dot11be multicast-nss

🕮 **メモ**:

dot11be multicast-nss コマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

dot11be multicast-nss *nss-number* **eth-mcs** *index*

undo dot11be multicast-nss

デフォルト

設定なし

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

nss-number: マルチキャスト NSS を指定します。範囲は 1〜8 です。

index: ETH-MCS NSS のインデックスを指定します。範囲は 0〜13 です。

説明

dot11be multicast-nss コマンドはマルチキャスト NSS と ETH-MCS インデックスを設定します。

undo dot11ax multicast-nss コマンドはデフォルトに戻します。

このコマンドを設定する前に、**dot11be mandatory maximum-nss** コマンドを設定してください。

このコマンドで設定する 802.11be マルチキャストの NSS の値は、**dot11be mandatory maximum-nss** コマンドで設定されている必須 NSS の最大値を超えることはできません。

このコマンドは Radio type が 802.11be、802.11gbe、および 802.11abe の無線でのみ使用することができます。Radio type が 802.11be、802.11gbe、802.11abe 以外のモードに切り替わると、このコマンドは無効になります。

例

必須最大 NSS 値を 2、マルチキャスト NSS を 2、マルチキャスト ETH-MCS インデックスを 2 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1240

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11be

[AC-wlan-ap-ap1-radio-1] dot11be mandatory maximum-nss 2

[AC-wlan-ap-ap1-radio-1] dot11be multicast-nss 2 eth-mcs 2

関連コマンド

dot11be mandatory maximum-nss

2.1.35 dot11be support maximum-nss

🕮 **メモ**:

dot11be support maximum-nss コマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

dot11be support maximum-nss *nss-number*

undo dot11be support maximum-nss

デフォルト

8

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

nss-number: 最大サポート NSS を指定します。範囲は 1～8 です。

説明

dot11be support maximum-nss コマンドは最大サポート NSS を設定します。

undo dot11be support maximum-nss コマンドはデフォルトに戻します。

このコマンドは Radio type が 802.11be、802.11gbe、および 802.11abe の無線でのみ使用することができます。Radio type が 802.11be、802.11gbe、802.11abe 以外のモードに切り替わると、このコマンドは無効になります。

例

#最大サポート NSS 値を 8 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1240

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11be

[AC-wlan-ap-ap1-radio-1] dot11be support maximum-nss 8

関連コマンド

type dot11be

type dot11abe

type dot11gbe

2.1.36 dot11g protection

Syntax

dot11g protection { **disable** | **enable** }

undo dot11g protection

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、802.11g 保護は無効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 802.11g 保護を無効にします。

enable: 802.11g 保護を有効にします。

説明

dot11g protection enable コマンドは 802.11g 保護を有効にします。

dot11g protection disable コマンドは 802.11g 保護を無効にします。

undo dot11g protection コマンドはデフォルトに戻します。

本コマンドは、802.11g、802.11n(2.4GHz)および 802.11gac 無線にのみ適用されます。無線モードを 802.11g、802.11n(2.4GHz)または 802.11gac 以外に変更した場合、802.11g 保護設定は削除されます。

802.11g、802.11n、802.11gac 装置は、チャネル上で 802.11b 信号を検出したときに限り、データを送信する前に RTS/CTS パケットもしくは CTS-to-self パケットを送信します。

802.11g 保護は、802.11b クライアントが 802.11g、802.11n(2.4GHz)または 802.11gac の AP に接続されたときに自動的に有効になります。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、802.11g 保護を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] type dot11gn

[AC-wlan-ap-ap1-radio-2] dot11g protection enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、802.11g 保護を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 2

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-2] type dot11gn

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-2] dot11g protection enable

関連コマンド

protection-mode

2.1.37 dot11n mandatory maximum-mcs

Syntax

dot11n mandatory maximum-mcs *index*

undo dot11n mandatory maximum-mcs

デフォルト

radio view でのデフォルト設定は以下の通りです。

- 最大サポート MCS インデックスが設定されている場合、最大必須 MCS は設定されていません。
- 最大サポート MCS インデックスが設定されていない場合、無線は AP group radio view の設定を使用します。

AP group radio view では、最大必須 MCS インデックスは設定されていません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

index: 最大必須 MCS インデックスを指定します。範囲は 0～76 です。

説明

dot11n mandatory maximum-mcs コマンドは最大必須 MCS インデックスを設定します。

undo dot11n mandatory maximum-mcs コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。

最大必須 MCS インデックスは、**dot11n multicast-mcs** コマンドを設定する前に設定しなければいけません。

最大必須 MCS インデックスの変更後、無線に接続している、変更された MCS インデックスをサポートしないクライアントの接続が解除されます。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、最大必須 MCS インデックスを 14 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] dot11n mandatory maximum-mcs 14

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、最大必須 MCS インデックスを 14 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] dot11n mandatory maximum-mcs 14

2.1.38 dot11n multicast-mcs

Syntax

dot11n multicast-mcs *index*

undo dot11n multicast-mcs

デフォルト

radio view でのデフォルト設定は以下の通りです。

- 最大必須 MCS インデックスか最大サポート MCS インデックスが設定されている場合、マルチキャスト MCS インデックスは設定されていません。
- 最大必須 MCS インデックスと最大サポート MCS インデックスのいずれも設定されていない場合、無線は AP group radio view の設定を使用します。

AP group radio view では、マルチキャスト MCS インデックスは設定されていません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

index: マルチキャスト MCS インデックスを指定します。範囲は 0～76 です。

説明

dot11n multicast-mcs コマンドはマルチキャスト MCS インデックスを設定します。

undo dot11n multicast-mcs コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax 無線にのみ適用可能です。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。

マルチキャスト MCS インデックスは、802.11n、802.11ac、802.11ax クライアントが存在する場合にのみ有効です。

802.11a / b / g クライアントが存在する場合、AP とクライアントは 802.11a / b / g マルチキャストレートを使用してマルチキャストパケットを送信します。

マルチキャスト MCS インデックスは、帯域モードが 20MHz か 40MHz かによらず、20MHz 帯域モードのレートにマッピングされます。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、マルチキャスト MCS インデックスを 14 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] dot11n mandatory maximum-mcs 14

[AC-wlan-ap-ap1-radio-1] dot11n multicast-mcs 14

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、マルチキャスト MCS インデックスを 14 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] dot11n mandatory maximum-mcs 14

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] dot11n multicast-mcs 14

2.1.39 dot11n protection

Syntax

dot11n protection { **disable** | **enable** }

undo dot11n protection

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、802.11n 保護は無効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 802.11n 保護を無効にします。

enable: 802.11n 保護を有効にします。

説明

dot11n protection enable コマンドは 802.11n 保護を有効にします。

dot11n protection disable コマンドは 802.11n 保護を無効にします。

undo dot11n protection コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax および 802.11gac 無線にのみ適用可能です。無線のモードを 802.11n、802.11ac、802.11ax および 802.11gac 以外のモードに変更すると、802.11n 保護設定が削除されます。

802.11n 装置は、チャネル上で 802.11a/b/g 信号を検出したときに限り、データを送信する前に RTS/CTS パケットもしくは CTS-to-self パケットを送信します。

802.11n 保護は、802.11a/b/g クライアントが 802.11n、802.11ac、802.11ax または 802.11gac の AP に接続されたときに自動的に有効になります。

radio view の設定は、AP group radio view の設定に優先します。

🕮 **メモ**:

802.11n 装置とは、802.11n および 802.11ac/ax 装置のことを指します。

例

AP **ap1** で、802.11n 保護を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] dot11n protection enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、802.11n 保護を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] dot11n protection enable

関連コマンド

protection-mode

2.1.40 dot11n support maximum-mcs

Syntax

dot11n support maximum-mcs *index*

undo dot11n support maximum-mcs

デフォルト

radio view でのデフォルト設定は以下の通りです。

- 最大必須 MCS インデックスが設定されている場合、最大必須 MCS は 76 となります。
- 最大必須 MCS インデックスが設定されていない場合、無線は AP group radio view の設定を使用します。

AP group radio view では、最大サポート MCS インデックスは 76 となります。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

index: 最大サポート MCS インデックスを指定します。範囲は 0～76 です。

説明

dot11n support maximum-mcs コマンドは最大サポート MCS インデックスを設定します。

undo dot11n support maximum-mcs コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。

最大サポート MCS インデックスは、最大必須 MCS インデックスより小さくなることはできません。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、最大サポート MCS インデックスを 14 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] dot11n support maximum-mcs 14

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、最大サポート MCS インデックスを 14 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] dot11n support maximum-mcs 14

2.1.41 dtim

Syntax

dtim *counter*

undo dtim

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、DTIM 間隔は 1 となっています。AP はバッファリングされたブロードキャストおよびマルチキャストフレームを毎回ビーコンフレームごとに送信します。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

counter: DTIM 間隔を指定します。範囲は 1～31 です。

説明

dtim コマンドは DTIM（Delivery Traffic Indication Map）間隔を設定します。

undo dtim コマンドはデフォルトに戻します。

AP は、DTIM（Delivery Traffic Indication Map）に従ったビーコンを周期的にブロードキャストします。ビーコンをブロードキャストした後、AP は DTIM 間隔の値に基づいてバッファリングされたブロードキャストおよびマルチキャストフレームを送信します。例えば、DTIM 間隔を 5 に設定した場合、AP はバッファリングされたブロードキャストおよびマルチキャストフレームを 5 ビーコンフレームごとに送信します。

クライアント数が最大に達すると、AP は新しいクライアントの許可を停止します。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、DTIM 間隔を 5 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] dtim 5

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、DTIM 間隔を 5 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] dtim 5

2.1.42 fragment-threshold

Syntax

fragment-threshold *size*

undo fragment-threshold

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、フラグメンテーションしきい値は 2346 バイトです。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

size: フラグメンテーションしきい値を指定します。範囲は 256～2346 バイトです。この引数の値は偶数でなければいけません。

説明

fragment-threshold コマンドはフレームのフラグメンテーションしきい値を設定します。

undo fragment-threshold コマンドはデフォルトに戻します。

フラグメンテーションしきい値より大きいフレームは、伝送の前にフラグメントされます。フラグメンテーションしきい値より小さいフレームは、フラグメントされずに伝送されます。

干渉が大きい WLAN では、ネットワーク処理能力と効率を向上させるために、フラグメンテーションしきい値を低く設定してください。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、フラグメンテーションしきい値を 2048 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] fragment-threshold 2048

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、フラグメンテーションしきい値を 2048 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] fragment-threshold 2048

2.1.43 green-energy-management

Syntax

green-energy-management { **disable** | **enable** }

undo green-energy-management

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、エネルギ節約機能は無効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: エネルギ節約機能を無効にします。

enable: エネルギ節約機能を有効にします。

説明

green-energy-management enable コマンドはエネルギ節約機能を有効にします。

green-energy-management disable コマンドはエネルギ節約機能を無効にします。

undo green-energy-management コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、エネルギ節約機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] green-energy-management enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、エネルギ節約機能を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] green-energy-management enable

2.1.44 ldpc

Syntax

ldpc { **disable** | **enable** }

undo ldpc

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、LDPC は無効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

説明

ldpc enable コマンドは LDPC を有効にします。

ldpc disable コマンドは LDPC を無効にします。

undo ldpc コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。

装置は LDPC パケットを受信できますが、送信することはできません。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、LDPC を無効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] ldpc disable

AP グループ 1 の型番 **QX-W1020** の AP で、LDPC を無効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] ldpc disable

2.1.45 long-retry threshold

Syntax

long-retry threshold *count*

undo long-retry threshold

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、大きいフレームの最大再送信回数は 4 回です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

count: 大きいフレームのハードウェア最大再送信回数を指定します。範囲は 1～15 です。

説明

long-retry threshold コマンドは大きいフレームのハードウェア最大再送信回数を設定します。

undo long-retry threshold コマンドはデフォルトに戻します。

このタスクを実行して、RTS しきい値を超えるフレームのハードウェア再送信の最大数を設定します。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、大きいフレームのハードウェア最大再送信回数を 5 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] long-retry threshold 5

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、大きいフレームのハードウェア最大再送信回数を 5 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] long-retry threshold 5

関連コマンド

- **protection-threshold**
- **short-retry threshold**

2.1.46 max-power

Syntax

max-power *radio-power*

undo max-power

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、AP はサポートされる最大伝送電力を使用します。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

radio-power: 最大伝送電力を指定します。

QX-W1000 シリーズの範囲は

QX-W1010 の場合、radio 1 が 1～20dBm、radio 2 が 1～16dBm、

QX-W1020 の場合、radio 1 が 1～12dBm、radio 2 が 1～20dBm、radio 3 が 1～14dBm、

QX-W1030 の場合、radio 1 が 1～11dBm、radio 2 が 1～19dBm、radio 3 が 1～14dBm

です。

QX-W1100 シリーズの範囲は

ソフトウェアバージョン 7.2.63 を含む以前のソフトウェアでは、

QX-W1110 の場合、radio1 が 1～18dBm、radio2 が 1～16dBm、

QX-W1120 の場合、radio 1 が 1～11dBm、radio 2 が 1～19dBm、radio 3 が 1～14dBm、

QX-W1130 の場合、radio 1 が 1～13dBm、radio 2 が 1～20dBm、radio 3 が 1～14dBm

ソフトウェアバージョン 7.2.67 を含む以降のソフトウェアでは、

QX-W1110 の場合、radio1 が 1～18dBm、radio2 が 1～17dBm、

QX-W1120 の場合、radio 1 が 1～12dBm、radio 2 が 1～19dBm、radio 3 が 1～14dBm、

QX-W1130 の場合、radio 1 が 1～13dBm、radio 2 が 1～20dBm、radio 3 が 1～15dBm

です。

QX-W1240：

Radio 1 の場合は、バンド幅の設定によって設定可能な範囲が変化します。

バンド幅が 20M/40M/80M の場合は、1～13dBm の範囲で設定することができます。

バンド幅が 160M の場合は、1～12dBm の範囲で設定することができます。

Radio 2 (W52/W53 帯)の場合は、1～14dBm の範囲で設定することができます。

Radio 2 (W56 帯)の場合は、1～21dBm の範囲で設定することができます。

Radio 3(2.4G) の場合は、タイプの設定によって設定可能な範囲が変化します。

無線タイプが 802.11b 以外の場合は、1～17dBm の範囲で設定することができます。

無線タイプが 802.11b の場合は、1～12dBm の範囲で設定することができます。

QX-W1230：

Radio 1(6GHz)の場合は、バンド幅の設定によって設定可能な範囲が変化します。

バンド幅が 20M/40M/80M の場合は、1～13dBm の範囲で設定することができます。

バンド幅が 160M/320M の場合は、1～12dBm の範囲で設定することができます。

Radio 1(5GHz) (W52/W53 帯)の場合は、1～13dBm の範囲で設定することができます。

Radio 2(5GHz) (W56 帯)の場合は、1～20dBm の範囲で設定することができます。

Radio 3(2.4G) の場合は、タイプの設定によって設定可能な範囲が変化します。

無線タイプが 802.11b 以外の場合は、1～16dBm の範囲で設定することができます。

無線タイプが 802.11b の場合は、1～12dBm の範囲で設定することができます。

QX-W1210：

Radio 1(6GHz)の場合は、バンド幅の設定によって設定可能な範囲が変化します。

バンド幅が 20M/40M/80M の場合は、1～13dBm の範囲で設定することができます。

バンド幅が 160M/320M の場合は、1～12 dBm の範囲で設定することができます。

Radio 1(5GHz) (W52/W53 帯)の場合は、1～14dBm の範囲で設定することができます。

Radio 1(5GHz) (W56 帯)の場合は、タイプの設定によって設定可能な範囲が変化します。

無線タイプが 802.11 abe/ax/ac であり、バンド幅が 20M/40M/80M の場合は、1～21dBm の範囲で設定することができます。

無線タイプが 802.11abe/ax/ac であり、バンド幅が 160M の場合は、1～14dBm の範囲で設定することができます。

無線タイプが 802.11abe/ax/ac 以外の場合は、1～21dBm の範囲で設定することができます。

Radio 2(5GHz) (W52/W53 帯)の場合は、1～13 dBm の範囲で設定することができます。

Radio 2(5GHz) (W56 帯)の場合は、1～20dBm の範囲で設定することができます。

Radio 2(2.4GHz)の場合は、タイプの設定によって設定可能な範囲が変化します。

無線タイプが 802.11b 以外の場合は、1～15dBm の範囲で設定することができます。

無線タイプが 802.11b の場合は、1～10dBm の範囲で設定することができます。

説明

max-power コマンドは最大伝送電力を設定します。

undo max-power コマンドはデフォルトに戻します。

無線でサポートされる伝送電力の範囲は、カントリーコード、チャネル、AP モデル、無線モード、アンテナタイプ、帯域幅モードにより変化します。最大伝送電力を設定後に無線に対するこれらの特性を変更した場合、設定された最大伝送電力がサポートされた伝送電力の範囲外になる可能性があります。この場合、システムは自動的に最大伝送電力を有効な値に適応させます。

電力ロックを有効にした場合、ロックされた電力が最大伝送電力になります。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、最大伝送電力を 11dBm に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] max-power 11

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、最大伝送電力を 11dBm に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] max-power 11

2.1.47 mru

🕮 **メモ：**

- **mru** コマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。
- AP group Radio view での設定は、ソフトウェアバージョン 7.2.89 を含む以降のソフトウェアからサポートしています。

Syntax

mru { **disable** | **enable** }

undo mru

デフォルト

ソフトウェアバージョンにより異なります。

ソフトウェアバージョン 7.2.85a を含む以前のソフトウェア：

radio view：無効

ソフトウェアバージョン 7.2.89 を含む以降のソフトウェア：

radio view：AP group radio view の設定を使用します。

AP group radio view：無効

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: Multiple Resource Unit (MRU)を無効にします。

enable: Multiple Resource Unit (MRU)を有効にします。

説明

mru enable コマンドは Multiple Resource Unit (MRU)を有効にします。

mru disable コマンドは Multiple Resource Unit (MRU)を無効にします。

undo mru コマンドはデフォルトに戻します。

Multiple Resource Unit (MRU) は、マルチユーザシナリオにおいて、スペクトルリソースの使用率を向上させるために使用される手法です。

従来は、各ユーザが使用できるリソースユニット (RU) は 1 つのみでした。

MRU の機能により、ユーザは複数の RU を使用できます。同じ帯域幅で、1 つの STA が同時に複数の RU リソースを占有できるため､スペクトルリソースの使用率が向上し、通信遅延が削減されます。

このコマンドは Radio type が 802.11be、802.11abe、802.11gbe の無線でのみ使用することができます。Radio type が 802.11be、802.11abe、802.11gbe 以外のモードに切り替わると、このコマンドは無効になります。

例

AP **ap1** で、MRU を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1240

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11be

[AC-wlan-ap-ap1-radio-1] mru enable

AP グループ **apgroup1** の型番 **QX-W1240** の AP で、MRU を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1240

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1240] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1240-radio-1] mru enable

2.1.48 mu-txbf

Syntax

mu-txbf { **disable** | **enable** }

undo mu-txbf

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、ソフトウェアバージョンによりデフォルト状態が異なります。

ソフトウェアバージョン 7.2.21 を含む以前のソフトウェアでは有効です。

ソフトウェアバージョン 7.2.27, 7.2.27a から 7.2.59 のソフトウェアでは無効です。

ソフトウェアバージョン 7.2.63 のソフトウェアでは有効(コンフィグ上は非表示)です。

ソフトウェアバージョン7.2.67 を含む以降のソフトウェアでは無効(コンフィグ上は非表示)です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: マルチユーザ送信ビームフォーミング（TxBF）を無効にします。

enable: マルチユーザ送信ビームフォーミング（TxBF）を有効にします。

説明

mu-txbf enable コマンドはマルチユーザ送信ビームフォーミング（TxBF）を有効にします。

mu-txbf disable コマンドはマルチユーザ送信ビームフォーミング（TxBF）を無効にします。

undo mu-txbf コマンドはデフォルトに戻します。

このコマンドは、802.11ac、802.11gac、802.11ax、802.11gax 無線にのみ適用されます。無線モードを 802.11a、802.11b、802.11g、802.11n に変更すると、コマンドが無効になります。

TxBF を使用すると、AP はチャネル情報に基づいて送信パラメータを調整し、意図したクライアントに RF 信号を集中させることができます。この機能により、RF 信号の品質が向上します。

マルチユーザ TxBF は 802.11ac Wave2 の一部です。マルチユーザ TxBF を使用すると、異なる RF 信号を意図したクライアントに集中させ、干渉や伝送遅延を減らすことができます。これにより、トラフィックスループットと帯域幅使用率が改善されます。マルチユーザ TxBF は、多数のクライアントを持ち、高い帯域幅使用率と低い伝送遅延を必要とする WLAN に適用できます。

マルチユーザ TxBF は、シングルユーザ TxBF が有効な場合にのみ有効です。

マルチユーザ TxBF で有効になっている AP のデフォルトの MIMO 設定を変更しないことを推奨します。

radio view の設定は、AP group radio view の設定よりも優先されます。

例

AP **ap1** のマルチユーザ TxBF を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] su-txbf enable

[AC-wlan-ap-ap1-radio-1] mu-txbf enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、マルチユーザ TxBF を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] su-txbf enable

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] mu-txbf enable

関連コマンド

- **mimo**
- **su-txbf**

2.1.49 power-lock

Syntax

power-lock { **disable** | **enable** }

undo power-lock

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、電力ロック機能は無効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 電力ロック機能を無効にします。

enable: 電力ロック機能を有効にします。

説明

power-lock enable コマンドは電力ロック機能を有効にします。

power-lock disable コマンドは電力ロック機能を無効にします。

undo power-lock コマンドはデフォルトに戻します。

このコマンドは TPC(RRM)機能と同時に使用します。TPC(RRM)機能は電力値を自動的に変更します。変更中の電力値をそのまま継続して使用したい場合に"power-lock enable"にします。通常はこのコマンドを使用する必用はありません。

電力値の変更が多い場合、一部の装置の電力値を固定して状況が変化するか確認することができます。

電力ロックを有効にした場合、現在の電力がロックされて最大伝送電力となります。ロックされた電力は、AC 再起動後も有効になります。

電力ロックが有効にされた無線が、ロックされた電力より低い電力を供給する新たなチャネルに切り替わった場合、新しいチャネルによってサポートされた最大電力が有効になります。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、電力ロック機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] power-lock enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、電力ロック機能を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] power-lock enable

2.1.50 preamble

Syntax

preamble { **long** | **short** }

undo preamble

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、short が使用されます。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

long: 長いプリアンブルを指定します。 長いプリアンブルは、従来モデルのすべての無線装置との互換性が確保されます。

short: 短いプリアンブルを指定します。短いプリアンブルはネットワーク性能を改善します。

説明

preamble コマンドはプリアンブルタイプを設定します。

undo preamble コマンドはデフォルトに戻します。

本コマンドは、802.11b、802.11g、802.11gn 無線でのみ適用可能です。

プリアンブルとは、送信側と受信側の間で伝送信号を同期させるためのパケットヘッダ内のビットのセットです。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、プリアンブルタイプを **long** に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] preamble long

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、プリアンブルタイプを **long** に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 2

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-2] preamble long

2.1.51 pre-puncture static

🕮 **メモ：**

- **pre-puncture static** コマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。
- AP group Radio view での設定は、ソフトウェアバージョン 7.2.89 を含む以降のソフトウェアからサポートしています。

Syntax

pre-puncture static { **disable** | **enable** }

undo pre-puncture static

デフォルト

ソフトウェアバージョンにより異なります。

ソフトウェアバージョン 7.2.85a を含む以前のソフトウェア：

radio view：無効

ソフトウェアバージョン 7.2.89 を含む以降のソフトウェア：

radio view：AP group radio view の設定を使用します。

AP group radio view：無効

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: Preamble puncturing を無効にします。

enable: Preamble puncturing を有効にします。

説明

pre-puncture static enable コマンドは Preamble puncturing を有効にします。

pre-puncture static disable コマンドは Preamble puncturing を無効にします。

undo pre-puncture static コマンドはデフォルトに戻します。

本コマンドを使用すると、非連続チャネルを使用したデータ通信が可能になることによって、チャネル干渉を防ぎ、チャネルの使用効率が向上します。

このコマンドは、80MHz 帯、160MHz 帯でのみ適用できます。

このコマンドは、802.11be、802.11gbe、および 802.11abe でのみ有効にすることができます。Radio type が他のモードに切り替わると、このコマンドは無効になります。

例

AP **ap1** で、Preamble puncturing を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1240

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] type dot11be

[AC-wlan-ap-ap1-radio-2] pre-puncture static enable

AP グループ **apgroup1** の型番 **QX-W1240** の AP で、Preamble puncturing を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1240

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1240] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1240-radio-1] pre-puncture static enable

2.1.52 protection-mode

Syntax

protection-mode { **cts-to-self** | **rts-cts** }

undo protection-mode

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、CTS-to-self モードが使用されます。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

cts-to-self: CTS-to-self モードを指定します。

rts-cts: RTS/CTS モードを指定します。

説明

protection-mode コマンドは衝突回避モードを設定します。

undo protection-mode コマンドはデフォルトに戻します。

AP に対して以下の衝突回避モードのいずれかを指定することができます。

- **RTS/CTS**－AP は、クライアントにデータを送信する前に、RTS パケットを送信します。RTS パケットを受信した後、クライアントは CTS パケットを AP に送信します。CTS パケット受信後、AP はデータの送信を開始します。また、その RTS パケットもしくは CTS パケットを検出した別の装置が、指定された時間内にデータを送信することはありません。
- **CTS-to-self**－AP は、クライアントにデータを送信する前に、CTS パケットを送信します。この CTS パケットには、AP 自体の MAC アドレスが宛て先 MAC アドレスとして付随されています。CTS-to-self パケット受信後、AP はデータの送信を開始します。また、その CTS-to-self パケットを受信した別の装置が、指定された時間内にデータを送信することはありません。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、RTS/CTS モードを設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] protection-mode rts-cts

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、RTS/CTS モードを設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 2

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-2] protection-mode rts-cts

関連コマンド

- **dot11g protection**
- **dot11n protection**
- **protection-threshold**

2.1.53 protection-threshold

Syntax

protection-threshold *size*

undo protection-threshold

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、RTS しきい値は 2346 バイトです。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

size: RTS しきい値を指定します。範囲は 0～2346 バイトです。

説明

protection-threshold コマンドは RTS しきい値を設定します。

undo protection- threshold コマンドはデフォルトに戻します。

システムは、パケットが RTS しきい値より大きい場合に限り衝突回避を実行します。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、RTS しきい値を 2048 バイトに設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] protection-threshold 2048

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、RTS しきい値を 2048 バイトに設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] protection-threshold 2048

関連コマンド

protection-mode

2.1.54 radar-channel-switchback disable

🕮 **メモ：**

このコマンドは、ソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

radar-channel-switchback disable

undo radar-channel-switchback

デフォルト

有効

View

Global configuration view

定義済みユーザロール

network-admin

説明

radar-channel-switchback disable コマンドは、レーダチャネルスイッチバックを無効にします。

undo radar-channel-switchback コマンドは、デフォルトに戻します。

無線の作動チャネル上でレーダ信号が検出されると、チャネルが手動で指定されているか自動的に割り当てられているかにかかわらず、無線は使用中のチャネルを変更します。

レーダチャネルスイッチバックを無効にすると、レーダ信号の検出によるチャネル変更をしてから 30 分経過しても、AP が元のチャネルに切り替えないようにすることができます。この場合、AP は新しいチャネルを使用し続けます。

例

レーダチャネルスイッチバックを無効にします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] radar-channel-switchback disable

2.1.55 radio

Syntax

radio *radio-id*

View

AP view

AP group AP model view

定義済みユーザロール

network-admin

パラメータ

radio-id: 無線を ID で指定します。範囲は装置モデルにより異なります。

説明

radio コマンドは radio view に入ります。

例

radio view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1]

AP グループ radio view に移行します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-apgroup1] ap-model QX-W1020

[AC-wlan-ap-apgroup1-ap-model-QX-W1020] radio 1

2.1.56 radio { disable | enable }

Syntax

radio { **disable** | **enable** }

undo radio

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、無線は無効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 無線を無効にします。

enable: 無線を有効にします。

説明

radio enable コマンドは無線を有効にします。

radio disable コマンドは無線を無効にします。

undo radio コマンドはデフォルトに戻します。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、無線を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] radio enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、無線を有効にします。

Enable radio 1 for APs with model QX-W1020 in AP group apgroup1.

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] radio enable

2.1.57 radio-type 2.4g

🕮 **メモ：**

radio-type 2.4g コマンドはソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

radio-type 2.4g { dot11g | dot11gac | dot11gax | dot11gn }

undo radio-type 2.4g

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

dot11g: 802.11g モードを指定します。

dot11gac: 802.11gac モードを指定します。

dot11gax: 802.11gax モードを指定します。

dot11gn: 802.11n (2.4 GHz) モードを指定します。

説明

radio-type 2.4g コマンドは 2.4 GHz 帯の無線モードを指定します。

undo radio-type 2.4g コマンドはデフォルトに戻します。

デフォルトでは、無線に設定した無線モードが、この無線によって提供されるすべての BSS に適用されます。

無線が異なる無線モードを使用して BSS を提供するには、このコマンドを実行してサービステンプレート毎に異なる無線モードを指定し、サービステンプレートを無線にバインドします。

2.4 GHz 無線モードのレベルは、802.11gax、802.11gac、802.11gn、802.11g の順に低くなります。Service template view と Radio view の両方で無線モードを設定すると、下位レベルの無線モードが有効になります。無線表示で指定した無線モードのレベルが、

バインドされたサービステンプレートのいずれかで指定した無線モードよりも高いことを確認してください。

このコマンドを実行する前に、サービステンプレートが無効になっていることを確認してください。

例

2.4 GHz 帯の無線モードを 802.11 n に設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] radio-type 2.4g dot11gn

関連コマンド

display wlan service-template

2.1.58 radio-type 5g

🕮 **メモ**:

radio-type 5g コマンドはソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

radio-type 5g { **dot11a** | **dot11ac** | **dot11an** | **dot11ax** }

undo radio-type 5g

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

dot11a: 802.11a モードを指定します。

dot11ac: 802.11ac モードを指定します。

dot11an: 802.11n (5 GHz)モードを指定します。

dot11ax: 802.11ax モードを指定します。

説明

radio-type 5g コマンドは 5 GHz 帯の無線モードを指定します。

undo radio-type 5g コマンドはデフォルトに戻します。

デフォルトでは、無線に設定した無線モードが、この無線によって提供されるすべての BSS に適用されます。

無線が異なる無線モードを使用して BSS を提供するには、このコマンドを実行してサービステンプレート毎に異なる無線モードを指定し、サービステンプレートを無線にバインドします。

5 GHz 無線モードのレベルは、802.11ax、802.11ac、802.11an、802.11a の順に低くなります。Service template view と Radio view の両方で無線モードを設定すると、下位レベルの無線モードが有効になります。Radio view で指定した無線モードのレベルが、バインドされたサービステンプレートのいずれかで指定した無線モードよりも高いことを確認してください。

このコマンドを実行する前に、サービステンプレートが無効になっていることを確認してください。

例

5 GHz 帯の無線モードを 802.11 n に設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] radio-type 5g dot11an

関連コマンド

display wlan service-template

2.1.59 rate

Syntax

rate { **multicast** { **auto** | *rate-value* } | { **disabled** | **mandatory** | **supported** } *rate-value* }

undo rate

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では以下となります。

- 802.11a/802.11an/802.11ac/802.11ax
  - **禁止速度**－なし
  - **必須速度**－6、12、24
  - **マルチキャスト速度**－必須速度から選択されます。

- □ **サポート速度**－9、18、36、48、54
- 802.11b
  - □ **禁止速度**－なし
  - □ **必須速度**－1、2
  - □ **マルチキャスト速度**－最大の必須速度
  - □ **サポート速度**－5.5、11
- 802.11g/802.11gn/802.11gac
  - □ **禁止速度**－なし
  - □ **必須速度**－1、2、5.5、11
  - □ **マルチキャスト速度**－必須速度から選択
  - □ **サポート速度**－6、9、12、18、24、36、48、54

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disabled: AP で使用できない速度を指定します。

mandatory: AP と接続するためにクライアントがサポートしなければならない速度を指定します。

multicast: AP がパケットをマルチキャストする速度を指定します。マルチキャスト速度は、必須速度の中から選択されなければなりません。

supported: AP がサポートする速度を指定します。クライアントが AP と接続した後に、クライアントは AP と通信するために、サポートされた速度の中から、より高い速度や低い速度を選択することが可能です。

auto: マルチキャスト速度として、必須速度を自動的に選択します。

rate-value: 速度を Mbps で指定します。スペース区切りで複数の速度を設定することができます。利用可能な引数は以下の通りです。

- **802.11a/802.11an/802.11ac/802.11ax**－6、9、12、18、24、36、48、54
- **802.11b**－1、2、5.5、11
- **802.11g/802.11gn802.11gac**－1、2、5.5、6、9、11、12、18、24、36、48、54

説明

rate コマンドは無線の伝送速度を設定します。

undo rate コマンドはデフォルトに戻します。

必須速度とマルチキャスト速度を未設定にすることはできません。必須速度が 1 種類しかない場合は、サポート速度または禁止速度として必須速度を指定することはできません。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、必須速度として 6Mbps、12Mbps、24Mbps を設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rate mandatory 6 12 24

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、必須速度として 6Mbps、12Mbps、24Mbps を設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] rate mandatory 6 12 24

2.1.60 reset wlan statistics ap radio

🕮 **メモ：**

- **reset wlan statistics ap radio** コマンドはソフトウェアバージョン 7.2.55 を含む以降のソフトウェアからサポートしています。

Syntax

reset wlan statistics ap { **all** | **name** *ap-name* } **radio**

View

User view

定義済みユーザロール

network-admin

パラメータ

ap: AP を指定します。

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

reset wlan statistics ap radio コマンドは無線統計情報を削除します。

例

#AP **ap1** の無線統計情報を削除します

<AC> reset wlan statistics ap name ap1 radio

2.1.61 short-gi

Syntax

short-gi { **disable** | **enable** }

undo short-gi

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、ショート GI は有効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: ショート GI (Guard Interval)を無効にします。

enable: ショート GI (Guard Interval)を有効にします。

説明

short-gi enable コマンドはショート GI (Guard Interval)を有効にするには、を使用します。

short-gi disable コマンドはショート GI (Guard Interval)を無効にします。

undo short-gi コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、ショート GI を無効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] short-gi disable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、ショート GI を無効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] short-gi disable

2.1.62 short-retry threshold

Syntax

short-retry threshold *count*

undo short-retry threshold

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、小さいフレームのハードウェア最大再送信回数は 7 回です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

count: 小さいフレームのハードウェア最大再送信回数を指定します。範囲は 1～15 です。

説明

short-retry threshold コマンドは小さいフレームのハードウェア最大再送信回数を設定します。

undo short-retry threshold コマンドはデフォルトに戻します。

このタスクを実行して、RTS しきい値未満のフレームのハードウェア再送信の最大数を設定します。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、小さいフレームのハードウェア最大再送信回数を 10 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] short-retry threshold 10

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、小さいフレームのハードウェア最大再送信回数を 10 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] short-retry threshold 10

関連コマンド

- **long-retry threshold**
- **protection-threshold**

2.1.63 smart-antenna

Syntax

smart-antenna { **disable** | **enable** }

undo smart-antenna

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、スマートアンテナ機能は有効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: スマートアンテナ機能を無効にします。

enable: スマートアンテナ機能を有効にします。

説明

smart-antenna enable コマンドはスマートアンテナ機能を有効にします。

smart-antenna disable コマンドはスマートアンテナ機能を無効にします。

undo smart-antenna コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、スマートアンテナ機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] smart-antenna enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、スマートアンテナ機能を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] smart-antenna enable

2.1.64 smart-antenna policy

Syntax

smart-antenna policy { **auto** | **high-availability** | **high-throughput** }

undo smart-antenna policy

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、auto モードが使用されます。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

auto: 自動モードを指定します。本モードが有効の場合、音声パケットと映像パケットに対しては高可用性モードを使用し、その他のパケットに対しては高処理能力モードを使用します。

high-availability: 高可用性モードを指定します。このモードはクライアントに対して帯域幅を保証し、安定した帯域幅を要求する WLAN に適用可能です。

high-throughput: 高処理能力モードを指定します。このモードは、可能な限りの接続を保証します。ハイパフォーマンスを要求する WLAN に適用可能です。

説明

smart-antenna policy コマンドはスマートアンテナモードを設定します。

undo smart-antenna policy コマンドはデフォルトに戻します。

スマートアンテナモードは、スマートアンテナ機能を有効にした後のみ有効になります。

本コマンドは、802.11n、802.11ac、802.11ax および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、スマートアンテナモードを高可用性モードに指定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] smart-antenna policy high-availability

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、スマートアンテナモードを高可用性モードに指定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] smart-antenna policy high-availability

2.1.65 stbc

Syntax

stbc { **disable** | **enable** }

undo stbc

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、STBC は有効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: STBC を無効にします。

enable: STBC を有効にします。

説明

stbc enable コマンドは STBC を有効にします。

stbc disable コマンドは STBC を無効にします。

undo stbc コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、STBC を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] stbc enable

AP グループ 1 の型番 **QX-W1020** の AP で、STBC を有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] stbc enable

2.1.66 su-txbf

Syntax

su-txbf { **disable** | **enable** }

undo su-txbf

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、ソフトウェアバージョンによりデフォルト状態が異なります。

ソフトウェアバージョン 7.2.21 を含む以前のソフトウェアでは有効です。

ソフトウェアバージョン 7.2.27, 7.2.27a から 7.2.59 のソフトウェアでは無効です。

ソフトウェアバージョン 7.2.63 のソフトウェアでは有効(コンフィグ上は非表示)です。

ソフトウェアバージョン7.2.67 を含む以降のソフトウェアでは無効(コンフィグ上は非表示)です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: シングルユーザの TxBF を無効にします。

enable: シングルユーザの TxBF を有効にします。

説明

su-txbf enable コマンドはシングルユーザの TxBF を有効にします。

su-txbf disable コマンドはシングルユーザの TxBF を無効にします。

undo su-txbf コマンドはデフォルトに戻します。

このコマンドは、802.11ac、802.11gac、802.11ax、802.11gax 無線にのみ適用されます。無線モードを 802.11a、802.11b、802.11g、802.11n に変更すると、コマンドが無効になります。

シングルユーザ TxBF を使用すると、AP は目的の 1 つのクライアントへの信号を改善できます。シングルユーザ TxBF は、広く普及しているクライアント、ネットワーク品質の悪い WLAN、および深刻な信号減衰に適用されます。

radio view の設定は、AP group radio view の設定よりも優先されます。

例

AP **ap1** のシングルユーザ TxBF を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] su-txbf enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、シングルユーザ TxBF を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] su-txbf enable

関連コマンド

mu-txbf

2.1.67 twt negotiate

🕮 メモ：

- **twt negotiate** コマンドはソフトウェアバージョン 7.2.42 を含む以降のソフトウェアからサポートしています。
- **twt negotiate** コマンドは QX-W1100 シリーズおよび QX-W1200 シリーズでのみサポートしています。

Syntax

twt negotiate { **disable** | **enable** }

undo twt negotiate

デフォルト

radio view では、AP group radio view の設定を使用します。

AP group radio view では、ソフトウェアバージョンにより異なります。

ソフトウェアバージョン V7.2.55 を含む以前のソフトウェアでは無効(コンフィグ上は非表示)です。

ソフトウェアバージョン V7.2.56 を含む以降のソフトウェアでは有効(コンフィグ上は非表示)です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

説明

twt negotiate enable コマンドは Target Wake Time(TWT)ネゴシエーションを有効にします。

twt negotiate disable コマンドは TWT ネゴシエーションを無効にします。

undo twt negotiate コマンドはデフォルトに戻します。

このコマンドは、802.11 ax および 802.11 gax でのみ有効です。無線タイプを 802.11 a/b/g/n/ac/gac に変更すると、設定が削除されます。

Trget Wake Time (TWT) ネゴシエーションを使用すると、クライアントと AP はサービス期間中にのみデータパケットを交換し、クライアントの休止状態をスケジュールして、クライアントの電力消費量と無線リソースの競合を減らすことができます。

TWT ネゴシエーションを有効にすると、クライアントはサービス期間、TWT 間隔、および最初のスリープ状態解除時間(クライアントによって計算される)を含むネゴシエーション要求を AP に送信します。このような要求を受信すると、AP は応答を送信します。クライアントはスケジュールに従って起動し、その AP からのトリガーフレームを待機します。トリガーフレームを受信すると、クライアントはサービス期間に入り、その AP とのデータパケットの交換を開始します。サービス期間が終了すると、データパケットの交換が完了していなくても、クライアントは休止モードに入ります。

無線は、最大 8 台のクライアントに TWT サービスを提供できます。8 つのクライアントの TWT ネゴシエーション要求に応答した後、無線は他のクライアントからの要求を拒否します。

Radio view の設定は AP group radio view の設定よりも優先されます。

例

AP ap1 の Radio1 で TWT ネゴシエーションを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ax

[AC-wlan-ap-ap1-radio-1] twt negotiate enable

AP グループ apgroup1 の AP の Radio1 で TWT ネゴシエーションを有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1]ap-model QX-W1130

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] type dot11ax

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] twt negotiate enable

関連コマンド

type dot11ax

2.1.68 type

🕮 **メモ**:

QX-W1240 は 802.11be (draft)に対応しています。

Syntax

type { **dot11a** | **dot11abe** | **dot11ac** | **dot11an** | **dot11ax** | **dot11b** | **dot11be** | **dot11eax** | **dot11g** | **dot11gac** | **dot11gax** | **dot11gbe | dot11gn** }

undo type

デフォルト

QX-W1010 の Radio1、Radio2 の無線モードは、それぞれ dot11ac、dot11gn です。

QX-W1020、QX-W1030 の Radio1、Radio2、Radio3 の無線モードは、それぞれ dot11ac、dot11ac、dot11gn です。

QX-W1110 の Radio1、Radio2 の無線モードは、それぞれ dot11ax、dot11gax です。

QX-W1120 の Radio1、Radio2、Radio3 の無線モードは、それぞれ dot11ax、dot11ax、dot11gn です。

QX-W1130 の Radio1、Radio2、Radio3 の無線モードは、それぞれ dot11ax、dot11ax、dot11gax です。

QX-W1210 の Radio1、Radio2 の無線モードは、それぞれ dot11abe、dot11gbe です。

QX-W1230 の Radio1、Radio2、Radio3 の無線モードは、それぞれ dot11be、dot11abe、dot11gbe です。

QX-W1240 の Radio1、Radio2、Radio3 の無線モードは、それぞれ dot11be、dot11abe、dot11gbe です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

dot11a: 802.11a 無線モードを指定します。

dot11ac: 802.11ac 無線モードを指定します。

dot11an: 802.11n(5GHz)無線モードを指定します。

dot11ax: 802.11ax 無線モードを指定します。

dot11b: 802.11b 無線モードを指定します。

dot11be:802.11be(6GHz 帯) 無線モードを指定します。

dot11eax：802.11ax (6GHz 帯) 無線モードを指定します。

dot11g: 802.11g 無線モードを指定します。

dot11gac: 802.11gac 無線モードを指定します。

dot11gax: 802.11gax 無線モードを指定します。

dot11gbe：802.11be (2.4GHz 帯) 無線モードを指定します。

dot11gn: 802.11n (2.4 GHz) 無線モードを指定します。

🕮 **メモ：**

802.11ac を 2.4GHz で使用するモードを 802.11gac と定義します。
802.11ax を 2.4GHz で使用するモードを 802.11gax と定義します。

説明

type コマンドは無線モードを指定します。

undo type コマンドはデフォルトに戻します。

⚠ **注意：**

有効になっている無線のモードを変更すると、すべての接続されたクライアントが接続解除されます。

メモ：

- QX-W1100 シリーズは Raido3 で 802.11a、ac、an も指定できますが設定した場合 Raido3 が無効になります。
- QX-W1120 は Radio3 で 802.11gax を設定することができません。Radio 3 を 802.11a、ac、an のいずれかに設定することで、Radio 2 を 802.11gax に設定することができます。

AP group radio view で無線のモードを変更すると、無線のモードに関連するコマンドのデフォルト設定が復元されます。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、無線モードを 802.11n (5 GHz)に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、無線モードを 802.11n (5 GHz)に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

2.1.69 ul-ofdma

🕮 **メモ：**

- **ul-ofdma** コマンドはソフトウェアバージョン 7.2.42 を含む以降のソフトウェアからサポートしています。
- **ul-ofdma** コマンドは QX-W1100 シリーズおよび QX-W1200 シリーズでのみサポートしています。

Syntax

ul-ofdma { **disable** | **enable** }

undo ul-ofdma

デフォルト

radio view では、AP group radio view の設定を使用します。

AP group radio view では、ソフトウェアバージョンにより異なります。

ソフトウェアバージョン V7.2.55 を含む以前のソフトウェアでは無効(コンフィグ上は非表示)です。

ソフトウェアバージョン V7.2.56 を含む以降のソフトウェアでは有効(コンフィグ上は非表示)です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

説明

ul-ofdma enable コマンドはアップリンク OFDMA を有効にします。

ul-ofdma disable コマンドはアップリンク OFDMA を無効にします。

undo ul-ofdma コマンドはデフォルトに戻します。

このコマンドは、802.11 ax および 802.11 gax でのみ有効です。無線タイプを 802.11 a/b/g/n/ac/gac に変更すると、設定が削除されます。

Radio view の設定は AP group radio view の設定よりも優先されます。

OFDMA は、小さなデータパケットが送信される高密度環境で有効にすると、次の利点があります。

- 複数ユーザへの同時通信
- 無線使用率の向上
- 転送遅延の短縮
- 衝突バックオフの削減

例

AP ap1 の Radio1 でアップリンク OFDMA を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ax

[AC-wlan-ap-ap1-radio-1] ul-ofdma enable

AP グループ apgroup1 の AP の Radio1 でアップリンク OFDMA を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1]ap-model QX-W1130

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] type dot11ax

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] ul-ofdma enable

関連コマンド

type dot11ax

2.1.70 wlan in-band 6g-discovery

🕮 メモ：

wlan in-band 6g-discovery コマンドはソフトウェアバージョン 7.2.82 を含む以降のソフトウェアからサポートしています。

Syntax

wlan in-band 6g-discovery { enable | mode { fils | upr } }

undo wlan in-band 6g-discovery { enable | mode }

デフォルト

無効

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

enable : 6GHz の無線サービスの検出機能を有効にします。

mode fils : 6GHz の無線サービスの検出方法として **fils** モードを指定します。

mode upr : 6GHz の無線サービスの検出方法として **upr** モードを指定します。

説明

wlan in-band 6g-discovery コマンドは、6GHz の無線サービスの検出機能を有効にし、無線サービスの検出方法を設定します。

undo wlan in-band 6g-discovery コマンドはデフォルトに戻します。

この機能を有効にすると、6GHz 無線で有効になっている無線サービスの情報を、以下のいずれかのフレームを 6GHz 無線から送信することで検出できるようにします。

- **fils** モードでは、FILS(Fast Initial Link Setup）discovery フレームを使用して 6GHz の無線サービスを検出します。FILS discovery フレームは圧縮ビーコンフレームであり、SSID、BSSID、およびチャネルなどの重要な情報のみを含みます。この方法が構成されていると、AP の 6GHz 無線は 20 ミリ秒の間隔で FILS discovery フレームをブロードキャストします。無線サービスの検出方法を指定せずにこの機能を有効にした場合、**fils** モードが使用されます。
- **upr** モードでは、UPR(Unsolicited Probe Response)フレームを使用して 6GHz 無線サービスを検出します。UPR フレームはビーコンフレームと同じ詳細情報を含みます。この方法が構成されていると、AP の 6GHz 無線は 20 ミリ秒の間隔で UPR をブロードキャストします。

例

6GHz 帯無線サービス検出機能を有効にし、検出方法として **fils** を指定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] wlan in-bound 6g-discovery enable

[AC-wlan-global-configuration] wlan in-band 6g-discovery mode fils

2.1.71 wlan multiple-bssid enable

🕮 **メモ：**

wlan multiple-bssid enable コマンドはソフトウェアバージョン 7.2.82 を含む以降のソフトウェアからサポートしています。

Syntax

wlan multiple-bssid enable

undo wlan multiple-bssid

デフォルト

無効

View

Global configuration view

定義済みユーザロール

network-admin

説明

wlan multiple-bssid enable コマンドは、マルチ BSSID 機能を有効にします。

undo wlan multiple-bssid コマンドはデフォルトに戻します。

この設定は 6GHz 無線を使用するときに有効にします。

この機能を有効にすると、AP は 1 つのビーコンフレームまたはプローブ応答に複数の BSSID に関する情報を含めて送信します。

例

#マルチ BSSID 機能を有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] wlan multiple-bssid enable

2.1.72 wlan out-band 6g-discovery

🕮 **メモ**:

wlan out-band 6g-discovery enable コマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

wlan out-band 6g-discovery enable

undo wlan out-band 6g-discovery enable

デフォルト

有効

View

Global configuration view

定義済みユーザロール

network-admin

説明

wlan out-band 6g-discovery enable コマンドは、6GHz 帯無線サービス検出機能を有効にします。

undo wlan out-band 6g-discovery enable コマンドは 6GHz 帯無線サービス検出機能を無効にします。

この設定は 6GHz 無線を使用するときに有効にします。

6GHz 帯無線サービス検出機能を有効にすると、AP の 6GHz 無線インタフェースで有効になっている BSSID の情報を、5GHz または 2.4GHz の無線から送信するパケット内に追加して送信します。

6GHz 無線に対応したクライアントは AP の 2.4GHz または 5GHz の無線から送信されたパケット内の BSSID の情報を読み取ることで、AP の 6GHz 無線を検出することができます。

この設定を使用する場合は、AP の Radio2(5GHz)、または、Radio3(2.4GHz)を有効にして、サービステンプレートを割り当てる必要があります。

例

#AP ap1 の radio2 にサービステンプレート radio2 を割り当て、 6GHz 帯無線サービス検出機能を有効にします。

<AC> system-view

[AC] wlan service-template radio2

[AC-wlan-st-radio2] ssid radio2

[AC-wlan-st-radio2] service-template enable

[AC-wlan-st-radio2] quit

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] radio enable

[AC-wlan-ap-ap1-radio-2] wlan service-template radio2

[AC-wlan-ap-ap1-radio-2] return

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] wlan out-bound 6g-discovery enable

2.1.73 wlan radio

Syntax

wlan radio { **disable** | **enable** }

undo wlan radio

デフォルト

radio view または AP group radio view で無線が有効になっていない場合、無線は無効になります。

View

System view

定義済みユーザロール

network-admin

パラメータ

disable: すべての無線を無効にします。

enable: すべての無線を有効にします。

説明

wlan radio enable コマンドはすべての無線を有効にします。

wlan radio disable コマンドはすべての無線を無効にします。

undo wlan radio コマンドはデフォルトに戻します。

⚠ **注意：**

この機能は、すべての手動 AP とオンライン自動 AP で有効です。

---

wlan radio { **disable** | **enable** }コマンドと **radio** { **disable** | **enable** }コマンドを使用すると、最新の設定が有効になります。

例

すべての無線を有効にする。

<AC> system-view

[AC] wlan radio enable

関連コマンド

radio { **disable** | **enable** }

目次

このセクションのページは **2-x-x** です。

3 章 WLAN アクセスの設定 3-1
3.1 WLAN アクセスの設定コマンド 3-1
3.1.1 access-control acl 3-1
3.1.2 beacon ssid-hide 3-2
3.1.3 broadcast-probe reply 3-3
3.1.4 client association-location 3-4
3.1.5 client cache aging-time 3-5
3.1.6 client forwarding-location 3-7
3.1.7 client frame-format 3-8
3.1.8 client idle-timeout 3-9
3.1.9 client keep-alive 3-10
3.1.10 client keep-alive interval 3-11
3.1.11 client max-count 3-12
3.1.12 client preferred-vlan authorized 3-13
3.1.13 client vlan-alloc 3-13
3.1.14 description 3-14
3.1.15 display wlan ap region-code 3-15
3.1.16 display wlan blacklist 3-16
3.1.17 display wlan bss 3-17
3.1.18 display wlan client 3-19
3.1.19 display wlan client device-information 3-27
3.1.20 display wlan client failure 3-29
3.1.21 display wlan client history-record mac-address 3-30
3.1.22 display wlan client online-duration 3-32
3.1.23 display wlan client status 3-33
3.1.24 display wlan region-code ap (v7.1.13 以前のみ) 3-35
3.1.25 display wlan service-template 3-36
3.1.26 display wlan statistics (v7.1.13 以前のみ) 3-42
3.1.27 display wlan statistics client 3-45
3.1.28 display wlan statistics connect-history 3-46
3.1.29 display wlan statistics service-template 3-48
3.1.30 display wlan whitelist 3-49
3.1.31 dot11ax support maximum-he-mcs 3-50
3.1.32 inherit exclude service-template 3-51
3.1.33 map-configuration 3-52
3.1.34 nas-id 3-53

3.1.35 nas-port-id 3-54
3.1.36 nas-vlan 3-56
3.1.37 quick-association enable 3-56
3.1.38 region-code 3-57
3.1.39 region-code-lock 3-59
3.1.40 reset wlan client 3-60
3.1.41 reset wlan dynamic-blacklist 3-61
3.1.42 reset wlan statistics client 3-61
3.1.43 reset wlan statistics service-template 3-62
3.1.44 service-template 3-63
3.1.45 service-template enable 3-64
3.1.46 snmp-agent trap enable wlan client 3-65
3.1.47 snmp-agent trap enable wlan client-audit 3-66
3.1.48 ssid 3-66
3.1.49 unknown-client 3-68
3.1.50 user-profile 3-69
3.1.51 vlan 3-70
3.1.52 wlan client failure history aging 3-71
3.1.53 wlan client forwarding enable 3-71
3.1.54 wlan client reauthentication-period 3-72
3.1.55 wlan dynamic-blacklist active-on-ap 3-73
3.1.56 wlan dynamic-blacklist lifetime 3-74
3.1.57 wlan link-test 3-75
3.1.58 wlan nas-port-id format 3-76
3.1.59 wlan permit-ssid 3-78
3.1.60 wlan service-template 3-79
3.1.61 wlan static-blacklist mac-address 3-79
3.1.62 wlan web-server api-path 3-80
3.1.63 wlan web-server host 3-81
3.1.64 wlan web-server max-client-entry 3-82
3.1.65 wlan whitelist mac-address 3-83

3章 WLAN アクセスの設定

3.1 WLANアクセスの設定コマンド

3.1.1 access-control acl

🕮 メモ：

access-control acl コマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

access-control acl *acl-number*

undo access-control acl

デフォルト

設定無し

View

AP view

Service template view

定義済みユーザロール

network-admin

パラメータ

acl-number: レイヤ 2 ACL の番号を 4000 から 4999 の範囲で指定します。

説明

access-control acl コマンドは ACL にもとづくアクセスに使用する ACL を設定します。

undo access-control acl コマンドはデフォルトに戻します。

この機能は、指定された ACL ルールを使用してクライアントアクセスを制御します。デバイスはアソシエーション要求を受信すると、次のアクションを実行します。

- クライアントの MAC アドレスがルール内の MAC アドレス属性または MAC アドレス OUI 属性と一致し、ルールアクションが permit の場合に、クライアントに WLAN へのアクセスを許可します。複数のクライアントが OUI 属性に一致する場合、これらのすべてのクライアントは WLAN へのアクセスを許可されます。
- 一致するルールが見つからない場合、または一致するルールのアクションが deny の場合、クライアントの WLAN へのアクセスを拒否します。

この機能を設定する場合は、次の制約事項および注意事項に従ってください。

- 指定した ACL に permit ルールが設定されていない場合、クライアントのアクセスは許可されません。
- 指定できる ACL は 1 つだけです。このコマンドを複数回実行した場合は、最新の設定が有効になります。
- AP View の設定は、サービステンプレート View の設定よりも優先されます。

例

ACL 4000 を作成し、MAC アドレスが 006e-35b2-000e のクライアントおよび指定された OUI のクライアントアクセスを許可する ACL ルールを作成します。サービステンプレート service 1 に ACL4000 を指定します。

<AC> system-view

[AC] acl mac 4000

[AC-acl-mac-4000] rule 0 permit source-mac 006e-35b2-000e ffff-ffff-ffff

[AC-acl-mac-4000] rule 1 permit source-mac 006e-3500-0000 ffff-ff00-0000

[AC-acl-mac-4000] quit

[AC] wlan service-template service1

[AC-wlan-st-service1] access-control acl 4000

ACL 4000 を作成し、MAC アドレスが 006e-35b2-000e のクライアントおよび指定された OUI のクライアントを許可する ACL ルールを作成します。AP ap1 に ACL 4000 を指定します。

<AC> system-view

[AC] acl mac 4000

[AC-acl-mac-4000] rule 0 permit source-mac 006e-35b2-000e ffff-ffff-ffff

[AC-acl-mac-4000] rule 1 permit source-mac 006e-3500-000f ffff-ff00-0000

[AC-acl-mac-4000] quit

[AC] wlan ap ap1 model QX-W1010

[AC-wlan-ap-ap1] access-control acl 4000

3.1.2 beacon ssid-hide

Syntax

beacon ssid-hide

undo beacon ssid-hide

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

beacon ssid-hide コマンドは SSID ステルスを有効にします。

undo beacon ssid-hide コマンドはデフォルトに戻します。

このコマンドを有効にすると、無線がビーコンフレーム内で SSID を伝送しないようになり、指定したサービステンプレートが無線にバインドされた後にプローブ要求に応答しなくなります。

⚠ **注意：**

6GHz 帯の SSID で SSID ステルスを有効にすると接続できない端末があります。
6GHz 帯で利用するサービステンプレートでは SSID ステルスを有効にしないでください。

例

ビーコンフレームで SSID の通知を無効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] beacon ssid-hide

3.1.3 broadcast-probe reply

Syntax

broadcast-probe reply { **disable** | **enable** }

undo broadcast-probe reply

デフォルト

AP view：AP group view の設定を使用します。

AP group view：ブロードキャストプローブ要求に応答します。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: AP のブロードキャストプローブ要求への応答を無効にします。

enable: AP のブロードキャストプローブ要求への応答を有効にします。

説明

broadcast-probe reply enable コマンドは AP のブロードキャストプローブ要求への応答を有効にします。

broadcast-probe reply disable コマンドは AP のブロードキャストプローブ要求への応答を無効にします。

undo broadcast-probe reply コマンドはデフォルトに戻します。

ブロードキャストプローブ要求には SSID は含まれません。AP はブロードキャストプローブ要求を受信すると、AP のサービス情報を含んだプローブ応答を返信します。ユニキャストプローブ要求を送信するクライアントが AP に接続することができるようにするには、AP がブロードキャストプローブ要求に応答しないようにします。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1** をブロードキャストプローブ要求に応答しないようにします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] broadcast-probe reply disable

AP グループ **group1** の AP をブロードキャストプローブ要求に応答しないようにします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] broadcast-probe reply disable

3.1.4 client association-location

Syntax

client association-location { **ac** | **ap** }

undo client association-location

デフォルト

AC

View

Service template view

定義済みユーザロール

network-admin

パラメータ

ac: AC でのクライアントの関連付けを有効にします。

ap: AP でのクライアントの関連付けを有効にします。

説明

client association-location コマンドは AC または AP でのクライアントアソシエーションを有効にします。

undo client association-location コマンドはデフォルトに戻します。

client association-location コマンドと **client-security authentication-location** コマンドでは同一の装置を指定してください。**client-security authentication-location** コマンドの詳細については、コマンドマニュアルのセクション 2 *WLAN* の“*WLAN 認証*”を参照してください。

このコマンドを実行する前に、サービステンプレート が無効であることを確認してください。

例

AC でのクライアントの関連付けを有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client association-location ac

関連コマンド

client-security authentication-location（コマンドマニュアルのセクション 2 *WLAN “WLAN 認証”*）

3.1.5 client cache aging-time

Syntax

client cache aging-time aging-time

undo client cache aging-time

デフォルト

180 秒

View

Service template view

定義済みユーザロール

network-admin

パラメータ

aging-time: エージングタイマを指定します。設定範囲は 0～86400 秒です。エージングタイマを 0 に設定した場合、クライアントがオフラインになった直後にクライアントのキャッシュ情報を削除します。

説明

client cache aging-time コマンドはクライアントキャッシュエージングタイマを設定します。

undo client cache aging-time コマンドはデフォルトに戻します。このコマンドを実行する前に、サービステンプレートが無効であることを確認してください。

クライアントキャッシュは、クライアント用の PMK リストやアクセス VLAN などの情報を保存します。クライアントはキャッシュエージングタイマが経過する前に別の AP にローミングすると、キャッシュ情報を継承できます。キャッシュエージングタイマが経過する前にクライアントがオンラインにならない場合、そのキャッシュ情報はクリアされます。

例

エージングタイマを 100 秒に設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client cache aging-time 100

3.1.6 client forwarding-location

Syntax

client forwarding-location { **ac** | **ap** }

undo client forwarding-location

デフォルト

AP

View

Service template view

定義済みユーザロール

network-admin

パラメータ

ac: AC がクライアントデータトラフィックを転送します。

ap: AP がクライアントデータトラフィックを転送します。

説明

client forwarding-location コマンドはクライアントデータトラフィックフォワーダを指定します。

ソフトウェアバージョン 7.2.18 を含む以前のソフトウェアでは、**undo client forwarding-location** コマンドは ac が設定されます。

ソフトウェアバージョン 7.2.21 を含む以降のソフトウェアでは、**undo client forwarding-location** コマンドは ap が設定されます。

このコマンドを実行する前に、サービステンプレート が無効であることを確認してください。

AC トラフィックがクライアントトラフィックフォワーダとして設定されている場合、クライアントのトラフィックフォワーディングが有効になっていることを確認してください。

例

AP がクライアントデータトラフィックを転送するように設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client forwarding-location ap

3.1.7 client frame-format

Syntax

client frame-format { **dot3** | **dot11** }

undo client frame-format

デフォルト

802.3 カプセル化フォーマット

View

Service template view

定義済みユーザロール

network-admin

パラメータ

dot3: クライアントデータフレームを 802.3 フォーマットでカプセル化します。

dot11: クライアントデータフレームを 802.11 フォーマットでカプセル化します。

説明

client frame-format コマンドはクライアントデータフレームのカプセル化モードを設定します。

undo client frame-format コマンドはデフォルトに戻します。

このコマンドを実行する前に、サービステンプレートが無効であることを確認してください。

このコマンドは、中央転送モードでのみ有効です。

例

#クライアントデータフレームを 802.11 フォーマットでカプセル化します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client frame-format dot11

関連コマンド

client forwarding-location

3.1.8 client idle-timeout

Syntax

client idle-timeout *interval*

undo client idle-timeout

デフォルト

AP view：AP group view の設定を使用します。

AP group view：ソフトウェアバージョンにより異なります。

ソフトウェアバージョン 7.2.79 を含む以前のソフトウェア：3600 秒

ソフトウェアバージョン 7.2.82 を含む以降のソフトウェア：300 秒

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

interval: クライアントアイドルタイムアウト時間を指定します。設定範囲は 60～86400 秒です。

説明

client idle-timeout コマンドはクライアントアイドルタイムアウト時間を設定します。

undo client idle-timeout コマンドはデフォルトに戻します。

クライアントアイドルタイムアウト時間内にオンラインクライアントが接続した AP にフレームを送信しない場合、AP はクライアントをログオフします。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1** のクライアントアイドルタイムアウト時間を 200 秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] client idle-timeout 200

AP group **group1** のクライアントアイドルタイムアウト時間を 200 秒に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] client idle-timeout 200

3.1.9 client keep-alive

Syntax

client keep-alive { **disable** | **enable** }

undo client keep-alive

デフォルト

AP view： AP group view の設定を使用します。

AP group view：無効

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: クライアントキープアライブを無効にします。

enable: クライアントキープアライブを有効にします。

説明

client keep-alive enable コマンドはクライアントキープアライブを有効にします。

client keep-alive disable コマンドはクライアントキープアライブを無効にします。

undo client keep-alive コマンドはデフォルトに戻します。

AP は、クライアントにキープアライブ間隔でキープアライブパケットを送信し、クライアントがオンラインかどうかを確認できます。キープアライブ間隔 3 回でクライアントからの応答を受信しない場合、AP はクライアントをログオフします。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1** のクライアントキープアライブを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] client keep-alive enable

AP group **group1** のクライアントキープアライブを有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] client keep-alive enable

関連コマンド

client keep-alive interval

3.1.10 client keep-alive interval

Syntax

client keep-alive interval *value*

undo client keep-alive interval

デフォルト

AP view：AP group view の設定を使用します。

AP group view：300 秒

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

interval: クライアントのキープアライブ間隔を指定します。設定範囲は 3～1800 秒です。

説明

client keep-alive interval コマンドはクライアントキープアライブ間隔を設定します。

undo client keep-alive interval コマンドはデフォルトに戻します。

このコマンドを実行する前に、クライアントキープアライブを有効にしてください。

AP は、クライアントにキープアライブ間隔でキープアライブパケットを送信し、クライアントがオンラインかどうかを確認できます。キープアライブ間隔 3 回でクライアントからの応答を受信しない場合、AP はクライアントをログオフします。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1 の**キープアライブ間隔を 20 秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] client keep-alive interval 20

AP group **group1 の**キープアライブ間隔を 20 秒に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] client keep-alive interval 20

関連コマンド

client keep-alive enable

3.1.11 client max-count

Syntax

client max-count *max-number*

undo client max-count

デフォルト

制限なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

max-number: 1～512 の範囲内のクライアントの最大数を指定します。

説明

client max-count コマンドはサービステンプレートに関連するクライアントの最大数を設定します。

undo client max-count コマンドはデフォルトに戻します。

この機能を設定すると、新しいクライアントは最大数に達すると WLAN にアクセスできなくなります。

例

サービステンプレート **service1** の関連するクライアントの最大数を 38 に設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client max-count 38

3.1.12 client preferred-vlan authorized

Syntax

client preferred-vlan authorized

undo client preferred-vlan authorized

デフォルト

クライアントは、ローミング後に許可 VLAN を使用します。

View

Service template view

定義済みユーザロール

network-admin

説明

client preferred-vlan authorized コマンドはローミング後に許可 VLAN を優先するようにクライアントを設定します。

undo client preferred-vlan authorized コマンドはローミング後にクライアント VLAN が変更されないように設定します。

この機能は 802.1X および MAC 認証クライアントでのみ有効です。

通常、クライアントの VLAN は、クライアントのローミング後も変更されません。ただし、クライアントが別の AP にローミングした後に QMC で設定されたセキュリティ警告をトリガすると、ユーザ分離のために発行された許可 VLAN が有効になります。

例

ローミング後に許可 VLAN を優先するようにクライアントを設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client preferred-vlan authorized

3.1.13 client vlan-alloc

Syntax

client vlan-alloc { **dynamic** | **static** }

undo client vlan-alloc { **dynamic** | **static** }

デフォルト

dynamic

View

Service template view

Predefined user roles

network-admin

パラメータ

dynamic: ダイナミック VLAN 割り当てを指定します。

static: スタティック VLAN 割り当てを指定します。

定義済みユーザロール

client vlan-alloc コマンドはクライアントの VLAN 割り当て方法を指定します。

undo client vlan-alloc コマンドはデフォルトに戻します。

クライアントが初めてオンラインになると、無線はランダムな VLAN を割り当てます。クライアントが再びオンラインになると、クライアントに割り当てられた VLAN は割り当て方法に依存します。

- **Static allocation**–クライアントは、割り当てられた VLAN を継承します。IP アドレスのリースが期限切れになっていない場合、クライアントは同じ IP アドレスを使用します。この方法は、IP アドレスを節約するのに役立ちます。
- **Dynamic allocation**–クライアントに VLAN が再割り当てされます。この方法では、すべての VLAN のクライアントで負荷を分散させます。

例

クライアントの VLAN 割り当て方法をダイナミックに指定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client vlan-alloc dynamic

3.1.14 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

text: description 名を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別します。

説明

description コマンドはサービステンプレートの説明を構成します。

undo description コマンドはデフォルトに戻します。

例

サービステンプレート service1 に description 名 wlanst を指定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] description wlanst

3.1.15 display wlan ap region-code

🕮 **メモ：**

display wlan ap region-code コマンドはソフトウェアバージョン 7.2.18 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan ap { **all** | **name** *ap-name* } **region-code**

View

すべての view

定義済みユーザロール

network-admin

パラメータ

all: 全ての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan region-code ap コマンドはすべての AP または指定した AP の地域コード情報を表示します。

例

すべての AP の地域コード情報を表示します。

<AC> display wlan ap all region-code

```
Region Code
--------------------------------------------------------------------------
AP name              Region Code
ap1                  JP  JAPAN
ap2                  JP  JAPAN
ap3                  JP  JAPAN
```

表 3-1 コマンド出力

フィールド	説明
Region Code	地域コード。地域コードの詳細については、表 3-16を参照してください。

3.1.16 display wlan blacklist

Syntax

display wlan blacklist { **dynamic** | **static** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dynamic: 動的なブラックリストを指定します。

static: 静的なブラックリストを指定します。

説明

display wlan blacklist コマンドはブラックリストエントリを表示します。

例

静的なブラックリストエントリを表示します。

<AC> display wlan blacklist static

```
Total number of clients: 3
 MAC addresses:
  000e-35b2-000e
  0019-5b8e-b709
  001c-f0bf-9c92
```

動的なブラックリストエントリを表示します。

<AC> display wlan blacklist dynamic

```
Total number of clients: 3
MAC address    APID  Lifetime (s)  Duration (hh:mm:ss)
000f-e2cc-0001  1    300           00:02:11
000f-e2cc-0002  2    300           00:01:17
000f-e2cc-0003  3    300           00:02:08
```

表 3-2 コマンド出力

フィールド	説明
MAC address	クライアントMACアドレス。
APID	不正なクライアントを検出したAPのID。
Lifetime (s)	エントリの寿命（秒単位）。
Duration (hh:mm:ss)	エントリが動的ブラックリストに追加されてからエントリ期間。

3.1.17 display wlan bss

🕮 **メモ：**

display wlan bss コマンドはソフトウェアバージョン 7.2.46 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan bss { **all** | **ap** *ap-name* | **bssid** *bssid* } [**slot** *slot-number*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての BSS を表示します。

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

bssid *bssid*: BSS を ID で指定します。ID は、48 ビットの 16 進数で H-H-H の形式で指定してください。

slot *slot-number*: IRF スタックのメンバ装置のメンバ ID を指定します。メンバ ID を指定しない場合、マスタ装置の情報を表示します。

verbose: 詳細な BSS 情報を表示します。 このキーワードを指定しない場合、BSS 情報の概要を表示します。

説明

display wlan bss コマンドは BSS（Basic Service Set）情報を表示します。

例

すべての BSS の簡潔な情報を表示します。

<AC> display wlan bss all

```
Current BSS number: 4
Max BSS number: 16384
Bound BSS number: 4
AP name                 RID  SSID                        BSSID
ap1                     1    SSID1                       0f00-ef65-6400
ap1                     2    SSID1                       0f00-ef65-6401
ap2                     1    SSID1                       0f00-ef14-dd08
ap2                     2    SSID1                       0f00-ef14-dd09
```

ID が 0f00-ef65-6400 の BSS の詳細情報を表示します。

<AC> display wlan bss bssid 0f00-ef65-6400 verbose

```
AP name                    : ap1
BSSID                      : 0f00-ef65-6400
Radio ID                   : 1
Service template name      : servcie1
```

```
SSID                        : SSID1
VLAN ID                     : 1
Service VLAN ID             : N/A
AKM mode                    : Not configured
User authentication mode    : Bypass
```

表 3-3 コマンド出力

フィールド	説明
AKM mode	AKMモード： • 802.1X • PSK • 設定なし
User authentication mode	ユーザ認証モード： • **Bypass**－クライアント認証なし • **MAC** • **802.1X** • **OUI**

3.1.18 display wlan client

Syntax

display wlan client [**ap** *ap-name* [**radio** *radio-id*] | **mac-address** *mac-address* | **service-template** *service-template-name* | **frequency-band** { **2.4** | **5** }] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*: 指定した AP に接続されているクライアントに関する情報を表示します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

radio *radio-id*: 指定した無線に接続されているクライアントに関する情報を表示します。*radio-id* の範囲は、デバイスモデルによって異なります。このオプションを指定しないと、指定した AP に接続されているすべてのクライアントに関する情報が表示されます。

mac-address *mac-address*: クライアントを MAC アドレスで指定します。

service-template *service-template-name*: 指定したサービステンプレートに関連付けられているクライアントに関する情報を表示します。サービステンプレート名は、1～63 文字の文字列です。大文字と小文字を区別しません。

frequency-band: 指定されたバンドで作業しているクライアントに関する情報を表示します。

2.4: 2.4GHz 帯を指定します。

5: 5GHz 帯を指定します。

verbose: 詳細なクライアント情報を表示します。このキーワードを指定しない場合、クライアント情報の概要を表示します。

説明

display wlan client コマンドはクライアント情報を表示します。

例

すべてのクライアントに関する簡潔なクライアント情報を表示します。

<AC> display wlan client

```
Total number of clients: 3

MAC address    Username  AP name       RID   IP address     IPv6 address   VLAN
000f-e265-6400 N/A       ap1           1     1.1.1.1                       100
000f-e265-6401 user      ap2           1     3.0.0.3                       200
000f-e214-dd08 N/A       ap1           1     5.5.5.3        1::2:0:0:3     1
```

表 3-4 コマンド出力

フィールド	説明
MAC address	クライアントMACアドレス。
Username	クライアントユーザ名 ● クライアントのユーザ名（802.1X認証またはMAC認証を使用している場合） ● N/A（802.1X認証またはMAC認証を使用していない場合） 🕮 **メモ：** クライアントがポータル認証を使用する場合、このフィールドにクライアントのポータルユーザ名は表示されません。

フィールド	説明
AP name	クライアントが関連付けられているAPの名前。
RID	クライアントが関連付けられている無線のID。
IP address	クライアントのIPv4アドレス。
IPv6 address	クライアントのIPv6アドレス。
VLAN ID	クライアントが属するVLANのID。

すべてのクライアントに関する詳細なクライアント情報を表示します。

<AC> display wlan client verbose

```
Total number of clients: 1

 MAC address                    : d0c6-37af-8cc3
 IPv4 address                   : 1.1.1.1
 IPv6 address                   : N/A
 Username                       : N/A
 AID                            : 1
 AP ID                          : 1
 AP name                        : ap1
 Radio ID                       : 1
 Channel                        : 36
 SSID                           : office
 BSSID                          : 882a-5e6c-4e60
 VLAN ID                        : 1
 Service VLAN ID                : N/A
 Sleep count                    : 0
 Wireless mode                  : 802.11ac
 Channel bandwidth              : 80MHz
 SM power save                  : Disabled
 Short GI for 20MHz             : Supported
 Short GI for 40MHz             : Supported
 Short GI for 80MHz             : Supported
 Short GI for 160/80+80MHz      : Not supported
 STBC RX capability             : Supported
 STBC TX capability             : Supported
 LDPC RX capability             : Supported
 Beamformee STS capability      : N/A
 Number of Sounding Dimensions  : N/A
 SU beamformee capability       : Not supported
```

```
 MU beamformee capability        : Not supported
 Block Ack                      : N/A
 Supported VHT-MCS set           : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
                                 NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
 Supported HT MCS set            : 0, 1, 2, 3, 4, 5, 6, 7,
                                 8, 9, 10, 11, 12, 13, 14,
                                 15
 Supported rates                 : 6, 9, 12, 18, 24, 36,
                                 48, 54 Mbps
 QoS mode                       : WMM
 Listen interval                 : 250
 RSSI                           : 0
 Rx/Tx rate                     : 0/0 Mbps
 Speed                          : N/A
 Authentication method           : Open system
 Security mode                  : RSN
 AKM mode                       : PSK
 Cipher suite                   : CCMP
 User authentication mode        : Bypass
 WPA3 status                    : Disabled
 Authorization CAR               : N/A
 Authorization ACL ID            : N/A
 Authorization user profile      : N/A
 Roam status                    : N/A
 Key derivation                 : SHA1
 PMF status                     : N/A
 Forwarding policy name          : Not configured
 Online time                    : 0days 0hours 0minutes 36seconds
 FT status                      : Inactive
BTM mode                        : Inactive
```

表 3-5 コマンド出力

フィールド	説明
MAC address	クライアントMACアドレス。
IPv4 address	クライアントIPv4アドレス。
IPv6 address	クライアントIPv6アドレス。

フィールド	説明
Username	クライアントユーザ名 ● クライアントのユーザ名（802.1X認証またはMAC認証を使用している場合） ● **N/A**（802.1X認証またはMAC認証を使用していない場合） 🕮 メモ： クライアントがポータル認証を使用する場合、このフィールドにクライアントのポータルユーザ名は表示されません。
AID	アソシエーションID。
AP ID	クライアントが接続しているAPのID。
AP name	クライアントが接続しているAPの名前。
Radio ID	クライアントが接続している無線のID。
SSID	クライアントが接続しているSSID。
VLAN ID	クライアントが属するVLANのID。
Sleep count	スリープ状態への遷移数。
Wireless mode	無線モード。 ● 802.11a. ● 802.11b. ● 802.11g. ● 802.11gn. ● 802.11an. ● 802.11ac. ● 802.11ax.
Channel bandwidth	チャネル帯域幅、20MHz、40MHz、80MHz、160MHz。
SM Power Save	SM Power Saveは、クライアントの1つのアンテナだけをアクティブ状態、他のものはスリープ状態で動作させ、電力を節約することを可能にします。 ● **Enabled**–有効 ● **Disabled**–無効
SM power save mode	省電力モード。 ● Dynamic. ● Static.

フィールド	説明
Short GI for 20MHz	チャネル帯域幅が20MHzのときにクライアントがショートGIをサポートするかどうか。 ● Supported. ● Not supported.
Short GI for 40MHz	チャネル帯域幅が40MHzのときにクライアントがショートGIをサポートするかどうか。 ● Supported. ● Not supported.
Short GI for 80MHz	チャネル帯域幅が80MHzのときにクライアントがショートGIをサポートするかどうか。 ● Supported. ● Not supported.
Short GI for 160/80+80MHz	チャネル帯域幅が160/80+80MHzのときにクライアントがショートGIをサポートするかどうか。 ● Supported. ● Not supported.
STBC Rx Capability	クライアントSTBC受信能力 ● Not supported. ● Supported.
STBC Tx Capability	クライアントSTBC送信能力 ● Not supported. ● Supported.
LDPC Rx capability	クライアントLDPC受信能力 ● Not supported. ● Supported.
SU beamformee capability	クライアントSU beamformee 能力 ● Not supported. ● Supported. このフィールドは802.11ac/ax無線でのみサポートします。
MU beamformee capability	クライアントMU beamformee 能力 ● Not supported. ● Supported. このフィールドは802.11ac/ax無線でのみサポートします。
Beamformee STS capability	クライアント beamformee STS能力 ● Not supported. ● Supported. このフィールドは802.11ac/ax無線でのみサポートします。

フィールド	説明
Block Ack	TIDを用いたブロックアックのネゴシエーション結果。 • **IN**–受信方向からトラフィックのブロックアックを送信します。 • **OUT**–送信方向からトラフィックのブロックアックを送信します。 • **BOTH**–送受信方向からトラフィックのブロックアックを送信します。
Supported VHT-MCS set	クライアントによってサポートされたVHT-MCS
Supported HT MCS set	クライアントによってサポートされたHT-MCS
QoS mode	QoS モード。 • **N/A**–WMMに対応しません。 • **WMM**–WMMに対応します。 WMM情報ネゴシエーションは、WMMをサポートするAPとクライアントの間で実行されます。
Listen interval	クライアントがビーコンフレームを受信するためにウェイクアップする間隔。 ビーコン間隔でカウントされます。
RSSI	受信した信号強度の表示。この値は、APによって検出されたクライアントの信号強度を示します。
Rx/Tx rate	データ、管理、制御フレームの送信および受信レート。
Speed	過去2分間の送受信レートの表示(Kbps単位)。小数点以下3桁で四捨五入。 N/A：送信レートと受信レートの両方が0の場合。
Authentication method	認証方式、オープンシステム、または共有鍵。
Security mode	セキュリティモード。 • **RSN**–ビーコンおよびプローブ応答はRSN IEを伝送します。 • **WPA**–ビーコンおよびプローブ応答はWPA IEを伝送します。 • **PRE-RSNA**-ビーコンおよびプローブ応答はRSN IE/WPA IEを伝送しません。
AKM mode	AKMモード。 • 802.1X • PSK • Not configured.

フィールド	説明
Cipher suite	暗号スイート。 ● N/A. ● WEP40. ● WEP104. ● WEP128. ● CCMP. ● TKIP.
User authentication mode	ユーザ認証モード。 ● **Bypass**–クライアント認証なし。 ● **MAC**. ● **802.1X**. ● **OUI**.
Authorization ACL ID	許可されたACL番号表示 ● ACL番号：許可されたACLが有効になった場合 ● ACL番号 + **Not effective**: 許可されたACLが無効になった場合 ● **N/A**：許可されたACLがない場合
Authorization user profile	許可されたユーザプロファイル名表示 ● 許可されたユーザプロファイル名：許可されたACLが有効になった場合 ● 許可されたユーザプロファイル名 + **Not effective** : 許可されたACLが無効になった場合 ● **N/A**：許可されたユーザプロファイルがない場合
Roam status	Roam状態 ● Roaming in progress. ● Inter-AC slow roaming. ● Inter-AC fast roaming. ● Intra-AC slow roaming. ● Intra-AC fast roaming. ● **N/A**：クライアントがオンラインになった後、1つのBSSに留まっている場合
Key derivation	キー派生タイプ： ● **SHA1**–HMAC-SHA1ハッシュアルゴリズムを使用します。 ● **SHA256**–HMAC-SHA256ハッシュアルゴリズムを使用します。 ● **N/A**–アルゴリズムを使用しません。

フィールド	説明
PMF status	PMF状態 ● **Enabled**–管理フレーム保護が有効になっています。 ● **Disabled**–管理フレーム保護が無効になっています。 ● **N/A**–管理フレームの保護は行われません。
Forward policy	WLAN転送ポリシ ● **Not configured**– WLAN転送ポリシが設定されていません。 ● policy-name.
Online time	クライアントのオンライン期間。
FT status	Fast BSS transition (FT). ● **Active**-FT有効 ● **Inactive**-FT無効
BTM mode	BSS transition management (BTM) ● **Active**-BTM有効 ● **Inactive**-BTM無効

3.1.19 display wlan client device-information

🕮 **メモ：**

display wlan client device-information コマンドはソフトウェアバージョン 7.2.46 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan client device-information [**mac-address** *mac-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address *mac-address*: クライアントを MAC アドレスで指定します。MAC アドレスを省略した場合、オンライン状態の全クライアントのデバイス情報を表示します。

説明

display wlan client device-information コマンドはクライアントのデバイス情報を表示します。

例

指定したクライアントのデバイス情報を表示します。

<AC> display wlan client device-information mac-address 80b6-5511-2233

```
MAC address                              : 80b6-5511-2233
 Vendor Name                             : Unknown
 Host Name                               : DESKTOP-abcdef
```

すべてのクライアントのデバイス情報を表示します。

<AC> display wlan client device-information

```
Total number of clients: 3

MAC address                              : 80b6-5511-2233
 Vendor Name                             : Unknown
 Host Name                               : DESKTOP-abcdef

 MAC address                             : b40e-de12-3456
 Vendor Name                             : PC
 Host Name                               : LAPTOP-112233

MAC address                              : 4826-2caa-bbcc
 Vendor Name                             : Apple
 Host Name                               : test
```

表 3-6 コマンド出力

フィールド	説明
MAC address	クライアントMACアドレス。
Vendor Name	クライアントのMACアドレスOUIから判別したベンダー名を表示します。 以下の場合は、Unknownが表示されます。 ● クライアントがIOSオペレーティングシステムを使用している場合 ● クライアントがランダムMACアドレスを使用している場合 ● OUIリストからベンダーが特定できなかった場合
Host Name	クライアントのホスト名を表示します。 クライアントの送信したDHCP option21から情報を取得して表示します。 以下の場合は、Unknownが表示されます。 ● クライアントがIOSオペレーティングシステムを使用している場合 ● クライアントが固定IPアドレスを使用している場合

3.1.20 display wlan client failure

🕮 メモ：

display wlan client failure コマンドは、ソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan client failure

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan client failure コマンドはクライアントの接続失敗情報を表示します。

同じクライアントの失敗情報は最新情報のみ記録されます。

失敗したクライアントが最終的に接続に成功した場合、リストから削除されます。

失敗情報の記憶時間は **wlan client failure history aging** コマンドで設定できます。

例

クライアントの接続失敗情報を表示します。

<AC> display wlan client failure

```
association failures: 1
authentication failures: 1
-----------
 Association failures:
 Client-info                      AP name    R SSID    Time
 D8E2-657A-670F/-(-)               ap1        1 xxx     2022-09-12 15:09:49

 Authentication failures:
 Client-info                      AP name    R SSID    Time
 15AB-C5E7-DDE4/-(-)               ap2        1 yyy     2022-09-12 15:30:52
```

表 3-7 コマンド出力

フィールド	説明
association failures	アソシエーションフェーズで失敗したクライアントリストの数です。
authentication failures	認証フェーズで失敗したクライアント数です。
Association failures	アソシエーションフェーズで失敗したクライアントの情報を表示します。
Authentication failures	認証フェーズで失敗したクライアントの情報を示します。
Client-info	失敗したクライアントの情報です。MACアドレス、IPアドレス、ユーザ名が表示されます。情報がない部分は"-"で表示されます。
AP name	失敗したAP名
R	失敗したラジオ
SSID	失敗したSSID
Time	失敗時刻

3.1.21 display wlan client history-record mac-address

🕮 **メモ：**

display wlan client history-record mac-address コマンドは、ソフトウェアバージョン 7.2.93a を含む以降のソフトウェアからサポートしています。

Syntax

display wlan client history-record mac-address *mac-address*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address: クライアントの MAC アドレスを H-H-H の形式で指定します。

説明

display wlan client history-record mac-address コマンドは、指定された MAC アドレスのクライアントの接続および切断記録を表示します。

例

MAC アドレス 0394-11aa-22bb のクライアントの接続および切断記録を表示します。

<AC> display wlan client history-record mac-address 0394-11aa-22bb

```
Tips: To view the meaning of the reason code, run the "display system internal
wlan client history-record help reason-code" command in probe view
Time           AP name  AP ID/RID        SSID          State   Reason
06-17 05:09:27 w1120     12/1     000-test-ssid       Online    0
06-17 05:09:14 w1120      12/1     000-test-ssid      Offline 5025
06-17 05:08:42 w1120      12/1     000-test-ssid      Online    0
```

表 3-8 コマンド出力

フィールド	説明
Time	クライアントがオンラインまたはオフラインになった日時。
AP name	クライアントが関連付けられているAPの名前。
AP ID/RID	クライアントが関連付けられているAPおよび無線のID。
SSID	クライアントが関連付けられているSSID。
State	クライアントの関連付けおよび切断のステータス。Onlineは関連付けの成功、Offlineは切断、Failedは関連付けの失敗を表します。
Reason	クライアントの関連付けまたは切断イベントの理由コード。probe viewで display system internal wlan client history-record help reason-code コマンドを実行すると、理由コードの説明が表示されます。

3.1.22 display wlan client online-duration

🕮 メモ：

display wlan client online-duration コマンドは、ソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan client online-duration [**ap** *ap-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*: 1～64 文字で AP 名を指定します。大文字と小文字は区別されます。文字列には英字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）スラッシュ（/）、ハイフン(-)を使用できます。

説明

display wlan client online-duration コマンドはクライアントのオンライン時間の情報を表示します。

例

クライアントのオンライン時間情報を表示します。

<AC> display wlan client online-duration

```
Total number of online clients: 1

MAC address     IPv4 address     Online duration
abcd-ef13-f4a3  192.168.6.64     0days 0hours 0minutes 24seconds
```

表 3-9 コマンド出力

フィールド	説明
MAC address	クライアントのMACアドレス
IPv4 address	クライアントのIPv4アドレス
Online duration	クライアントのオンライン時間

3.1.23 display wlan client status

Syntax

display wlan client status [**mac-address** *mac-address*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address *mac-address*: クライアントの MAC アドレスを H-H-H の形式で指定します。このオプションを指定しないと、すべてのクライアントに関するステータス情報が表示されます。

verbose: 詳細なクライアントのステータス情報を表示します。このキーワードを指定しない場合、コマンドはクライアント状況情報の概要を表示します。

説明

display wlan client status コマンドはクライアントステータス情報を表示します。

例

指定したクライアントに関する簡易的なステータス情報を表示します。

<AC> display wlan client status mac-address 001c-f08f-f804

```
Total number of clients: 1

MAC address    RSSI Rx/Tx(bps)    Speed(bps)     Discard AP name      RID
001c-f08f-f804 45   2.4G/6M       0.1K/0.2K      0.00%   ap1          1#
```

すべてのクライアントの概要状況を表示します。

<AC> display wlan client status

```
Total number of clients: 2

MAC address    RSSI   Rx/Tx(bps)    Speed(bps)     Discard AP name      RID
001c-f08f-f804 45     2.4G/6M       0.1K/0.2K      0.00%   ap1          1
```

表 3-10 000f-e265-6401 35 2.4G/6M 0.1K/0.2K 0.00% ap1 2 コマンド出力

フィールド	説明
MAC address	クライアントMACアドレス。
RSSI	クライアントのRSSI
Rx/Tx rate	データ、管理、制御フレームの送信および受信レート
Speed(bps)	過去2分間の送受信レートの表示(Kbps単位)。小数点以下3桁で四捨五入。 N/A：送信レートと受信レートの両方が0の場合。
Discard	クライアントに廃棄されるパケットの割合
AP name	クライアントが紐付いたAPの名前
RID	クライアントが紐付いた無線のID

特定のクライアントの詳細な状況を表示します。

<AC> display wlan client status mac-address 001c-f08f-f804 verbose

```
Total number of clients: 1

MAC address                    : 001c-f08f-f804
AP name                        : ap2
Radio ID                       : 2
Access time                    : 41 ms
RSSI                           : 0
Rx/Tx rate                     : 39/117 Mbps
Speed                          : 0.003/0.000Kbps
Received:
 Retransmitted packets         : 84
 Retransmitted packet ratio    : 64.12%
Sent:
 Retransmitted packets         : 0
 Retransmitted packet ratio    : 0.00%
Discarded:
 Discarded packets             : 0
 Discarded packet ratio        : 0.00%
```

表 3-11 コマンド出力

フィールド	説明
MAC address	クライアントMACアドレス。
AP name	クライアントが紐付いたAPの名前
Radio ID	クライアントが紐付いた無線のID
Access time	クライアントがWLANに紐付く時間
RSSI	クライアントのRSSI
Rx/Tx rate	クライアントがデータ、管理パケット、制御パケットを送受信する速度
Speed(bps)	過去2分間の送受信レートの表示(Kbps単位)。小数点以下3桁で四捨五入。 N/A：送信レートと受信レートの両方が0の場合。
Received	受信パケット統計情報 ● 再伝送パケット ● 再伝送パケット比率
Sent	送信パケット統計情報 ● 再伝送パケット ● 再伝送パケット比率
Discarded	廃棄パケット統計情報 ● 廃棄パケット ● 廃棄パケット比率

3.1.24 display wlan region-code ap (v7.1.13 以前のみ)

Syntax

display wlan region-code ap { **all** | **name** *ap-name* }

View

すべての view

定義済みユーザロール

network-admin

パラメータ

all: 全ての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別しない 1～64 文字の文字列です。

説明

display wlan region-code ap コマンドはすべての AP または指定した AP の地域コード情報を表示します。

例

すべての AP の地域コード情報を表示します。

<AC> display wlan region-code ap all

```
Region Code
--------------------------------------------------------------------------
AP name              Region Code
ap1                  JP  JAPAN
ap2                  JP  JAPAN
ap3                  JP  JAPAN
```

表 3-12 コマンド出力

フィールド	説明
Region Code	地域コード。 地域コードの詳細については、表 3-16を参照してください。

3.1.25 display wlan service-template

Syntax

display wlan service-template [*service-template-name*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

service-template-name: サービステンプレート名を指定します。サービステンプレート名は、1～63 文字の文字列です。大文字と小文字を区別しません。この引数を指定しない場合は、すべてのサービステンプレートに関する情報が表示されます。

verbose: 詳細なサービステンプレート情報を表示します。

説明

display wlan service-template コマンドはサービステンプレート情報を表示します。

例

すべてのサービステンプレートに関する簡易情報を表示します。

<AC> display wlan service-template

```
Total number of service templates: 2
Service template name     SSID              Status
1                         2333              Enabled
2                         3222              Enabled
```

すべてのサービステンプレートに関する詳細情報を表示します。

<AC> display wlan service-template verbose

```
Service template name        : service1
Description                 : Not configured
SSID                       : wuxianfuwu
SSID-hide                   : Disabled
User-isolation              : Disabled
Service template status      : Disabled
Maximum clients per BSS      : 64
Frame format                : Dot3
Seamless roam status         : Disabled
Seamless roam RSSI threshold  : 0
Seamless roam RSSI gap       : 0
VLAN ID                    : 1
AKM mode                   : PSK
Security IE                 : RSN
Cipher suite                : CCMP
TKIP countermeasure time     : 100 sec
PTK lifetime                : 43200 sec
GTK rekey                  : Enabled
GTK rekey method            : Time-based
GTK rekey time              : 86400 sec
GTK rekey client-offline     : Enabled
User authentication mode     : Bypass
Intrusion protection         : Disabled
Intrusion protection mode    : Temporary-block
Temporary block time         : 180 sec
Temporary service stop time   : 20 sec
Fail VLAN ID               : 1
802.1X handshake            : Enabled
802.1X handshake secure      : Disabled
```

```
802.1X domain              : my-domain
MAC-auth domain            : Not configured
Max 802.1X users per BSS     : 4096
Max MAC-auth users per BSS   : 4096
802.1X re-authenticate       : Enabled
Authorization fail mode      : Online
Accounting fail mode         : Online
Authorization              : Permitted
Key derivation             : SHA1
PMF status                 : Optional
Hotspot policy number        : Not configured
Forwarding policy status     : Disabled
Forward policy name          : Not configured
Forwarder                  : AC
FT status                  : Enabled
QoS trust                  : Port
QoS priority               : 0
```

表 3-13 コマンド出力

フィールド	説明
SSID	サービステンプレートのSSID
SSID-hide	SSIDステルス ● Disabled. ● Enabled.
User-isolation	ユーザ分離 ● Disabled. ● Enabled.
Service template status	サービステンプレート 状態 ● Disabled. ● Enabled.
Maximum clients per BSS	BSSがサポートするクライアントの最大数。
Frame format	クライアントデータフレームのカプセル化フォーマット： ● **Dot3**–802.3フォーマット. ● **Dot11**–802.11フォーマット.
Seamless roam status	シームレスなローミング： ● Disabled. ● Enabled. 現在のリリースでは、このフィールドはサポートされていません。

フィールド	説明
Seamless roam RSSI threshold	シームレスなローミングRSSIしきい値。 現在のリリースでは、このフィールドはサポートされていません。
Seamless roam RSSI gap	シームレスなローミングRSSIギャップ。 現在のリリースでは、このフィールドはサポートされていません。
VLAN ID	クライアントがサービステンプレートを使用してオンラインになった後に属しているVLANのID。
AKM mode	AKM モード,802.1XまたはPSK.
Security IE	Security IE ● RSN. ● WPA.
Cipher suite	暗号方式 ● WEP40. ● WEP104. ● WEP128. ● TKIP. ● CCMP.
TKIP countermeasure time	TKIP対策時間。 設定値0は、対策が取られていないことを表します。
GTK rekey	GTK rekeyが有効/無効： ● Enabled. ● Disabled.
GTK rekey method	GTK rekey方式。時間ベースまたはパケットベース
GTK rekey time	GTK rekey間隔.
GTK rekey packets	GTKをリフレッシュする前に送信できるパケット数。
GTK rekey client-offline	client-off GTK rekeyが有効/無効： ● Enabled. ● Disabled.
User authentication mode	認証モード: ● **Bypass**–認証なし。 ● **MAC**. ● **MAC-or-802.1X**. ● **802.1X**. ● **802.1X-or-MAC**.

フィールド	説明
	• **OUI-or-802.1X**.
Intrusion protection	client-off GTK rekeyが有効/無効： • Enabled. • Disabled.
Intrusion protection mode	侵入防止モード： • **Temporary-block**－ブロックリストに侵入者を一時的に追加します。 • **Service-stop**－リセットされるまで、不正なパケットを受信するBSSによって提供されるすべてのサービスを停止します。 • **Temporary-service-stop**－不正なパケットを受信したBSSが提供するアクセスサービスを一時的に停止します。
Temporary block time	一時的なブロック時間（秒）。
Temporary service stop time	一時的なサービス停止時間（秒）。
Fail VLAN ID	認証サーバが正常で認証に合格できない場合に、クライアントが追加されるVLANのID。未設定の場合“**Not configured**”が表示されます。
Critical VLAN ID	認証サーバが異常で認証に合格できない場合に、クライアントが追加されるVLANのID。未設定の場合“**Not configured**”が表示されます。
802.1X handshake	802.1Xハンドシェークが有効/無効： • Enabled. • Disabled.
802.1X handshake secure	セキュア802.1Xハンドシェークが有効/無効： • Enabled. • Disabled.
802.1X domain	802.1X認証ドメイン。未設定の場合“**Not configured**”が表示されます。
MAC-auth domain	MAC認証ドメイン。未設定の場合“**Not configured**”が表示されます。
Max 802.1X users per BSS	BSSでサポートされている802.1Xユーザの最大数
Max MAC-auth users per BSS	BSSでMAC認証に合格するサポートされるユーザの最大数。
802.1X re-authenticate	802.1X再認証が有効/無効： • Enabled. • Disabled.

フィールド	説明
Authorization fail mode	許可失敗モード ● **Offline**－認証に失敗すると、クライアントはログオフされます。 ● **Online**－認証に失敗しても、クライアントはログオフされません。
Accounting fail mode	アカウンティング失敗モード ● **Offline**－アカウンティングに失敗すると、クライアントはログオフされます。 ● **Online**－アカウンティングに失敗しても、クライアントはログオフされません。
Authorization	許可情報： ● **Permitted**－RADIUSサーバまたはローカルデバイスによって発行された許可情報を適用します。 ● **Ignored**－RADIUSサーバまたはローカルデバイスによって発行された認証情報を無視します。
Key derivation	キーの導出タイプ ● **SHA1**－HMAC-SHA1 hash algorithm使用 ● **SHA256**－HMAC-SHA256 hash algorithm使用 ● **SHA1-AND-SHA256**－HMAC SHA1 and SHA256 hash algorithm使用
PMF status	PMF状態 ● **Disabled**－管理フレームの保護が無効になっています。 ● **Optional**－オプションモードでの管理フレーム保護が有効になっています。 ● **Mandatory**－必須モードの管理フレーム保護が有効になっています。
Forwarding policy status	WLANフォワーディングポリシstatus ● Disabled. ● Enabled.
Forwarding policy name	WLANフォワーディングポリシ名 ● **Not configured**－設定なし ● *policy name*.
Forwarder	クライアントトラフィックフォワーダ ● AC. ● AP.

フィールド	説明
FT status	FT状態 ● Disabled. ● Enabled.
QoS trust	QoSプライオリティトラストモード : ● **Port**－Portプライオリティトラストモード ● **Dot11e**－802.11eプライオリティトラストモード
QoS priority	ポートプライオリティ。設定範囲は0～7です。

3.1.26 display wlan statistics (v7.1.13 以前のみ)

Syntax

display wlan statistics { **ap** { **all** | **name** *ap-name* } **connect-history** | **client** [**mac-address** *mac-address*] | **service-template** *service-template-name* [**connect-history**] }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap: AP を指定します。

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別しない 1～64 文字の文字列です。

connect-history: 接続履歴を表示します。

client: クライアント統計を指定します。

mac-address *mac-address*: クライアントを MAC アドレスで指定します。このオプションを指定しない場合、すべてのクライアントの統計が表示されます。

service-template *service-template-name*: サービステンプレートを名前で指定します。**connect-history** キーワードも指定すると、指定したサービステンプレートの接続履歴が表示されます。

説明

display wlan statistics コマンドはクライアント統計情報またはサービステンプレート統計情報を表示します。

例

すべてのクライアントの統計情報を表示します。

<AC> display wlan statistics client

```
MAC address              : 0014-6c8a-43ff
AP name                  : ap1
Radio ID                 : 1
SSID                     : office
BSSID                    : 000f-e2ff-7700
RSSI                     : 31
Sent frames:
  Back ground            : 0/0 (frames/bytes)
  Best effort            : 9/1230 (frames/bytes)
  Video                  : 0/0 (frames/bytes)
  Voice                  : 2/76 (frames/bytes)
Received frames:
  Back ground            : 0/0 (frames/bytes)
  Best effort            : 18/2437 (frames/bytes)
  Video                  : 0/0 (frames/bytes)
  Voice                  : 7/468 (frames/bytes)
Discarded frames:
  Back ground            : 0/0 (frames/bytes)
  Best effort            : 0/0 (frames/bytes)
  Video                  : 0/0 (frames/bytes)
  Voice                  : 5/389 (frames/bytes)
```

表 3-14 コマンド出力

フィールド	説明
SSID	サービステンプレートのSSID
MAC address	クライアントのMACアドレス
Back ground	AC-BK queue.
Best effort	AC-BE queue.
Video	AC-VI queue.
Voice	AC-VO queue.

サービステンプレート 1 の統計情報を表示します。

<AC> display wlan statistics service-template 1

```
AP name                    : ap1
Radio ID                   : 1
Received:
  Frame count              : 1713
  Frame bytes              : 487061
  Data frame count          : 1683
  Data frame bytes          : 485761
  Association request count   : 2
Sent:
  Frame count              : 62113
  Frame bytes              : 25142076
  Data frame count          : 55978
  Data frame bytes          : 22626600
  Association response count  : 2
```

サービステンプレート 1 の接続履歴を表示します。

<AC> display wlan statistics service-template 1 connect-history

```
AP name                  : ap1
Radio ID                 : 1
Associations              : 132
Association failures       : 3
Reassociations            : 30
Rejections               : 12
Exceptional deassociations  : 2
Current associations       : 57

AP name                  : ap1
Radio ID                 : 2
Associations              : 1004
Association failures       : 35
Reassociations            : 59
Rejections               : 4
Exceptional deassociations  : 22
Current associations       : 300
```

AP ap1 の接続履歴を表示します。

<AC> display wlan statistics ap name ap1 connect-history

```
AP name                    : ap1
Associations                : 1
Reassociations              : 0
```

```
Failures                  : 0
Rejections                : 0
Exceptional deassociations   : 0
Current associations       : 1
```

3.1.27 display wlan statistics client

🕮 メモ：

display wlan statistics client コマンドは、ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan statistics client [**mac-address** *mac-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address *mac-address*: クライアントを MAC アドレスで指定します。このオプションを指定しない場合、すべてのクライアントの統計が表示されます。

説明

display wlan statistics client コマンドはクライアントの統計情報を表示します。

例

すべてのクライアントの統計情報を表示します。

<AP> display wlan statistics client

```
MAC address             : 0014-6c8a-43ff
AP name                 : ap1
Radio ID                : 1
SSID                    : office
BSSID                   : 000f-e2ff-7700
RSSI                    : 31
Sent frames:
  Back ground           : 0/0 (frames/bytes)
  Best effort           : 9/1230 (frames/bytes)
```

```
  Video                : 0/0 (frames/bytes)
  Voice                : 2/76 (frames/bytes)
Received frames:
  Back ground           : 0/0 (frames/bytes)
  Best effort           : 18/2437 (frames/bytes)
  Video                : 0/0 (frames/bytes)
  Voice                : 7/468 (frames/bytes)
Discarded frames:
  Back ground           : 0/0 (frames/bytes)
  Best effort           : 0/0 (frames/bytes)
  Video                : 0/0 (frames/bytes)
  Voice                : 5/389 (frames/bytes)
```

表 3-15 コマンド出力

フィールド	説明
SSID	サービステンプレートのSSID
MAC address	クライアントのMACアドレス
Back ground	AC-BK queue.
Best effort	AC-BE queue.
Video	AC-VI queue.
Voice	AC-VO queue.

3.1.28 display wlan statistics connect-history

🕮 メモ：

display wlan statistics connect-history コマンドは、ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan statistics connect-history { **ap** { **all** | **name** *ap-name* } | **service-template** *service-template-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap all: すべての AP のクライアント接続履歴を表示します。

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

service-template *service-template-name*: サービステンプレートを名前で指定します。

説明

display wlan statistics connect-history コマンドはクライアントの接続履歴を表示します。

例

#AP ap1 の接続履歴を表示します。

<AP> display wlan statistics connect-history ap name ap1

```
AP name                 : ap1
Radio ID                : 1
Associations             : 132
Association failures       : 3
Reassociations            : 30
Rejections               : 12
Abnormal disassociations    : 2
Current associations       : 57

AP name                 : ap1
Radio ID                : 2
Associations             : 1004
Association failures       : 35
Reassociations            : 59
Rejections               : 4
Abnormal disassociations    : 22
Current associations       : 300
```

サービステンプレート 1 の接続履歴を表示します。

<AP> display wlan statistics connect-history service-template 1

```
AP name                 : ap1
Radio ID                : 1
Associations             : 132
Association failures       : 3
```

```
Reassociations            : 30
Rejections               : 12
Abnormal disassociations   : 2
Current associations       : 57

AP name                  : ap1
Radio ID                 : 2
Associations              : 1004
Association failures       : 35
Reassociations            : 59
Rejections               : 4
Abnormal disassociations   : 22
Current associations       : 300
```

3.1.29 display wlan statistics service-template

🕮 メモ：

display wlan statistics service-template コマンドは、ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan statistics service-template *service-template-name*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

service-template *service-template-name*: サービステンプレートを名前で指定します。

説明

display wlan statistics service-template コマンドはサービステンプレートの統計情報を表示します。

例

サービステンプレート 1 の統計情報を表示します。

<AP> display wlan statistics service-template 1

```
AP name                    : ap1
Radio ID                   : 1
Received:
  Frame count              : 1713
  Frame bytes              : 487061
  Data frame count          : 1683
  Data frame bytes          : 485761
  Association request count   : 2
Sent:
  Frame count              : 62113
  Frame bytes              : 25142076
  Data frame count          : 55978
  Data frame bytes          : 22626600
  Association response count  : 2
```

3.1.30 display wlan whitelist

Syntax

display wlan whitelist

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan whitelist コマンドはホワイトリストエントリを表示します。

例

#ホワイトリストエントリを表示します。

<AC> display wlan whitelist

```
Total number of clients: 3
 MAC addresses:
  000e-35b2-000e
  0019-5b8e-b709
  001c-f0bf-9c92
```

3.1.31 dot11ax support maximum-he-mcs

🕮 メモ：

dot11ax support maximum-he-mcs コマンドはソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

dot11ax support maximum-he-mcs *he-mcs-number*

undo dot11ax support maximum-he-mcs

デフォルト

設定無し

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

he-mcs-number: 802.11 ax でサポートされる HE-MCS の最大値を指定します。使用可能なオプションは 7、9、11 です。

説明

dot11ax support maximum-he-mc コマンドは 802.11 ax でサポートされる HE-MCS の最大値を設定します。

undo dot11ax support maximum-he-mcs コマンドはデフォルトに戻します。

802.11 ax ネットワークでは、ネットワークの品質が悪い場合、ネットワークデバイスが中程度または低レートで通信するために、802.11 ax でサポートされる HE-MCS の最大値を減らすことができます。これにより、高速レートと低速レートの間で頻繁にレートが変更されることによる通信遅延やジッターを回避できます。

指定した HE-MCS が無線のサポートされている最大レートよりも高い場合は、無線のサポートされているレートが使用されます。

この機能は、802.11 ax 無線でのみ有効です。

例

802.11ax でサポートされる HE-MCS の最大値を 7 に設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] dot11ax support maximum-he-mcs 7

3.1.32 inherit exclude service-template

Syntax

inherit exclude service-template *service-template-name*

undo inherit exclude service-template *service-template-name*

デフォルト

AP は、AP グループにバインドされたサービステンプレートを継承します。

View

Radio view

定義済みユーザロール

network-admin

パラメータ

service-template-name: サービステンプレート名を指定します。サービステンプレート名は、1～63 文字の文字列です。大文字と小文字を区別しません。

説明

inherit exclude service-template コマンドは AP グループから指定されたサービステンプレートを継承しないように AP を設定します。

undo inherit exclude service-template コマンドはデフォルトに戻します。

例

AP ap1 を AP グループからサービステンプレート st を継承しないように設定します。

<AC> system-view

[AC] wlan ap ap1

[AC-ap-ap1] radio 1

[AC-ap-ap1-radio-1] inherit exclude service-template st

3.1.33 map-configuration

🕮 **メモ：**

AP の設定には **remote-configuration** を使用することを推奨します。
remote-configuration で設定できないコマンドを設定したい場合に限り、**map-configuration** の併用をご検討ください。なお、**remote-configuration** を有効にした場合、**remote-configuration** で設定可能なコマンドがデフォルト値として適用されます。**remote-configuration** と **map-configuration** の両方に同じ機能を有するコマンド設定がある場合、AP へのコンフィグ適用が正常におこなわれません。

Syntax

map-configuration *filename*

undo map-configuration

デフォルト

コンフィグレーションファイルなし

View

AP view

AP group AP model view

定義済みユーザロール

network-admin

パラメータ

filename: コンフィグレーションファイル名を指定します。コンフィグレーションファイル名は、1～63 文字の文字列です。大文字と小文字を区別しません。コンフィグレーションファイルが AC の記憶媒体に保管されていることを確認してください。

説明

map-configuration コマンドはコンフィグレーションファイルを AP に展開します。

undo map-configuration コマンドはデフォルトに戻します。

コンフィグレーションファイルは完全なコマンドでなければなりません。

コンフィグレーションファイルは、AC への CAPWAP トンネルが実行状態にあるときに有効になります。AP の再起動後も存続しません。

AP がコンフィグレーションファイルを使用する設定の場合、AP 自身の設定は、AC への CAPWAP トンネルを確立するためにメイン IP アドレスのみを使用します。

例

#コンフィグレーションファイル downconfig.txt を AP ap1 に配置します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] map-configuration downconfig.txt

#コンフィグレーションファイル downconfig.txt を AP グループ apgroup1 のモデル QX-W1020 を持つ AP に配置します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] map-configuration downconfig.txt

3.1.34 nas-id

Syntax

nas-id *nas-id*

undo nas-id

デフォルト

AP view：AP group view の設定を使用します。

AP group view：global configuration view の設定を使用します。

global configuration view：設定なし

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

nas-id: NAS ID を指定します。NAS ID は、1～63 文字の文字列です。大文字と小文字を区別します。

説明

nas-id コマンドはネットワークアクセスサーバ識別子（NAS ID）を設定します。

オンライン後、クライアントは、NAS ID を持つ RADIUS 要求を RADIUS サーバに送信して、ネットワークアクセスサーバを指定します。

装置は、次の優先順位で NAS-ID を選択します。

1.サービステンプレートを無線にバインドする時に指定した NAS-ID パラメータ

2.AP View の設定

3. AP group View の設定

4. wlan global-configuration View の設定

5. ISP ドメイン View の設定

NAS-ID が設定されていない場合、装置はデバイス名を NAS-ID として使用します。

例

AP ap1 に NAS ID abc123 を設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] nas-id abc123

AP group group1 に NAS ID abc123 を設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] nas-id abc123

グローバル NAS ID に abc123 を設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] nas-id abc123

3.1.35 nas-port-id

Syntax

nas-port-id *nas-port-id*

undo nas-port-id

デフォルト

AP view：AP group view の設定を使用します。

AP group view：global configuration view の設定を使用します。

global configuration view：設定なし

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

nas-port-id: NAS port ID を指定します。NAS port ID は、1～63 文字の文字列です。大文字と小文字を区別します。

説明

nas-port-id コマンドはネットワークアクセスサーバのポート識別子（NAS ポート ID）を設定します。

undo nas-port-id コマンドはデフォルトに戻します。

オンライン後、クライアントは、NAS port ID を持つ RADIUS 要求を RADIUS サーバに送信して、ネットワークアクセスサーバを指定します。

サービステンプレートを無線にバインドするときに NAS port ID を設定します。NAS port ID は、AP view、AP group view、global configuration view に設定できます。これらの設定の優先順位は降順です。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 に NAS port ID abcd1234 を設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] nas-port-id abcd1234

AP group group1 に NAS port ID abcd1234 を設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] nas-port-id abcd1234

グローバル NAS port ID に abcd1234 を設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] nas-port-id abcd1234

3.1.36 nas-vlan

Syntax

nas-vlan *vlan-id*

undo nas-vlan

デフォルト

NAS VLAN ID が設定されていません。RADIUS サーバに送信された認証要求に NAS VLAN ID フィールドが含まれていません。

View

AP view

定義済みユーザロール

network-admin

パラメータ

vlan-id: NAS VLAN ID を 1～4096 の範囲で指定します。

説明

nas-vlan コマンドはネットワークアクセスサーバ VLAN 識別子（NAS VLAN ID）を設定し、VLAN ID を RADIUS 要求にカプセル化する AC を有効にします。

undo nas-vlan コマンドはデフォルトに戻します。

NAS VLAN ID が設定されると、AC はクライアントのネットワークアクセスサーバを示すために RADIUS サーバに送信される RADIUS 要求に VLAN ID をカプセル化します。

サードパーティのセキュリティアカウンティング管理（SAM）サーバを RADIUS サーバとして使用する場合は、NAS VLAN ID を設定します。

例

AP **ap1** の NAS VLAN ID を **1234** に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] nas-vlan 1234

3.1.37 quick-association enable

Syntax

quick-association enable

undo quick-association enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

quick-association enable コマンドはクイックアソシエーションを有効にします。

undo quick-association enable コマンドはデフォルトに戻します。

このコマンドは、AP が指定されたサービステンプレートに関連付けられたクライアント上でロードバランシングまたはバンドナビゲーションを実行できないようにします。

例

サービステンプレート **service1** の quick association を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] quick-association enable

3.1.38 region-code

Syntax

region-code *code*

undo region-code

デフォルト

AP view：AP group view の設定を使用します。

AP group view：global configuration view の設定を使用します。

global configuration view：JP

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

code: 地域コードを指定します。 地域コードの詳細については、表 3-16 を参照してください。

表 3-16 地域コード一覧

国	地域コード	国	地域コード
Japan	JP	South Africa	ZA

説明

region-code コマンドは地域コードを指定します。

undo region-code コマンドはデフォルトに戻します。

地域コードは、利用可能な周波数、利用可能なチャネル、および送信電力レベルなどの特性を決定します。

AP view、AP group view、および Global configuration view での設定の優先順位は降順です。

例

AP ap1 の地域コードを JP に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] region-code JP

AP group group1.の地域コードを JP に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] region-code JP

グローバル地域コードを JP に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] region-code JP

関連コマンド

region-code-lock

3.1.39 region-code-lock

Syntax

region-code-lock { **disable** | **enable** }

undo region-code-lock

デフォルト

AP view：AP group view の設定を継承します。

AP group view：global configuration view の設定を継承します。

global configuration view：ロックしません。

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

disable: 地域コードのロックを解除します。

enable: 地域コードをロックします。

説明

region-code-lock enable コマンドは地域コードをロックします。

region-code-lock disable コマンドは地域コードのロックを解除します。

undo region-code-lock コマンドはデフォルトに戻します。

ロックされると地域コードは変更できません。

AP view に地域コードを設定していない場合、AP view で地域コードをロックしても、AP は AP group view または AP group view に設定された地域コードを使用します。AP group view に地域コードが設定していない場合、AP group view で地域コードをロックしても、AP はグローバル地域コードを使用します。

AP view、AP group view、および Global configuration view での設定の優先順位は降順です。

例

AP ap1 の地域コードをロックします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] region-code-lock enable

AP group group1.の地域コードをロックします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] region-code-lock enable

#グローバル地域コードをロックします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] region-code-lock enable

関連コマンド

region-code

3.1.40 reset wlan client

Syntax

reset wlan client { **all** | **mac-address** *mac-address* }

View

User view

定義済みユーザロール

network-admin

パラメータ

mac-address *mac-address*: MAC アドレスでクライアントを指定します。

all: すべてのクライアントを指定します。

説明

reset wlan client コマンドはクライアントまたはすべてのクライアントからログオフします。

例

#すべてのクライアントをログオフします。

<AC> reset wlan client all

関連コマンド

display wlan client

3.1.41 reset wlan dynamic-blacklist

Syntax

reset wlan dynamic-blacklist [**mac-address** *mac-address*]

View

User view

定義済みユーザロール

network-admin

パラメータ

mac-address *mac-address*: MAC アドレスでクライアントを指定します。このオプションを指定しないと、このコマンドはダイナミックブラックリストからすべてのクライアントを削除します。

説明

reset wlan dynamic-blacklist コマンドは指定したクライアントまたはすべてのクライアントをダイナミックブラックリストから削除します。

例

ダイナミックブラックリストからすべてのクライアントを削除します。

<AC> reset wlan dynamic-blacklist

ダイナミックブラックリストから指定したクライアントを削除します。

<AC> reset wlan dynamic-blacklist mac-address b8ca-32a2-df69

関連コマンド

display wlan blacklist

3.1.42 reset wlan statistics client

Syntax

reset wlan statistics client { **all** | **mac-address** *mac-address* }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべてのクライアントを指定します。

mac-address *mac-address*: クライアントを MAC アドレスで指定します。

説明

reset wlan statistics client コマンドはクライアントの統計情報を削除します。

例

すべてのクライアントの統計情報を削除します。

<AC> reset wlan statistics client all

関連コマンド

display wlan statistics

3.1.43 reset wlan statistics service-template

Syntax

reset wlan statistics service-template { **service-template** *service-template-name* }

View

User view

定義済みユーザロール

network-admin

パラメータ

service-template *service-template-name*: サービステンプレートを名前で指定します。

説明

reset wlan statistics service-template コマンドはサービステンプレートの統計情報を削除します。

例

サービステンプレート service1 の統計情報を削除します。

<AP> reset wlan statistics service-template service 1

関連コマンド

display wlan statistics service-template

3.1.44 service-template

Syntax

service-template *service-template-name* [**nas-id** *nas-id* | **nas-port-id** *nas-port-id*] [**ssid-hide**] [**vlan** *vlan-id*]

undo service-template *service-template-name*

デフォルト

radio view：AP group radio view の設定を使用します。

AP group radio view：設定なし

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

service-template-name: サービステンプレート名を指定します。サービステンプレート名は、1～63 文字の文字列です。大文字と小文字を区別しません。

nas-id *nas-id*: NAS ID を指定します。NAS ID は、1～63 文字のスペースを含まない文字列です。大文字と小文字を区別しません。

nas-port-id *nas-port-id*: NAS port ID を指定します。NAS port ID は、1～63 文字のスペースを含まない文字列です。大文字と小文字を区別しません。

ssid-hide: ビーコンフレームで SSID を非表示にします。

vlan *vlan-id*: VLAN ID によって無線にバインドされる VLAN を指定します。範囲は 1～4094 です。このオプションを指定しない場合、無線はサービステンプレートにバインドされた VLAN を使用します。指定された VLAN が存在しない場合、このコマンドはクライアントがオンラインになったときに VLAN を作成します。

説明

service-template コマンドはサービステンプレートを無線インタフェースまたは無線インタフェースにバインドします。

undo service-template コマンドは無線または無線インタフェースからサービステンプレートをバインド解除します。

サービステンプレートは、無線または無線インタフェースにバインドする前に作成する必要があります。

このコマンドを使用して設定された VLAN ID は、サービステンプレート用に設定された VLAN ID よりも優先されます。

AP view の設定は、AP group view の設定よりも優先されます。

例

サービステンプレート service1 と VLAN group vg1 を radio 1 にバインドします。

<AC> system-view

[AC] wlan ap ap1

[AC-ap-ap1] radio 1

[AC-ap-ap1-radio-1] service-template service1 vlan 10

サービステンプレート service1 と VLAN 10 を AP group apgroup1 の radio 1 にバインドします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] service-template service1 vlan 10

3.1.45 service-template enable

Syntax

service-template enable

undo service-template enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

service-template enable コマンドはサービステンプレートを有効にします。

undo service-template enable コマンドはサービステンプレートを無効にします。

AC 上の BSS（basic service set）の数が制限を超える場合、新しいサービステンプレートを有効にできません。

例

サービステンプレート service1 を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] service-template enable

3.1.46 snmp-agent trap enable wlan client

Syntax

snmp-agent trap enable wlan client

undo snmp-agent trap enable wlan client

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan client コマンドは WLAN アクセスの SNMP 通知を有効にします。

undo snmp-agent trap enable wlan client コマンドはデフォルトに戻します。

この機能を有効にすると、クライアントのステータスが変更されるたびに、装置は NMS にクライアントステータス変更通知を送信します。通知を正しく送信するには、オペレーションマニュアルのセクション 11 *システム管理 "Information Center"* の説明に従って SNMP を設定する必要があります。

例

#WLAN アクセスに対して SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan client

3.1.47 snmp-agent trap enable wlan client-audit

Syntax

snmp-agent trap enable wlan client-audit

undo snmp-agent trap enable wlan client-audit

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan client-audit コマンドはクライアント監査の SNMP 通知を有効にします。

undo snmp-agent trap enable wlan client-audit コマンドはクライアント監査の SNMP 通知を無効にします。

この機能を有効にすると、クライアントがオンラインになったり、オフラインになったり、別の AP にローミングしたり、IP アドレスを取得した場合、装置は NMS にクライアントステータス変更通知を送信します。通知を正しく送信するには、オペレーションマニュアルのセクション 11 *システム管理 “Information Center”* の説明に従って SNMP を設定する必要があります。

例

クライアント監査の SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan client-audit

3.1.48 ssid

Syntax

ssid *ssid-name*

undo ssid

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

ssid-name: SSID 名を 1～32 文字の文字列で指定します。SSID 名には、大文字、小文字、数字、特殊文字が使用可能です。大文字と小文字は区別されます。特殊文字については 表 3-17 を参照してください。

表 3-17 使用可能な特殊文字

名称	文字	名称	文字
Tilde	~	Left angle bracket	<
Exclamation point	!	Right angle bracket	>
At sign	@	Hyphen	-
Pound sign	#	Underscore	_
Dollar sign	$	Plus sign	+
Percent sign	%	Equal sign	=
Caret	^	Vertical bar	|
Ampersand sign	&	Backslash	¥
Asterisk	*	Colon	:
Left brace	{	Semi-colon	;
Right brace	}	Quotation marks	"
Left parenthesis	(	Apostrophe	'
Right parenthesis	)	Comma	,
Left bracket	[	Dot	.
Right bracket	]	Slash	/

説明

ssid コマンドはサービステンプレートの SSID を設定します。

undo ssid コマンドはサービステンプレートの SSID を削除します。

このコマンドを実行する前に、サービステンプレートを無効にしてください。

QX では、サービステンプレートに個別の SSID を設定することを推奨します。

例

サービステンプレート service1 に SSID lynn を設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] ssid lynn

3.1.49 unknown-client

Syntax

unknown-client { **deauthenticate** | **drop** }

undo unknown-client

デフォルト

AP は未知のクライアントからのパケットを廃棄し、未知のクライアントの認証を解除します。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

deauthenticate: 未知のクライアントからのパケットを廃棄し、未知のクライアントの認証を解除します。

drop: 未知のクライアントからのパケットを廃棄します。

説明

unknown-client コマンドは AP が未知のクライアントからのトラフィックを処理する方法を設定します。

undo unknown-client コマンドはデフォルトに戻します。

例

AP ap1 サービステンプレート example に未知のクライアントからのパケットを廃棄するが、未知のクライアントの認証は解除しない設定をします。

<AC> system-view

[AC] wlan service-template example

[AC -wlan-st-example] unknown-client drop

3.1.50 user-profile

Syntax

user-profile *profile-name*

undo user-profile *profile-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

profile-name: ユーザプロファイル名を指定します。設定範囲は 1 から 31 文字です。大文字と小文字を区別します。英字、数字、アンダースコア (_) を使用でき、英字で始まる必要があります。名前は一意である必要があります。

説明

user-profile コマンドはユーザプロファイルを作成し、その view に移行するか、既存のユーザプロファイルの view に移行します。

undo user-profile コマンドはユーザプロファイルを削除します。

例

#ユーザプロファイル a123 を作成し、a123 の View に移行します。

<AC> system view

[AC] user-profile name a123

[AC-user-profile-a123]

3.1.51 vlan

Syntax

vlan *vlan-id*

undo vlan

デフォルト

サービステンプレートを使用してオンラインになった後、クライアントは VLAN 1 に割り当てられます。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN を VLAN ID で指定します。VLAN ID の設定範囲は 1～4094 です。指定した VLAN が存在しない場合、このコマンドは、クライアントがオンラインになったときに VLAN を作成します

説明

vlan コマンドはサービステンプレートを使用してオンラインになっているクライアントを VLAN に割り当てます。

undo vlan コマンドはデフォルトに戻します。

このコマンドを実行する前に、サービステンプレートを無効にしてください。

例

サービステンプレート **service1** を介してオンラインになっているクライアントを VLAN 2 に割り当てます。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] vlan 2

3.1.52 wlan client failure history aging

🕮 メモ：

wlan client failure history aging コマンドは、ソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

wlan client failure history aging *time*

undo wlan client failure history aging

デフォルト

72 時間

View

System view

定義済みユーザロール

network-admin

パラメータ

time: クライアントの接続失敗情報を記憶する時間を指定します。設定範囲は 1～720 時間です。

説明

wlan client failure history aging コマンドはクライアントの接続失敗情報を記憶する時間を設定します。

undo wlan client failure history aging コマンドはデフォルト設定に戻します。

例

クライアントの接続失敗情報を記憶する時間を 720 時間に設定します。

<AC> system-view

[AC] wlan client failure history aging 720

3.1.53 wlan client forwarding enable

Syntax

wlan client forwarding enable

undo wlan client forwarding enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

wlan client forwarding enable コマンドはクライアントトラフィックの転送を有効にします。

undo wlan client forwarding enable コマンドはクライアントトラフィックの転送を無効にします。

クライアントトラフィックフォワーダとして AC を設定する場合は、この機能を有効にする必要があります。

例

クライアントトラフィック転送を無効にします。

<AC> system-view

[AC] undo wlan client forwarding enable

関連コマンド

client forwarding-location

3.1.54 wlan client reauthentication-period

Syntax

wlan client reauthentication-period [*period-value*]

undo wlan client reauthentication-period

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

period-value: アイドル期間を 1～3600 秒の範囲で指定します。デフォルトでは、アイドル期間は 10 秒です。

説明

wlan client reauthentication-period コマンドはクライアント再認証の前にアイドル期間を設定します。

undo wlan client reauthentication-period コマンドはデフォルトに戻します。

クライアントの再認証の前にアイドル期間を設定して、再認証の失敗を減らします。

WLAN MAC 認証クライアントに対して URL リダイレクトが有効になっている場合、AP は MAC 認証を通過したクライアントからログオフします。次の MAC 認証試行で、クライアントは MAC 認証を通過し、WLAN にアクセスできます。アイドル期間が設定されていると、AP はクライアントをログオフした後にダイナミックブラックリストにクライアントを追加し、指定されたアイドル時間の経過後にクライアントエントリが期限切れになります。

例

クライアント再認証の前にアイドル期間を 100 秒に設定します。

<AC> system-view

[AC] wlan client reauthentication-period 100

3.1.55 wlan dynamic-blacklist active-on-ap

Syntax

wlan dynamic-blacklist active-on-ap

undo wlan dynamic-blacklist active-on-ap

デフォルト

ダイナミックブラックリストは AP に有効です。

View

System view

定義済みユーザロール

network-admin

説明

wlan dynamic-blacklist active-on-ap コマンドはダイナミックブラックリストを AP で有効にするように設定します。

undo wlan dynamic-blacklist active-on-ap コマンドはダイナミックブラックリストを AC に適用するように設定します。

ダイナミックブラックリストを AC に適用するように設定すると、AC に接続されているすべての AP はダイナミックブラックリストのクライアントを拒否します。ダイナミックブラックリストを AP に適用するように設定すると、ダイナミックブラックリスト内のクライアントに関連付けられている AP はクライアントを拒否しますが、クライアントは引き続き AC に接続されている他の AP と関連付けることができます。ダイナミックブラックリストを高密度環境で AC に適用するように設定することを推奨します。

例

ダイナミックブラックリストを AC 上で有効にするように設定します。

<AC> system-view

[AC] undo wlan dynamic-blacklist active-on-ap

3.1.56 wlan dynamic-blacklist lifetime

Syntax

wlan dynamic-blacklist lifetime *lifetime*

undo wlan dynamic-blacklist lifetime

デフォルト

300 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

lifetime: エージングタイマを指定します。設定範囲は 1～3600 秒です。

説明

wlan dynamic-blacklist lifetime コマンドはダイナミックブラックリストエントリのエージングタイマを設定します。

undo wlan dynamic-blacklist lifetime コマンドはデフォルトに戻します。

設定したエージングタイマは、設定後、ダイナミックブラックリストに追加されたエントリから有効です。

例

#ダイナミックブラックリストのエージングタイマを 3600 秒に指定します。

<AC> system-view

[AC] wlan dynamic-blacklist lifetime 3600

3.1.57 wlan link-test

Syntax

wlan link-test *mac-address*

View

すべての view

定義済みユーザロール

network-admin

パラメータ

mac-address: H-H-H 形式でクライアント MAC アドレスを指定します。

説明

wlan link-test コマンドはワイヤレスリンクの品質をテストします。

無線リンク品質検出により、AP は無線クライアントへのリンクの品質をテストできます。AP は、各サポートレートでクライアントに空のデータフレームを送信します。次に、クライアントからの応答に基づいて、RSSI、パケット再送信、RTT などのリンク品質情報を計算します。

無線リンク品質検出のタイムアウト時間は 10 秒です。タイムアウト時間内で無線リンク検出が完了しない場合、テスト結果を取得できません。

例

MAC アドレス 60a4-4cda-eff0 のクライアントに対して、無線リンク品質検出を実行します。

<AC> wlan link-test 60a4-4cda-eff0

```
Testing link to 60a4-4cda-eff0. Press CTRL + C to break.
                          Link Status
--------------------------------------------------------------------------
MAC address: 60a4-4cda-eff0
--------------------------------------------------------------------------
VHT-MCS  Rate(Mbps)  Tx packets  Rx packets  RSSI  Retries  RTT(ms)
--------------------------------------------------------------------------
NSS = 1
```

```
------------------------------------------------------------------------
0       6.5         5          5          54     0       0
1       13          5          5          51     0       0
2       19.5        5          5          49     0       0
3       26          5          5          47     0       0
4       39          5          5          45     0       0
5       52          5          5          45     0       0
6       58.5        5          5          44     0       0
7       65          5          5          44     0       0
8       78          5          5          44     0       0
------------------------------------------------------------------------
```

表 3-18 コマンド出力

フィールド	説明
No./MCS/VHT-MCS/HE-MCS	• **No**－802.11a、802.11b、802.11gクライアントのリンク品質テストの速度番号。 • **MCS**－802.11nクライアントのリンク品質テストのMCSインデックス。 • **VHT-MCS**－802.11acクライアントのリンク品質テストのVHT-MCSインデックス。 • **HE-MCS**－802.11axクライアントのリンク品質テストのHE-MCSインデックス。
Rate(Mbps)	APが無線リンク品質検出フレームを送信するレート。
Tx packets	APが送信した無線リンク品質検出フレームの数。
Rx packets	APが受信した無線リンク品質検出フレームの数。
RSSI	APが検出したクライアントのRSSI。
Retries	無線リンク品質検出フレームの再送信の数。
RTT(ms)	APからクライアントへの無線リンク品質検出フレームのラウンドトリップ時間。
NSS	802.11nまたは802.11ac/axクライアントでのリンク品質テスト用の空間ストリームの数。

3.1.58 wlan nas-port-id format

Syntax

wlan nas-port-id format { **2** | **4** }

undo wlan nas-port-id format

View

System view

定義済みユーザロール

network-admin

パラメータ

2: フォーマット 2（*SlotID***00***IfNOVlanID*）を指定します。このフォーマットにおいて、NAS ポート ID は以下の情報を含みます。

- **SlotID**－クライアントがアクセスするスロットの 2 桁の ID です。
- **IfNO**－クライアントがアクセスするインタフェースの 3 桁の番号です。
- **VlanID**－クライアント VLAN の 9 桁の ID です。

4: フォーマット 4（**slot=**;subslot=**;port=**;vlanid=**;vlanid2=****）を指定します。**vlanid2=****は、VLAN ターミネーションが有効なインタフェースで WLAN にアクセスするクライアントに対してのみ使用します。

説明

wlan nas-port-id format コマンドは NAS port ID フォーマットを指定します。

undo wlan nas-port-id format コマンドはデフォルトに戻します。

NAS port ID フォーマットは、NAS port ID が指定されていないときに適用されます。この場合、システムは NAS port ID フォーマットとクライアント情報に基づいて NAS port ID を生成します。NAS port ID が指定されている場合、指定された NAS port ID が使用されます。

例

NAS port ID フォーマットにフォーマット 4 を指定します。

<AC> system-view

[AC] wlan nas-port-id format 4

関連コマンド

nas-port-id

3.1.59 wlan permit-ssid

🕮 メモ：

wlan permit-ssid コマンドは、ソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

wlan permit-ssid *ssid-name*

undo wlan permit-ssid [*ssid-name*]

デフォルト

設定なし

View

User profile view

定義済みユーザロール

network-admin

パラメータ

ssid-name: SSID 名を指定します。1 から 32 文字で指定します。大文字と小文字は区別されます。

説明

wlan permit-ssid コマンドはクライアントアソシエーションを許可する SSID を設定します。

undo wlan permit-ssid コマンドは許可する SSID を削除します。*ssid-name* パラメータを指定しない場合、許可する SSID 設定を全て削除します。

クライアントアソシエーションを許可する SSID が設定されていない場合、クライアントアソシエーションは制限されません。

クライアントアソシエーションを許可する SSID が設定されている場合、クライアントは許可された SSID を介してのみ WLAN にアクセスできます。

例

クライアントアソシエーションを許可する SSID として SSID 名 ssid 1 を指定します。

<AC> system-view

[AC] user-profile profile1

[AC-user-profile-profile1] wlan permit-ssid ssid1

3.1.60 wlan service-template

Syntax

wlan service-template *service-template-name*

undo wlan service-template *service-template-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

service-template-name: サービステンプレート名を指定します。サービステンプレート名は、1～63 文字の文字列です。大文字と小文字を区別しません。

説明

wlan service-template コマンドはサービステンプレートを作成します。

undo wlan service-template コマンドはサービステンプレートを削除します。

指定したサービステンプレートが存在する場合、このコマンドにより service template view に移行します。

無線にバインドされているサービステンプレートは削除できません。

例

サービステンプレート **service1** を作成し、その view に移行します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1]

3.1.61 wlan static-blacklist mac-address

Syntax

wlan static-blacklist mac-address *mac-address*

undo wlan static-blacklist [**mac-address** *mac-address*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-address *mac-address*: クライアントの MAC アドレスを H-H-H の形式で指定します。

説明

wlan static-blacklist mac-address コマンドはスタティックブラックリストにクライアントを追加します。

undo wlan static-blacklist mac-address コマンドはスタティックブラックリストからクライアントを削除します。

スタティックブラックリストにオンラインクライアントを追加すると、クライアントをログオフします。

ホワイトリストとスタティックブラックリストの両方にクライアントを追加することはできません。

undo コマンドで、**mac-address** *mac-address* オプションを省略した場合、スタティックブラックリストからすべてのクライアントを削除します。

例

スタティックブラックリストに MAC アドレス 001c-f0bf-9c92 を追加します。

<AC> system-view

[AC] wlan static-blacklist mac-address 001c-f0bf-9c92

関連コマンド

display wlan blacklist

3.1.62 wlan web-server api-path

Syntax

wlan web-server api-path *path*

undo wlan web-server api-path

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

path: 1～256 文字の大文字と小文字を区別するパスを指定します。

説明

wlan web-server api-path コマンドはクライアント情報が報告される Web サーバのパスを設定します。

undo wlan web-server api-path コマンドはデフォルトに戻します。

Web サーバは、サーバのホスト名、ポート番号、およびパスが指定されている場合にのみ、クライアント情報を受け入れます。

このコマンドを複数回実行した場合、最新の設定が有効になります。

例

/wlan/dev-cfg として Web サーバのパスを指定します。

<AC> system-view

[AC] wlan web-server api-path /wlan/dev-cfg

関連コマンド

- **wlan web-server host**
- **wlan web-server max-client-entry**

3.1.63 wlan web-server host

Syntax

wlan web-server host *host-name* **port** *port-number*

undo wlan web-server host

デフォルト

Web サーバのホスト名とポート番号は指定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

host *host-name*: ホスト名を指定します。大文字、小文字を区別しない 3～127 文字です。文字列には、文字、数字、ハイフン（-）、アンダースコア（_）、ドット（.）を使用できます。

port *port-number*: ポート番号を 1～65534 の範囲で指定します。

説明

wlan web-server host コマンドはクライアント情報が報告される Web サーバのホスト名とポート番号を指定します。

undo wlan web-server host コマンドはデフォルトに戻します。

Web サーバは、サーバのホスト名、ポート番号、およびパスが指定されている場合にのみ、クライアント情報を受け入れます。

クライアント情報の変更はリアルタイムで Web サーバに報告されます。

このコマンドを複数回実行した場合、最新の設定が有効になります。

例

Web サーバのホスト名とポート番号は、それぞれ **www.abc.com** と **668** として指定します。

<AC> system-view

[AC] wlan web-server host www.abc.com port 668

関連コマンド

- **wlan web-server api-path**
- **wlan web-server max-client-entry**

3.1.64 wlan web-server max-client-entry

Syntax

wlan web-server max-client-entry *number*

undo wlan web-server max-client-entry

デフォルト

10

View

System view

定義済みユーザロール

network-admin

パラメータ

number: クライアントエントリの最大数を 1～25 の範囲で指定します。

説明

wlan web-server max-client-entry コマンドは一度に報告するクライアントエントリの最大数を設定します。

undo wlan web-server max-client-entry コマンドはデフォルトに戻します。

例

一度に報告するクライアントエントリの最大数を 12 に設定します。

<AC> system-view

[AC] wlan web-server max-client-entry 12

関連コマンド

- **wlan web-server api-path**
- **wlan web-server host**

3.1.65 wlan whitelist mac-address

Syntax

wlan whitelist mac-address *mac-address*

undo wlan whitelist [**mac-address** *mac-address*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-address *mac-address*: クライアントの MAC アドレスを H-H-H の形式で指定します。

説明

wlan whitelist mac-address コマンドはホワイトリストにクライアントを追加します。

undo wlan whitelist mac-address コマンドはホワイトリストからクライアントを削除します。

最初のクライアントをホワイトリストに追加すると、すべてのオンラインクライアントを切断するかどうかを尋ねるメッセージが表示されます。“Y”と入力するとホワイトリストが作成されます。

ホワイトリストからオンラインクライアントを削除すると、クライアントをログオフします。ホワイトリストからすべてのクライアントを削除すると、オンラインクライアントはログオフされません。

ホワイトリストとスタティックブラックリストの両方にクライアントを追加することはできません。

undo コマンドで、**mac-address** *mac-address* オプションを省略した場合、ホワイトリストからすべてのクライアントを削除します。

例

ホワイトリストに MAC アドレス 001c-f0bf-9c92 を追加します。

<AC> system-view

[AC] wlan whitelist mac-address 001c-f0bf-9c92

```
This command will disconnect all clients. Continue? [Y/N]:
```

関連コマンド

display wlan whitelist

目次

このセクションのページは **2-x-x** です。

4 章 WLAN セキュリティ 4-1
4.1 WLAN セキュリティコマンド 4-1
4.1.1 akm mode 4-1
4.1.2 akm sae pwe 4-2
4.1.3 cipher-suite 4-3
4.1.4 enhanced-open enable 4-5
4.1.5 enhanced-open transition-mode service-template 4-6
4.1.6 gtk-rekey client-offline enable 4-7
4.1.7 gtk-rekey enable 4-7
4.1.8 gtk-rekey method 4-8
4.1.9 key-derivation 4-10
4.1.10 pmf 4-11
4.1.11 pmf association-comeback 4-12
4.1.12 pmf saquery retrycount 4-13
4.1.13 pmf saquery retrytimeout 4-13
4.1.14 preshared-key 4-14
4.1.15 ptk-lifetime 4-16
4.1.16 ptk-rekey enable 4-16
4.1.17 security-ie 4-17
4.1.18 snmp-agent trap enable wlan usersec 4-19
4.1.19 tkip-cm-time 4-19
4.1.20 wep key 4-21
4.1.21 wep key-id 4-22
4.1.22 wep mode dynamic 4-24
4.1.23 wpa3 4-25

4章 WLAN セキュリティ

4.1 WLANセキュリティコマンド

4.1.1 akm mode

Syntax

akm mode { **dot1x** | **psk** | **anonymous-dot1x** }

undo akm mode

デフォルト

設定なし

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

dot1x: 802.1X を指定します。

psk: PSK を指定します。

anonymous-dot1x: ワイファイアライアンス Anonymous 802.1X を指定します。

説明

akm mode コマンドは AKM（Authentication and Key Management）モードを設定します。

undo akm mode コマンドはデフォルトに戻します。

RSNA ネットワークに AKM モードを設定する必要があります。

WLAN サービステンプレートは AKM モードを 1 つだけサポートします。WLAN サービステンプレートが無効なときだけ AKM モードを設定します。

OSEN IE モデルが使用される場合、ワイファイアライアンス Anonymous 802.1X AKM を設定します。

以下の AKM モードは、いずれも特定の認証モードで使用する必要があります。

- **802.1X AKM—**802.1X 認証モード
- **PSK AKM—**MAC もしくは認証バイパスモード
- ワイファイアライアンス Anonymous **802.1X AKM—**802.1X 認証モード

詳細は、オペレーションマニュアルのセクション 2 *WLAN “WLAN アクセスの設定”* を参照してください。

例

PSK AKM モードを設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] akm mode psk

関連コマンド

- **cipher-suite**
- **security-ie**

4.1.2 akm sae pwe

🕮 **メモ**:

- **akm sae pwe** コマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。
- **both-h2e-hnp** を指定すると **hnp** のみをサポートしたクライアントでローミングに失敗する場合があります。クライアントの問題ですが、ローミング失敗を避けるために”**akm sae pwe hnp**”を設定してください。

Syntax

akm sae pwe { both-h2e-hnp | h2e | hnp }

undo akm sae pwe

デフォルト

both-h2e-hnp

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

both-h2e-hnp: PWE の生成方式として、Hunting-and-Pecking (HnP)と Hash-to-Element (H2E)を指定します。

h2e: PWE の生成方式として、Hash-to-Element (H2E)を指定します。

hnp: PWE の生成方式として、Hunting-and-Pecking (HnP)を指定します。

説明

akm sae pwe コマンドは WPA 3-SAE の SAE 交換時の PWE 生成方式を設定します。

undo akm sae pwe コマンドはデフォルトに戻します。

WPA3-SAE は、Hunting-and-Pecking (HnP) と Hash-to-Element (H2E) を使用した PWE の生成をサポートしています。H2E は最新の PWE 生成方法であり、強化されたセキュリティパフォーマンスを提供します。

クライアントが指定された PWE 生成方式をサポートしていない場合、クライアントは WLAN にアクセスできません。クライアントの互換性を向上させる場合は、both-h2e-hnp キーワードを指定します。

例

WPA3-SAE の PWE 生成方式として H2E を設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] akm sae pwe h2e

関連コマンド

wpa3

4.1.3 cipher-suite

🕮 **メモ**:

- QX-W1000 シリーズの AP はソフトウェアバージョン 7.2.18 を含む以降のソフトウェアから **gcmp** パラメータをサポートしています。
- QX-W1100 シリーズの AP はソフトウェアバージョン 7.2.55 を含む以降のソフトウェアから **gcmp** パラメータをサポートしています。
- QX-W1120 の Radio3 は、**gcmp** パラメータをサポートしていません。
- QX-W1130 の Radio1 は、**gcmp** パラメータをサポートしていません。
- QX-W1200 シリーズの AP では、**wep40**、**wep104**、**wep128** のパラメータをサポートしていません。

⚠ **重要**:

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

Syntax

cipher-suite { **ccmp** | **gcmp** | **tkip** | **wep40** | **wep104** | **wep128** }

undo cipher-suite { **ccmp** | **gcmp** | **tkip** | **wep40** | **wep104** | **wep128** }

デフォルト

設定なし

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

ccmp: AES-CCMP 暗号方式を指定します。

gcmp: AES-GCMP 暗号方式を指定します。

tkip: TKIP 暗号方式を指定します。

wep40: WEP40 暗号方式を指定します。

wep104: WEP104 暗号方式を指定します。

wep128: WEP128 暗号方式を指定します。

説明

cipher-suite コマンドはフレーム暗号化に使用する暗号方式を指定します。

undo cipher-suite コマンドは指定した暗号方式を無効にします。

RSNA ネットワークに暗号方式を指定しなければなりません。WLAN サービステンプレートが無効の場合のみ暗号方式を設定します。

RSN IE あるいは WPA IE を設定するとき、TKIP、CCMP、あるいは GCMP 暗号方式を設定します。

WEP 暗号方式には、WEP40、WEP104、WEP128 の 3 タイプ含まれます。各 WLAN サービステンプレートは WEP 暗号方式の 1 タイプのみをサポートします。WEP 暗号方式のタイプを設定したあと、タイプの同じ鍵を作成および適用しなければなりません。

CCMP、TKIP あるいは GCMP 暗号方式が設定されている場合、WEP128 は設定できません。

例

フレーム暗号化用の TKIP 暗号方式を設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] cipher-suite tkip

関連コマンド

- **security-ie**
- **wep key**
- **wep key-id**

4.1.4 enhanced-open enable

> 🕮 **メモ：**
>
> **enhanced-open enable** コマンドはソフトウェアバージョン 7.2.27 を含む以降のソフトウェアでサポートしています。

Syntax

enhanced-open enable

undo enhanced-open enable

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

説明

enhanced-open enable コマンドは Enhanced Open システム認証を有効にします。

undo enhanced-open enable コマンドは Enhanced Open システム認証を無効にします。

例

Enhanced Open システム認証を有効にします。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] enhanced-open enable

関連コマンド

enhanced-open transition-mode service-template

4.1.5 enhanced-open transition-mode service-template

🕮 メモ：

enhanced-open transition-mode service-template コマンドはソフトウェアバージョン 7.2.27 を含む以降のソフトウェアでサポートしています。

Syntax

enhanced-open transition-mode service-template *service-template-name*

undo enhanced-open transition-mode service-template

デフォルト

設定なし

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

service-template-name: 大文字と小文字を区別しない 1～63 文字の文字列でサービステンプレートの名前を指定します。

説明

enhanced-open transition-mode service-template コマンドは移行モードでの推奨サービステンプレートを指定します。

undo enhanced-open transition-mode service-template コマンドはデフォルト設定に戻します。

このコマンドを複数回実行した場合、最後に実行した設定が反映されます。

例

サービステンプレート **service1** に対して、移行モードでの推奨サービステンプレートとして **service2** を指定します。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] enhanced-open transition-mode service-template service2

関連コマンド

- **beacon ssid-hide**

- **enhanced-open enable**

4.1.6 gtk-rekey client-offline enable

Syntax

gtk-rekey client-offline enable

undo gtk-rekey client-offline enable

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

説明

gtk-rekey client-offline enable コマンドは offline-triggered GTK update を有効にします。

undo gtk-rekey client-offline コマンドはデフォルトに戻します。

GTK update が有効な場合のみ offline-triggered GTK update を有効にします。

例

offline-triggered GTK update を有効にします。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] gtk-rekey client-offline enable

関連コマンド

gtk-rekey enable

4.1.7 gtk-rekey enable

Syntax

gtk-rekey enable

undo gtk-rekey enable

デフォルト

GTK update のデフォルト値は、ソフトウェアバージョンにより異なります。

ソフトウェアバージョン 7.2.56 を含む以前のソフトウェアでは有効(コンフィグ上は非表示)です。

ソフトウェアバージョン 7.2.58 を含む以降のソフトウェアでは無効(コンフィグ上は非表示)です。

View

WLAN service template view

定義済みユーザロール

network-admin

説明

gtk-rekey enable コマンドは GTK update を有効にします。

undo gtk-rekey enable コマンドは GTK update を無効にします。

例

GTK update を有効にします。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] gtk-rekey enable

4.1.8 gtk-rekey method

Syntax

gtk-rekey method { **packet-based** [*packet*] | **time-based** [*time*] }

undo gtk-rekey method

デフォルト

GTK は 86400 秒間隔でアップデートされます。

伝送パケット数のデフォルトは 10000000 です。

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

packet-based *packet*: GTK がアップデートされる前に、マルチキャストとブロードキャストを含む伝送パケットの数を指定します。*packet* 引数の値の範囲は 5000~4294967295 です。

time-based *time*: GTK がアップデートされる間隔を指定します。*time* 引数の値の範囲は 180~604800 秒であり、デフォルトは 86400 秒です。

説明

gtk-rekey method コマンドは GTK update 手法を設定します。

undo gtk-rekey method コマンドはデフォルトに戻します。

GTK update が有効な場合のみ GTK update 手法を設定します。

直近のコンフィグレーションは、それ以前のコンフィグレーションを上書きします。例えば、packet に基づく手法を設定した後 time に基づく設定をする場合、time に基づく手法が効力をもちます。

サービステンプレートが有効になった後 GTK update 手法を設定する場合、以下の条件が存在するとき変更点が反映されます。

- GTK update 間隔を変更する場合、すでに設定されていたタイマが終了したとき新たな間隔が反映されます。
- パケット数しきい値を変更する場合、新たなしきい値は即座に反映されます。
- GTK update 手法を packet に基づく設定に変更する場合、タイマが消去されパケット数がしきい値に達したとき新たな設定が反映されます。
- GTK update 手法を time に基づく設定に変更する場合、新たな設定は即座に反映されます。

例

アップデート間隔に基づく GTK update を有効にします。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] gtk-rekey method time-based 3600

パケットに基づく GTK update を有効にします。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] gtk-rekey method packet-based 600000

関連コマンド

gtk-rekey enable

4.1.9 key-derivation

Syntax

key-derivation { **sha1** | **sha1-and-sha256** | **sha256** }

undo key-derivation

デフォルト

sha1

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

sha1: HMAC-SHA1 アルゴリズムを KDF として指定します。

sha256: HMAC-SHA256 アルゴリズムを KDF として指定します。

sha1-and-sha256: HMAC-SHA1 アルゴリズムと HMAC-SHA256 アルゴリズムを KDF として指定します。

説明

key-derivation コマンドは KDF（Key Derivation Function）を設定します。

undo key-derivation コマンドはデフォルトに戻します。

KDF は、RSNA メカニズムを使用するネットワークに対してのみ有効です。

管理フレーム保護が有効になっている場合、HMAC-SHA256 アルゴリズムを KDF として構成することをお勧めします。

例

HMAC-SHA256 アルゴリズムを KDF として構成します。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] key-derivation sha256

関連コマンド

- **akm mode**
- **cipher-suite**
- **security-ie**

4.1.10 pmf

🕮 **メモ：**

- 192bitセキュリティなしのWPA3エンタープライズはWPA2+管理フレーム保護(**pmf**)と同じです。管理フレーム保護を必須(**mandatory**)として設定をすることで、192bit セキュリティなしの WPA3 エンタープライズと同等の動作をします。
- 管理フレーム保護を設定する場合は、KDF の設定”**key-derivation sha1-and-sha256**”をしてください。

Syntax

pmf { **mandatory** | **optional** }

undo pmf

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

mandatory: 必須モードを指定します。管理フレーム保護をサポートしたクライアントのみ WLAN にアクセスできます。

optional: オプションモードを指定します。すべてのクライアントが WLAN にアクセスできます。

説明

pmf コマンドは管理フレーム保護を有効にします。

undo pmf コマンドはデフォルトに戻します。

管理フレーム保護は、暗号化規格が RSN かつ暗号化方式が CCMP である RSNA メカニズムを使用するネットワークにのみ適用されます。

例

オプションモードで管理フレーム保護を有効にします。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] pmf optional

関連コマンド

- **cipher-suite**
- **security-ie**

4.1.11 pmf association-comeback

Syntax

pmf association-comeback *time*

undo pmf association-comeback

デフォルト

1 秒

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

time: アソシエーション復帰時間を指定します。設定範囲は 1~20 秒です。

説明

pmf association-comeback コマンドはアソシエーション復帰時間を設定します。

undo pmf association-comeback コマンドはデフォルトに戻します。

AP がクライアントからのアソシエーション要求もしくは再アソシエーション要求を拒否する場合、AP は要求が拒否されたことと、後でクライアントが接続できることを知らせる応答を送ります。この応答にはアソシエーション復帰時間が含まれています。。アソシエーション復帰時間が終了すると、AP はクライアントからのアソシエーション要求もしくは再アソシエーション要求の受信を開始します。

例

アソシエーション復帰時間を 2 秒に設定します。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] pmf association-comeback 2

4.1.12 pmf saquery retrycount

Syntax

pmf saquery retrycount *count*

undo pmf saquery retrycount

デフォルト

4 回

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

count: SA クエリ要求の最大試行回数を指定します。設定範囲は 1~16 です。

説明

pmf saquery retrycount コマンドは SA クエリ要求を再伝送する試行回数を最大にします。

undo pmf saquery retrycount コマンドはデフォルトに戻します。

最大試行回数に達した後 AP が SA クエリ要求への確認を受信しない場合、AP はクライアントをオフラインにします。

例

SA クエリ要求への最大試行回数を 3 に設定します。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] pmf saquery retrycount 3

関連コマンド

- **pmf**
- **pmf saquery retrytimeout**

4.1.13 pmf saquery retrytimeout

Syntax

pmf saquery retrytimeout *timeout*

undo pmf saquery retrytimeout

デフォルト

200 ミリ秒

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

timeout: AP が SA クエリ要求を送信する間隔を指定します。設定範囲は 100~500 ミリ秒です。

説明

pmf saquery retrytimeout コマンドは SA クエリ要求を送信する間隔を設定します。

undo pmf saquery retrytimeout コマンドはデフォルトに戻します。

例

SA クエリ要求を送信する間隔を 300 ミリ秒に設定します。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] pmf saquery retrytimeout 300

関連コマンド

- **pmf**
- **pmf saquery retrycount**

4.1.14 preshared-key

🕮 **メモ：**

ソフトウェアバージョン 7.2.79 を含む以降のソフトウェアから、**pass-phrase** 文字列で ”?” の文字の使用をサポートしています。
下記以外の文字は使用可能です。

- ダブルクォーテーション
- タブ
- キャリッジリターン

Syntax

preshared-key { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*

undo preshared-key

デフォルト

設定なし

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

pass-phrase: 文字列で PSK を設定します。

raw-key: 文字列で PSK を設定します。

cipher: 16 進数で PSK を設定します。

simple: プレーンテキストで鍵を設定します。セキュリティ上の理由から、プレーンテキストで指定された鍵は暗号化された形式で保存されます。

string: 鍵の文字列を指定します。この引数は大文字、小文字を区別します。鍵長は鍵タイプにより変わります。

- **pass-phrase(プレーンテキスト)**－8~63 文字
- **pass-phrase(暗号テキスト)**－8~117 文字
- **raw-key(プレーンテキスト)**－16 進数で 64 桁
- **raw-key(暗号テキスト)**－8~117 文字

説明

preshared-key コマンドは PSK を設定します。

undo preshared-key コマンドはデフォルトに戻します。

WLAN サービステンプレートが無効で、AKM モードが PSK のときにのみ PSK を設定します。AKM モードが 802.1X のときに PSK を設定した場合、WLAN サービステンプレートは有効ですが PSK コンフィグレーションは反映されません。

WLAN サービステンプレートに設定できる PSK は 1 つだけです。

例

PSK としてプレーンテキストで文字列 12345678 を設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] akm mode psk

[AC-wlan-st-security] preshared-key pass-phrase simple 12345678

関連コマンド

akm mode

4.1.15 ptk-lifetime

Syntax

ptk-lifetime *time*

undo ptk-lifetime

デフォルト

43200 秒

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

time: PTK ライフタイムを指定します。設定範囲は 180~604800 秒です。

説明

ptk-lifetime コマンドは PKT ライフタイムを設定します。

undo ptk-lifetime コマンドはデフォルトに戻します。

サービステンプレートが有効なときに PTK ライフタイムを設定する場合、その設定は既定のタイマが終了した後に反映されます。

例

PTK ライフタイムを 200 秒に設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] ptk-lifetime 200

4.1.16 ptk-rekey enable

Syntax

ptk-rekey enable

undo ptk-rekey enable

デフォルト

PTK 更新のデフォルト値は、ソフトウェアバージョンにより異なります。

ソフトウェアバージョン 7.2.56 を含む以前のソフトウェアでは有効(コンフィグ上は非表示)です。

ソフトウェアバージョン 7.2.58 を含む以降のソフトウェアでは無効(コンフィグ上は非表示)です。

View

WLAN service template view

定義済みユーザロール

network-admin

説明

ptk-rekey enable コマンドは PTK 更新を有効にします。

undo ptk-rekey enable コマンドは PTK 更新を無効にします。

この機能により、設定された PTK の有効期限が切れた後、装置は PTK を更新できます。

例

PTK 更新を有効にします。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] ptk-rekey enable

関連コマンド

ptk-lifetime

4.1.17 security-ie

Syntax

security-ie { **osen** | **rsn** | **wpa** }

undo security-ie { **osen** | **rsn** | **wpa** }

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

osen: AP から送信されたビーコンおよびプローブ応答フレーム内の OSEN IE を有効にします。OSEN IE は、AP の OSEN 機能をアドバタイズします。

rsn: AP から送信されたビーコンおよびプローブ応答フレーム内の RSN IE を有効にします。RSN IE は、AP の RSN 機能をアドバタイズします。

wpa: AP から送信されたビーコンおよびプローブ応答フレーム内の WPA IE を有効にします。WPA IE は、AP の WPA 機能をアドバタイズします。

説明

security-ie コマンドはビーコンおよびプローブ要求内で OSEN IE、RSN IE、あるいは WPA IE を有効にします。

undo security-ie コマンドはビーコンおよびプローブ要求内で OSEN IE、RSN IE、あるいは WPA IE を無効にします。

RSNA ネットワークの暗号化規格を設定する必要があります。WLAN サービステンプレートが無効で、CCMP または TKIP 暗号化方式が設定されている場合のみ、暗号化規格を設定できます。

同じ WLAN サービステンプレートに対して WPA IE と RSN IE の両方を設定できます。WPA IE と RSN IE は、WLAN サービステンプレートの OSEN IE と一緒に使用することはできません。

暗号化規格に WPA2 または WPA3 を使用する場合は RSN IE、WPA を使用する場合は WPA IE を設定します。ワイファイアライアンス Anonymous 802.1X AKM の場合、OSEN IE を設定します。

例

ビーコン応答とプローブ応答で RSN IE をイネーブルにします。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] security-ie rsn

関連コマンド

- **akm mode**
- **cipher-suite**

4.1.18 snmp-agent trap enable wlan usersec

Syntax

snmp-agent trap enable wlan usersec

undo snmp-agent trap enable wlan usersec

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan usersec コマンドは WLAN セキュリティに対して SNMP 通知を有効にします。

undo snmp-agent trap enable wlan usersec コマンドは WLAN セキュリティに対して SNMP 通知を無効にします

重要な WLAN セキュリティイベントを NMS に報告するために、WLAN セキュリティに対して SNMP 通知を有効にします。WLAN セキュリティイベント通知を正確に送信するため、オペレーションマニュアルのセクション 11 *システム管理 “SNMP”* に記載されているように SNMP の設定も行わなければなりません。

例

WLAN セキュリティに対して SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan usersec

4.1.19 tkip-cm-time

Syntax

tkip-cm-time *time*

undo tkip-cm-time

デフォルト

0 秒

AP は対策をとりません。

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

time: TKIP MIC 失敗ホールド時間を設定します。設定範囲は 0~3600 秒です。

説明

tkip-cm-time コマンドは TKIP MIC 失敗ホールド時間を設定します。

undo tkip-cm-time コマンドはデフォルトに戻します。

暗号化方式に TKIP が設定されているときにのみ TKIP MIC 失敗ホールド時間を設定します。

サービステンプレートが有効なときに MIC 失敗ホールド時間を設定する場合、その設定は既定のタイマが終了したあとに反映されます。

MIC 失敗ホールド時間内に AP が 2 つの MIC 失敗を検出した場合、AP はすべてのクライアントを 60 秒間分離させます。

例

TKIP MIC 失敗ホールド時間を 180 秒に設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] tkip-cm-time 180

関連コマンド

cipher-suite

4.1.20 wep key

⚠ **重要**：

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

🕮 **メモ**：

wep key コマンドは、QX-W1200 シリーズの AP ではサポートしていません。

Syntax

wep key *key-id* { **wep40** | **wep104** | **wep128** } { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*

undo wep key *key-id*

デフォルト

設定なし

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

key-id: key ID を設定します。設定範囲は 1~4 です。

wep40: WEP40 key を設定します。

wep104: WEP104 key を設定します。

wep128: WEP128 key を設定します。

pass-phrase: WEP key を文字列で設定します。

raw-key: WEP key を 16 進数で設定します。

cipher: 暗号テキストで鍵を設定します。

simple: プレーンテキストで鍵を設定します。セキュリティ上の理由から、平文形式で指定された鍵は暗号化された形式で保存されます。

string: 鍵列を指定します。大文字と小文字を区別します。設定範囲は 37~73 文字です。プレーンテキストの鍵の長さは鍵タイプにより異なります。

- **wep40 pass-phrase(プレーンテキスト)**－5 文字
- **wep104 pass-phrase(プレーンテキスト)**－13 文字
- **wep128 pass-phrase(プレーンテキスト)**－16 文字

- **wep40 raw-key(プレーンテキスト)**－16 進数で 10 桁
- **wep104 raw-key(プレーンテキスト)**－16 進数で 26 桁
- **wep128 raw-key(プレーンテキスト)**－16 進数で 32 桁

説明

wep key コマンドは WEP 鍵を設定します。

undo wep key コマンドは設定した WEP 鍵を削除します。

WLAN サービステンプレートが無効で、暗号化方式に WEP が設定されているときにのみ WEP key を設定します。最大で 4 つの WEP key を設定できます。

例

暗号化方式に WEP40 を設定し、WEP key 1 としてプレーンテキスト 12345 を設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] cipher-suite wep40

[AC-wlan-st-security] wep key 1 wep40 pass-phrase simple 12345

関連コマンド

- **cipher-suite**
- **wep key-id**

4.1.21 wep key-id

重要：

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

メモ：

wep key-id コマンドは、QX-W1200 シリーズの AP ではサポートしていません。

Syntax

wep key-id { **1** | **2** | **3** | **4** }

undo wep key-id

デフォルト

Key 1

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

1: ID が 1 の WEP key を指定します。

2: ID が 2 の WEP key を指定します。

3: ID が 3 の WEP key を指定します。

4: ID が 4 の WEP key を指定します。

説明

wep key-id コマンドは WEP key を適用します。

undo wep key-id コマンドはデフォルトに戻します。

WLAN サービステンプレートが無効のときのみ WEP key を適用します。

RSNA メカニズムでは key 1 が交渉される鍵です。WEP key を適用するために、ID が 1 でない鍵を指定してください。

既存の WEP キーのみを適用できます。

例

暗号化方式に WEP40 を設定し、WEP key 1 としてプレーンテキスト 12345 を設定し、WEP key 1 を適用します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] cipher-suite wep40

[AC-wlan-st-security] wep key 1 wep40 pass-phrase simple 12345

[AC-wlan-st-security] wep key-id 1

関連コマンド

wep key

4.1.22 wep mode dynamic

⚠ **重要：**

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

🕮 **メモ：**

wep mode dynamic コマンドは、QX-W1200 シリーズの AP ではサポートしていません。

Syntax

wep mode dynamic

undo wep mode dynamic

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

説明

wep mode dynamic コマンドはダイナミック WEP メカニズムを有効にします。

undo wep mode dynamic コマンドはダイナミック WEP メカニズムを無効にします。

WLAN サービステンプレートが無効のときのみ WEP メカニズムを有効にします。

ダイナミック WEP メカニズムはユーザアクセス認証のために 802.1X 認証を要求します。

ダイナミック WEP メカニズムが有効な場合、WEP key 4 を適用しないでください。

例

ダイナミック WEP メカニズムを有効にします。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] wep mode dynamic

関連コマンド

- **cipher-suite**

- **client-security authentication-mode**(コマンドマニュアルのセクション 2 *WLAN "WLAN アクセスの設定"*)
- **wep key**
- **wep key-id**

4.1.23 wpa3

🕮 **メモ**:

- **wpa3** コマンドはソフトウェアバージョン 7.2.18 を含む以降のソフトウェアからサポートしています。
- WPA3 エンタープライズの 192bit セキュリティモードは QX-W1100 シリーズの AP はソフトウェアバージョン 7.2.55 を含む以降のソフトウェアから WPA3 エンタープライズの 192bit セキュリティをサポートしています。
- QX-W1120 の Radio3 は、WPA3 エンタープライズの 192bit セキュリティをサポートしていません。
- QX-W1130 の Radio1 は、WPA3 エンタープライズの 192bit セキュリティをサポートしていません。
- QX-W1200 シリーズの 6GHz 帯の Radio は、WPA3 パーソナル(**mandatory**)と WPA3 エンタープライズ 192bit セキュリティモードが使用できます。ソフトウェアバージョン 7.2.85a を含む以降のソフトウェアから、WPA3 エンタープライズ 192bit セキュリティなしモード(**wpa3 enterprise-only-mode)**が使用できます。ソフトウェアバージョン 7.2.89 を含む以降のソフトウェアから、WPA3 パーソナル(**optional**)と WPA3 エンタープライズ 192bit セキュリティなしモード(**wpa3 enterprise-transition-mode)** が使用できます。
- WPA3 エンタープライズの 192bit セキュリティなしモードについては、管理フレーム保護の設定を参照して下さい。
- 192bit セキュリティなしの WPA3 エンタープライズについては、管理フレーム保護で実現します。**pmf** コマンドを参照して下さい。
- **enterprise-only-mode** のパラメータはソフトウェアバージョン 7.2.73 を含む以降のソフトウェアからサポートしています。
- **enterprise-transition-mode** のパラメータはソフトウェアバージョン 7.2.73 を含む以降のソフトウェアからサポートしています。
- **wpa3 enterprise-only-mode** と **wpa3 enterprise-transition-mode** を設定する場合、事前に **pmf** コマンドと **key-derivation** コマンドがサービステンプレートに設定されていないことを確認してください。

Syntax

wpa3 { **enterprise** | **enterprise-only-mode** | **enterprise-transition-mode** | **personal** { **mandatory** | **optional** } }

undo wpa3

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

mdc-admin

パラメータ

enterprise: WPA3 エンタープライズの 192bit セキュリティモードを使用します。

enterprise-only-mode: WPA3 エンタープライズで WPA3 セキュリティモードを必須モードに指定します。WPA3 セキュリティモードをサポートしていないクライアントはアクセスできません。このパラメータを指定した場合、**pmf mandatory**、**key-derivation sha256** を設定したときと同じ動作となります。

enterprise-transition-mode: WPA3 エンタープライズで WPA3 セキュリティモードを WPA3 移行モードに指定します。このモードでは、WPA3 セキュリティモードをサポートしているクライアントとサポートしていないクライアントのどちらもアクセスできます。このパラメータを指定した場合、**pmf optional**、**key-derivation sha1-and-sha256** を設定したときと同じ動作となります。

personal: WPA3 パーソナルを使用します。

mandatory: WPA3 パーソナルで WPA3 セキュリティモードを必須モードに指定します。WPA3 セキュリティモードをサポートしていないクライアントはアクセスできません。

optional: WPA3 パーソナルで WPA3 セキュリティモードをオプションモードに指定します。WPA3 セキュリティモードをサポートしているクライアントとサポートしていないクライアントのどちらもアクセスできます。

説明

wpa3 コマンドは WPA3 エンタープライズ(WPA3 必須モード、WPA3 移行モード、192bit セキュリティモード)、または、WPA3 パーソナルを有効にします。

undo wpa3 コマンドは WPA3 エンタープライズ(WPA3 必須モード、移行モード、192bit セキュリティモード)、または、WPA3 パーソナルを無効にします。

- WPA3 エンタープライズの 192bit セキュリティモードー暗号化規格を RSN に設定し、暗号化方式を GCMP に設定する必要があります。
- WPA3 エンタープライズ(192bit セキュリティなし)ー暗号化規格を RSN に設定し、暗号化方式を CCMP に設定する必要があります。管理フレーム保護(**pmf**)、または、**wpa3 enterprise-only-mode** コマンドか **wpa3 enterprise-transition-mode** コマンドを設定します。

- WPA3 パーソナル一暗号化規格を RSN に設定し、暗号化方式を CCMP に設定する必要があります。

WPA3 セキュリティモードを有効にした後、管理フレーム保護を同時に有効にすることを推奨します。

例

WPA3 セキュリティモードをパーソナルレベルの必須モードに設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] wpa3 personal mandatory

WPA3 エンタープライズのセキュリティモードを WPA3 必須モードに設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] wpa3 enterprise-only-mode

目次

このセクションのページは **2-x-x** です。

5 章 WLAN 認証 5-1
5.1 WLAN 認証設定コマンド 5-1
5.1.1 client-security accounting-delay time 5-1
5.1.2 client-security accounting-start trigger 5-2
5.1.3 client-security accounting-update trigger 5-3
5.1.4 client-security authentication fail-vlan 5-5
5.1.5 client-security authentication-location 5-6
5.1.6 client-security authentication-mode 5-7
5.1.7 client-security authorization-fail offline 5-9
5.1.8 client-security ignore-authorization 5-10
5.1.9 client-security intrusion-protection action 5-10
5.1.10 client-security intrusion-protection enable 5-12
5.1.11 client-security intrusion-protection timer temporary-block 5-13
5.1.12 client-security intrusion-protection timer temporary-service-stop 5-14
5.1.13 display wlan client-security block-mac 5-15
5.1.14 dot1x domain 5-16
5.1.15 dot1x handshake enable 5-17
5.1.16 dot1x handshake secure enable 5-18
5.1.17 dot1x max-user 5-19
5.1.18 dot1x re-authenticate enable 5-20
5.1.19 fail-permit enable 5-21
5.1.20 fail-permit template 5-23
5.1.21 mac-authentication domain 5-24
5.1.22 mac-authentication fast-connect enable 5-25
5.1.23 mac-authentication max-user 5-26
5.1.24 port-security oui 5-27
5.1.25 radius-server test-profile 5-28
5.2 Web 認証(ポータル認証)設定コマンド 5-30

5章 WLAN 認証

5.1 WLAN認証設定コマンド

本章では、WLAN に関する認証コマンドについて説明します。802.1X および MAC アドレス認証コマンドの情報については、コマンドマニュアルのセクション 9 *セキュリティ “802.1X”、“MAC アドレス認証”* を参照ください。

5.1.1 client-security accounting-delay time

Syntax

client-security accounting-delay time *time* [**no-ip-logoff**]

undo client-security accounting-delay time

デフォルト

装置がクライアントの IP アドレスを学習するとき、装置はアカウンティング開始要求をクライアントに送信します。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

time: クライアントが 802.1X 認証もしくは MAC 認証を通過した後に開始するアカウンティング遅延タイマを指定します。値の範囲は 1～600 秒です。

no-ip-logoff: 遅延タイマ以内にクライアントの IP アドレスを取得できない場合、装置はクライアントをログオフします。このパラメータを指定しない場合、装置は遅延タイマが終了したときアカウンティング開始要求を送信します。

説明

client-security accounting-delay time コマンドはアカウンティング遅延を設定します。

undo client-security accounting-delay time コマンドはデフォルトに戻します。

装置がクライアントの指定されたタイプの IP アドレスを遅延時間内に学習できない場合、装置はクライアントに対して事前に定義されたアクションを実行します。アカウンティング開始権限を持つ IP アドレスのタイプを指定するために、**client-security**

accounting-start trigger コマンドを使用します。IP アドレスのタイプを none に設定すると、アカウンティング遅延機能は適用されません。

アカウンティング遅延タイマを設定するとき、装置が IP アドレスを取得する時間を考慮してください。ローパフォーマンスなネットワークでは遅延タイマを大きく設定してください。

サービステンプレートが有効な状態でこのコマンドを実行すると、コマンド実行後に接続したクライアントにのみ設定が適用されます。このコマンドが実行される前からオンラインだったクライアントには適用されません。

例

サービステンプレート **service1** で、アカウンティング遅延タイマを 15 秒に設定します。装置がクライアントの IP アドレスを遅延タイマ以内に学習できない場合、クライアントをログオフするように設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security accounting-delay time 15 no-ip-logoff

関連コマンド

client-security accounting-start trigger

5.1.2 client-security accounting-start trigger

Syntax

client-security accounting-start trigger { **ipv4** | **none** }

undo client-security accounting-start trigger

デフォルト

IPv4

View

Service template view

定義済みユーザロール

network-admin

パラメータ

ipv4: IPv4 アドレスタイプを指定します。

none: クライアントが認証をパスしたとき、クライアントにアカウンティング開始要求を送信するように設定します。

説明

client-security accounting-start trigger コマンドはアカウンティング開始権限を持つように IP アドレスタイプを指定します。

undo client-security accounting-start trigger コマンドはデフォルトに戻します。

このコマンドを設定すると、特定の IP アドレスタイプを使用したクライアントのために、装置はアカウンティングサーバにアカウンティング開始要求を送信します。このコマンドは、802.1X 認証あるいは MAC 認証をパスしたクライアントに適用されます。アカウンティングに関する詳細はオペレーションマニュアルのセクション 9 *セキュリティ "AAA"* を参照してください。

アカウンティング開始権限を持つように IP アドレスのタイプを設定するには、IP アドレスタイプの学習を有効にする必要があります。無線クライアント IP アドレス学習に関する詳細は、オペレーションマニュアルのセクション 2 *WLAN "WLAN IP スヌーピング"* を参照してください。

このコマンドを使用して設定された IP アドレスタイプは、アカウンティングサーバのプロトコル要件を満たす必要があります。

サービステンプレートが有効な状態でこのコマンドを実行すると、コマンド実行後に接続したクライアントにのみ設定が適用されます。このコマンドが実行される前からオンラインだったクライアントには適用されません。

例

サービステンプレート **service1** で、IPv4 アドレスを使用するクライアントに対してのみアカウンティング開始要求を送信するように装置を設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security accounting-start trigger ipv4

関連コマンド

- **client ipv4-snooping arp-learning enable**
- **client-security accounting-delay time**
- **client-security accounting-update trigger**

5.1.3 client-security accounting-update trigger

Syntax

client-security accounting-update trigger ipv4

undo client-security accounting-update trigger

デフォルト

装置は、サーバに割り当てられた、もしくはユーザに定義されたリアルタイムアカウンティング間隔で、アカウンティングアップデート要求をアカウンティングサーバに送信します。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

ipv4: IPv4 アドレスタイプを指定します。装置は、学習済みのクライアントの IP アドレスが IPv4 アドレスに変更されたときにのみアカウンティングアップデートを引き起こします。

説明

client-security accounting-update trigger コマンドはアカウンティングアップデート権限を持つように IP アドレスタイプを指定します。

client-security accounting-update trigger コマンドはデフォルトに戻します。

このコマンドは **client-security accounting-start trigger** コマンドを適用している場合にのみ適用できます。

このコマンドは、定期的なリアルタイムアカウンティング機能の影響を受けません。例えば、アカウンティングアップデートトリガを ipv4 に設定した状態でリアルタイムアカウンティング間隔を 12 分に設定した場合、どちらの設定も適用されます。両方の設定を使用したクライアントに対し、装置はアップデートアカウンティング要求を 12 分おきに送信します。また、クライアントの IP アドレスが IPv4 に変更されるたびに、装置はアカウンティングアップデートします。

リアルタイムアカウンティング間隔を設定するためには、**timer realtime-accounting** コマンドを使用してください。

サービステンプレートが有効な状態でこのコマンドを実行すると、コマンド実行後に接続したクライアントにのみ設定が適用されます。このコマンドが実行される前からオンラインだったクライアントには適用されません。

例

サービステンプレート **service1** で、クライアントの IP アドレスが IPv4 アドレスに変更されると装置がアカウンティングアップデートするように設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security accounting-update trigger ipv4

関連コマンド

- **client-security accounting-start trigger**
- **timer realtime-accounting**

5.1.4 client-security authentication fail-vlan

🕮 **メモ：**

このコマンドは、認証モードが MAC アドレス認証または PSK＋MAC アドレス認証の時に使用することができます。
802.1X 認証、PSK 認証では使用できません。

Syntax

client-security authentication fail-vlan *vlan-id*

undo client-security authentication fail-vlan

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

vlan-id: WLAN 制限 VLAN の ID を指定します。範囲は 1～4094 です。VLAN が作成されていることを確認してください。

説明

client-security authentication fail-vlan コマンドはサービステンプレートで WLAN 制限 VLAN を設定します。

undo client-security authentication fail-vlan コマンドはデフォルトに戻します。

組織のセキュリティ戦略に遵守できずに失敗したことが原因で WLAN 認証に失敗したクライアントに対応するため、クライアントを WLAN の制限 VLAN に収容することができます。例えば、間違ったパスワードやユーザ名を入力したクライアントに制限 VLAN が適応されます。制限 VLAN は認証タイムアウトあるいはネットワークの接続問題のために認証に失敗した WLAN クライアントに適応しません。

本コマンドは、サービステンプレートが無効なときに設定可能であり、サービステンプレートが有効になると適用されます。

例

サービステンプレート 1 で制限 VLAN として VLAN 10 を設定します。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] client-security authentication fail-vlan 10

5.1.5 client-security authentication-location

🕮 **メモ**：

ap パラメータは、ソフトウェアバージョン 7.2.27 を含む以降のソフトウェアからサポートしています。

Syntax

client-security authentication-location { **ac** | **ap** }

undo client-security authentication-location

デフォルト

AC が WLAN クライアント認証の認証装置として動作します。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

ac: AC を認証装置として指定します。

ap: AP を認証装置として指定します。

説明

client-security authentication-location コマンドは WLAN クライアントの認証装置を指定します。

undo client-security authentication-location コマンドはデフォルトに戻します。

クライアントのデータトラフィックを転送するように AC が設定されている場合は、AP を認証者として指定することはできません（**client forwarding-location** コマンドを使用）。**client forwarding-location** コマンドの詳細については、コマンドマニュアルのセクション 2 *WLAN “WLAN アクセスの設定”* を参照してください。

client-security authentication-location コマンドと **client association-location** コマンドでは同一の装置を指定してください。**client association-location** コマンドの詳細については、コマンドマニュアルのセクション 2 *WLAN* の“*WLAN アクセスの設定*”を参照してください。

本コマンドは、サービステンプレートが無効なときに設定可能であり、サービステンプレートが有効になると適用されます。

例

サービステンプレート **s1** で WLAN クライアントの認証装置として AC を設定します。

<AC> system-view

[AC] wlan service-template s1

[AC-wlan-st-s1] client-security authentication-location ac

関連コマンド

- **client forwarding-location**
- **client association-location** （コマンドマニュアルのセクション 2 *WLAN “WLAN アクセスの設定”*）

5.1.6 client-security authentication-mode

🕮 **メモ**：

- **mac-and-dot1x** パラメータは、ソフトウェアバージョン 7.1.11 を含む以降のソフトウェアからサポートしています。
- **mac-then-dot1x** と **dot1x-then-mac** のパラメータは、EAP relay では使用できません。

Syntax

client-security authentication-mode { **dot1x** | **dot1x-then-mac** | **mac** | **mac-then-dot1x** | **oui-then-dot1x** | **mac-and-dot1x** }

undo client-security authentication-mode

デフォルト

設定なし。装置は認証を実行しません（認証バイパスモード）。クライアントは直接装置にアクセスすることができます。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

dot1x: 802.1X 認証のみを実行します。

dot1x-then-mac: 最初に 802.1X 認証を実行し、次に MAC アドレス認証を実行します。クライアントが 802.1X 認証を通過した場合、MAC アドレス認証は実行されません。

mac: MAC アドレス認証のみを実行します。

mac-then-dot1x: 最初に MAC アドレス認証を実行し、次に 802.1X 認証を実行します。クライアントが MAC 認証を通過した場合、802.1X 認証は実行されません。

oui-then-dot1x: 最初に OUI 認証を実行し、次に 802.1X 認証を実行します。クライアントが OUI 認証を通過した場合、802.1X 認証は実行されません。

mac-and-dot1x: MAC アドレス認証と 802.1X 認証の２つの認証（マルチステップ認証）を実行します。MAC アドレス認証を最初に実行し、MAC アドレス認証にパスした場合のみ、802.1X 認証を実行します。２つの認証にパスしたクライアントの接続が許可されます。

説明

client-security authentication-mode コマンドは WLAN クライアントの認証モードを設定します。

undo client-security authentication-mode コマンドはデフォルトに戻します。

サービステンプレートはどの認証モードにおいても複数の認証モードへのアクセスを許可します。802.1X クライアントの最大数を設定するには、**dot1x max-user** コマンドを使用します。MAC アドレス認証クライアントの最大数を設定するには、**mac-authentication max-user** コマンドを使用します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

例

サービステンプレート **service1** でサービスにおける WLAN クライアントの認証モードを **mac** に設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security authentication-mode mac

5.1.7 client-security authorization-fail offline

Syntax

client-security authorization-fail offline

undo client-security authorization-fail offline

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

client-security authorization-fail offline コマンドは authentication-fail offline 機能を有効にします。

undo client-security authorization-fail offline コマンドは authentication-fail offline 機能を無効にします。

authorization-fail-offline 機能は ACL あるいはユーザプロファイルで許可されていない WLAN クライアントをログオフします。

以下の状況では、クライアントは ACL あるいはユーザプロファイルの許可に失敗します。

- 装置あるいはサーバは、クライアントに指定した ACL あるいはユーザプロファイルの許可に失敗する。
- 許可された ACL あるいはユーザプロファイルが存在しない。

本機能が無効の場合、装置は ACL あるいはユーザプロファイルの許可に失敗した WLAN クライアントをログオフしませんが、装置は失敗ログを残します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

例

サービステンプレート **service1** で authorization-fail-offline 機能を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security authorization-fail offline

5.1.8 client-security ignore-authorization

Syntax

client-security ignore-authorization

undo client-security ignore-authorization

デフォルト

装置はサーバから受け取った認証情報を使用します。

View

Service template view

定義済みユーザロール

network-admin

説明

client-security ignore-authorization コマンドは装置が認証サーバ（RADIUS サーバやローカル装置）から受信した許可情報を無視するよう設定します。

undo client-security ignore-authorization コマンドはデフォルトに戻します。

クライアントが RADIUS あるいはローカル認証を通過した後、サーバはユーザアカウントに設定された許可属性に基づいて許可を実行します。例えば、サーバは VLAN を割り当てることが可能です。装置にこれらのクライアント許可属性を使用させたくない場合、本コマンドを設定してサーバからの許可情報を無視するよう設定します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に効果が発生します。

例

サービステンプレート **service1** で認証サーバからの許可情報を無視するよう設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security ignore-authorization

5.1.9 client-security intrusion-protection action

Syntax

client-security intrusion-protection action { **service-stop** | **temporary-block** | **temporary-service-stop** }

undo client-security intrusion-protection action

デフォルト

temporary-block

View

Service template view

定義済みユーザロール

network-admin

パラメータ

service-stop: 無線インタフェースの BSS が手動で有効にされるまで、不正フレームが受信された BSS を停止します。

temporary-block: 一定期間、不正フレームの送信元 MAC アドレスをブロック MAC アドレスリストに追加します。期間の設定には **client-security intrusion-protection timer temporary-block** コマンドを使用します。

temporary-service-stop: 一定期間、不正フレームが受信された BSS を停止します。期間の設定には **intrusion-protection timer temporary-service-stop** コマンドを使用します。

説明

client-security authentication-mode コマンドは不正フレームを検出した場合に装置が実施する侵入保護アクションを設定します。

undo client-security intrusion-protection action コマンドはデフォルトに戻します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

本コマンドの効果を発生させるには、侵入保護機能を有効にするため、**client-security intrusion-protection enable** コマンドを使用する必要があります。

例

サービステンプレート **service1** で、侵入保護機能が不正フレームを検出した装置で BSS を停止するよう設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security intrusion-protection enable

[AC-wlan-st-service1] client-security intrusion-protection action service-stop

関連コマンド

- **client-security intrusion-protection enable**
- **client-security intrusion-protection timer temporary-block**
- **client-security intrusion-protection timer temporary-service-stop**

5.1.10 client-security intrusion-protection enable

Syntax

client-security intrusion-protection enable

undo client-security intrusion-protection enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

client-security intrusion-protection enable コマンドは侵入保護機能を有効にします。

undo client-security intrusion-protection enable コマンドは侵入保護機能を無効にします。

装置が不正なクライアントからの接続要求を受信した場合、要求を受信した BSS で事前定義された保護アクションを実行します。WLAN 認証に失敗した場合、その MAC アドレスのクライアントは不正クライアントになります。保護アクションを設定するには、**client-security intrusion-protection action** コマンドを使用します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

例

サービステンプレート **service1** で、侵入保護機能を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security intrusion-protection enable

関連コマンド

client-security intrusion-protection action

5.1.11 client-security intrusion-protection timer temporary-block

Syntax

client-security intrusion-protection timer temporary-block *time*

undo client-security intrusion-protection timer temporary-block

デフォルト

180 秒

View

Service template view

定義済みユーザロール

network-admin

パラメータ

time: MAC アドレスがブロックされる期間を指定します。範囲は 60～300 秒です。

説明

client-security intrusion-protection timer temporary-block コマンドは侵入保護によって MAC アドレスがブロックされる期間を設定します。

undo client-security intrusion-protection timer temporary-block コマンドはデフォルトに戻します。

本コマンドは侵入保護アクションが **temporary-block** の場合のみ有効です。

サービステンプレートを有効にした後にブロック期間を変更した場合、新しい設定は、その後に検出した不正パケットに対して適用されます。

例

サービステンプレート **service1** で、不正 MAC アドレスのブロック期間を 120 秒に設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security intrusion-protection enable

[AC-wlan-st-service1] client-security intrusion-protection action temporary-block

[AC-wlan-st-service1] client-security intrusion-protection timer temporary-block 120

関連コマンド

- **client-security intrusion-protection action**
- **client-security intrusion-protection enable**

5.1.12 client-security intrusion-protection timer temporary-service-stop

Syntax

client-security intrusion-protection timer temporary-service-stop *time*

undo client-security intrusion-protection timer temporary-service-stop

デフォルト

20 秒

View

Service template view

定義済みユーザロール

network-admin

パラメータ

time: BSS が停止する期間を指定します。範囲は 10～300 秒です。

説明

client-security intrusion-protection timer temporary-service-stop コマンドは侵入保護による BSS 停止期間を設定します。

undo client-security intrusion-protection timer temporary-service-stop コマンドはデフォルトに戻します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に効果が発生します。

サービステンプレートを有効にした後に BSS 停止期間を変更した場合、新しい設定は、その後に検出した不正パケットに対して適用されます。

例

サービステンプレート **service1** で、BSS 停止期間を 30 秒に設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security intrusion-protection enable

[AC-wlan-st-service1] client-security intrusion-protection action temporary-service-stop

[AC-wlan-st-service1] client-security intrusion-protection timer temporary-service-stop 30

関連コマンド

- **client-security intrusion-protection action**
- **client-security intrusion-protection enable**

5.1.13 display wlan client-security block-mac

Syntax

display wlan client-security block-mac [**ap** *ap-name* [**radio** *radio-id*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

radio *radio-id*: 無線を ID で指定します。無線 ID の値の範囲は AP モデルにより異なります。本オプションを指定しない場合、本コマンドは指定された AP のすべての無線についてブロックされた MAC アドレスの情報を表示します。

説明

display wlan client-security block-mac コマンドは WLAN クライアントのブロックされた MAC アドレス情報を表示します。

侵入保護アクションが **temporary-block** である場合、認証に失敗した MAC アドレスがブロック MAC アドレスリストに追加されます。

例

すべてのブロックされた MAC アドレス情報を表示します。

<AC> display wlan client-security block-mac

```
MAC address        AP ID      RADIO ID    BSSID
0002-0002-0002     1          1           00ab-0de1-0001
000d-88f8-0577     1          1           0ef1-0001-02c1


Total entries: 2
```

表 5-1 コマンド出力

フィールド	説明
MAC address	ブロックされたMACアドレス。（H-H-H形式）
AP ID	ブロックされたMACアドレスのAP ID
RADIO ID	ブロックされたMACアドレスの無線ID
BSSID	ブロックされたMACアドレスのBSS-ID（H-H-H形式）
Total entries	ブロックされたMACアドレスの数

関連コマンド

- **client-security intrusion-protection action**
- **client-security intrusion-protection timer temporary-block**

5.1.14 dot1x domain

Syntax

dot1x domain *domain-name*

undo dot1x domain

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

domain-name: ISP ドメイン名を指定します。設定範囲は 1～255 文字です。大文字小文字を区別ません。

説明

dot1x domain コマンドはサービステンプレートで 802.1X クライアントのための認証ドメインを指定します。

undo dot1x domain コマンドはデフォルトに戻します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に効果が発生します。

802.1X は以下の順番で WLAN クライアントのための認証ドメインを選択します。

1) サービステンプレートで指定された認証ドメイン
2) ユーザ名で指定されたドメイン
3) デフォルト認証ドメイン

例

サービステンプレート **service1** で、802.1X クライアントのための認証ドメインとして **my-domain** を指定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] dot1x domain my-domain

5.1.15 dot1x handshake enable

Syntax

dot1x handshake enable

undo dot1x handshake enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

dot1x handshake enable コマンドは 802.1X オンラインユーザハンドシェイク機能を有効にします。

undo dot1x handshake enable コマンドは 802.1X オンラインユーザハンドシェイク機能を有効にします。

オンラインユーザハンドシェイク機能は、定期的にクライアントにハンドシェイクメッセージを送信することにより、オンライン 802.1X クライアントの接続状態を確認します。最大ハンドシェイク試行回数に到達してもハンドシェイクタイマ内にクライアントから応答を受信しない場合、装置はクライアントをオフライン状態にします。ハンドシェイクタイマの設定には、**dot1x timer handshake-period** コマンドを使用します。最大ハンドシェイク試行回数の設定には、**dot1x retry** コマンドを使用します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます

例

サービステンプレート **service1** で、802.1X クライアントのためのオンラインユーザハンドシェイク機能を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] dot1x handshake enable

関連コマンド

- **dot1x handshake secure enable**
- **dot1x retry**（コマンドマニュアルのセクション 9 *セキュリティ “802.1X”*）
- **dot1x timer handshake-period**（コマンドマニュアルのセクション 9 *セキュリティ “802.1X”*）

5.1.16 dot1x handshake secure enable

Syntax

dot1x handshake secure enable

undo dot1x handshake secure enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

dot1x handshake secure enable コマンドは 802.1X オンラインユーザハンドシェイクセキュリティ機能を有効にします。

undo dot1x handshake secure enable コマンドは 802.1X オンラインユーザハンドシェイクセキュリティ機能を無効にします。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に効果が発生します。

オンラインユーザハンドシェイクセキュリティ機能を有効にするには、オンラインユーザハンドシェイク機能が有効になっている必要があります。

オンラインユーザハンドシェイクセキュリティ機能は、認証されたオンラインの 802.1X クライアントのみを保護します。

例

サービステンプレート **service1** で、802.1X クライアントのためのオンラインユーザハンドシェイクセキュリティ機能を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] dot1x handshake enable

[AC-wlan-st-service1] dot1x handshake secure enable

関連コマンド

dot1x handshake enable

5.1.17 dot1x max-user

Syntax

dot1x max-user *count*

undo dot1x max-user

デフォルト

512

View

Service template view

定義済みユーザロール

network-admin

パラメータ

count: 同時接続 802.1X クライアントの最大数を設定します。範囲は 1～512 です。

説明

dot1x max-user コマンドはサービステンプレートで 802.1X クライアントの最大同時接続数を設定します。

undo dot1x max-user コマンドはデフォルトに戻します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

最大数に達した場合、サービステンプレートは以降の 802.1X クライアントを拒否します。

🕮 **メモ：**

- 802.1X 認証クライアント同時接続数を、サービステンプレートを設定した無線インタフェースごとに制限します。
- 1 つの無線インタフェースで同時に接続可能なクライアント最大数は、QX-W1200 シリーズは 512、QX-W1100 シリーズは 512、QX-W1000 シリーズは 256 です。
- 無線インタフェースで同時に接続可能なクライアント最大数を超えて接続することはできません。

例

サービステンプレート **service1** で、802.1X クライアントの最大接続数を 500 に設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] dot1x max-user 500

5.1.18 dot1x re-authenticate enable

Syntax

dot1x re-authenticate enable

undo dot1x re-authenticate enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

dot1x re-authenticate enable コマンドはサービステンプレートで 802.1X クライアントの定期的なオンラインユーザ再認証機能を有効にします。

undo dot1x re-authenticate enable コマンドはデフォルトに戻します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

定期的再認証により、サービステンプレートにおいてオンラインの 802.1X クライアントを装置が定期的に認証することが可能になります。本機能はオンラインクライアントの接続状態を確認し、サーバによって割り当てられた許可属性をアップデートします。属性には ACL、VLAN ベースのユーザプロファイルが含まれます。

dot1x timer reauth-period コマンドにより、再認証の間隔を設定することができます。

サーバによって割り当てられた RADIUS 属性の Session-Timeout、Termination-Action は、定期的なオンラインユーザの再認証に影響します。サーバによって割り当てられた Session-Timeout、Termination-Action を表示するには、**display dot1x connection** コマンドを使用します（コマンドマニュアルのセクション 9 *セキュリティ “802.1X”* を参照してください）。

- Termination-Action が **Default**（ログオフ）の場合、テンプレート内のオンラインユーザ再認証は、定期的再認証タイマがセッションタイムアウトタイマよりも小さい場合のみ適用されます。
- Termination-Action が **Radius-request** の場合、テンプレート内のオンラインユーザ再認証は動作しません。装置は、セッションタイムアウトタイマの期限切れ後にオンライン 802.1X クライアントを再認証します。

例

サービステンプレート **service1** で、802.1X クライアントの定期的再認証機能を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] dot1x re-authenticate enable

関連コマンド

dot1x timer（コマンドマニュアルのセクション 9 *セキュリティ “802.1X”*）

5.1.19 fail-permit enable

🕮 **メモ**：

- このコマンドはソフトウェアバージョン 7.2.21 を含む以降のソフトウェアからサポートしています。
- **hybrid remote-ap enable** コマンドが設定されている AP では、AP が AC と通信不能になっても、失敗許可機能は使用できません。

Syntax

fail-permit enable [**keep-online**]

undo fail-permit enable

デフォルト

無効

Views

Service template view

定義済みユーザロール

network-admin

パラメータ

keep-online: 失敗許可機能が動作する際、オンラインのクライアントが切断されるのを防ぎます。

説明

fail-permit enable コマンドは失敗許可機能を有効にします。

undo fail-permit enable コマンドは失敗許可機能を無効にします。

失敗許可機能は以下の目的で使用します。

- **認証失敗許可**—RADIUS サーバもしくは AC と AP が切断されたあと、802.1X 認証、MAC 認証、もしくは PSK 認証クライアントがネットワークにアクセスできるようになります。RADIUS サーバもしくは AC との切断が発生すると、AP はクライアントに対して継続してアクセスサービスを提供し、トラフィックを転送します。

fail-permit enable コマンドは、サービステンプレートが無効になっている場合にのみ実行でき、サービステンプレートが有効になった後に有効になります。

fail-permit enable コマンドと **fail-permit template** コマンドを同一のサービステンプレートに設定しないでください。

例

#サービステンプレートをで失敗許可機能を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] fail-permit enable

関連コマンド

fail-permit template

5.1.20 fail-permit template

🕮 **メモ**:

- このコマンドはソフトウェアバージョン 7.2.18 を含む以降のソフトウェアからサポートしています。
- 802.1X 認証での失敗許可機能はソフトウェアバージョン 7.2.27 を含む以降のソフトウェアからサポートしています。
- 1 つの無線に対して設定できるバックアップ用のサービステンプレート(SSID)は 1 つのみです。

Syntax

fail-permit template

undo fail-permit template

デフォルト

設定なし

Views

Service template view

定義済みユーザロール

network-admin

説明

fail-permit template コマンドはレーダーによる通信停止回避のため、もしくは 802.1X 認証での失敗許可機能のためのバックアップ用サービステンプレートとして指定します。

undo fail-permit template コマンドはレーダーによる通信停止回避のため、もしくは 802.1X 認証での失敗許可機能のためのバックアップ用サービステンプレート指定を削除します。

レーダーによる通信停止回避を行うためには 1 つのサービステンプレートに対して、1 つのバックアップ用のサービステンプレートを用意します。

- バックアップ用サービステンプレートには、fail-permit service template コマンドを追加する点を除き、オリジナルのサービステンプレートと同じ設定を含める必要があります。
- バックアップ用サービステンプレートは、オリジナルのサービステンプレートとは異なる無線にバインドする必要があります。

802.1X 認証で失敗許可機能を使用する場合、サービステンプレートを 2 つ設定します。1 つのサービステンプレートには 802.1X 認証の設定および **fail-permit enable** コマンドを設定します。もう一方のサービステンプレートにはバックアップ用に PSK 認証もしく

は 802.1X 認証および **fail-permit template** コマンドを設定します。AP が AC もしくは RADIUS サーバと通信不能になるまではバックアップ用の SSID は表示されません。AP が AC と通信不能になってから、もしくは RADIUS サーバと通信不能になってから数分後に失敗許可機能が動作します。接続済みのクライアントは接続を維持します。新規クライアントは、失敗許可機能動作後に接続可能です。AC もしくは RADIUS サーバと AP の切断前は、クライアントは 802.1X 認証で認証されます。切断後はバックアップ用の PSK 認証で認証されます。

fail-permit template コマンドは、サービステンプレートが無効になっている場合にのみ実行でき、サービステンプレートが有効になった後に有効になります。

fail-permit template コマンドと **fail-permit enable** コマンドを同一のサービステンプレートに設定しないでください。

例

#サービステンプレートを障害許可サービステンプレートとして指定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] fail-permit template

関連コマンド

fail-permit enable

5.1.21 mac-authentication domain

Syntax

mac-authentication domain *domain-name*

undo mac-authentication domain

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

domain-name: ISP ドメイン名を指定します。設定範囲は 1～255 文字です。大文字と小文字を区別しません。

説明

mac-authentication domain コマンドはサービステンプレートで MAC 認証クライアントのための認証ドメインを指定します。

undo mac-authentication domain コマンドはデフォルトに戻します

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

MAC 認証は以下の順番で WLAN クライアントのための認証ドメインを選択します。

1) サービステンプレートで指定された認証ドメイン
2) ユーザ名で指定されたドメイン
3) デフォルト認証ドメイン

例

サービステンプレート **service1** で、MAC 認証クライアントのための認証ドメインとして **my-domain** を指定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] mac-authentication domain my-domain

5.1.22 mac-authentication fast-connect enable

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.46 を含む以降のソフトウェアからサポートしています。

Syntax

mac-authentication fast-connect enable

undo mac-authentication fast-connect enable

デフォルト

有効

View

Service template view

定義済みユーザロール

network-admin

説明

mac-authentication fast-connect enable コマンドは、MAC 認証クライアントのための AC 内ローミング高速接続を有効にします。

undo mac-authentication fast-connect enable コマンドは、MAC 認証クライアントのための AC 内ローミング高速接続を無効にします。

本コマンドを有効にすることで、AC で MAC 認証されたクライアントが、同じ AC に管理された別の AP に移動する際、再認証なしでローミングできるようになります。

本機能は MAC 認証を利用する無線クライアントにのみ適用され、authentication-location と association-location はどちらも AC である必要があります。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

例

サービステンプレート **service1** で、MAC 認証クライアントのための AC 内ローミング高速接続を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] mac-authentication fast-connect enable

関連コマンド

- **client-security authentication-mode**
- **client-security authentication-location**
- **client association-location** （コマンドマニュアルのセクション 2 *WLAN “WLAN アクセスの設定”*）

5.1.23 mac-authentication max-user

Syntax

mac-authentication max-user *count*

undo mac-authentication max-user

デフォルト

512

View

Service template view

定義済みユーザロール

network-admin

パラメータ

count: 同時接続 MAC 認証クライアントの最大数を設定します。範囲は 1～512 です。

説明

mac-authentication max-user コマンドはサービステンプレートで MAC 認証クライアントの最大同時接続数を設定します。

undo mac-authentication max-user コマンドはデフォルトに戻します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

最大数に達した場合、サービステンプレートは以降の MAC 認証クライアントを拒否します。

🕮 **メモ**:

- MAC 認証クライアント同時接続数を、サービステンプレートを設定した無線インタフェースごとに制限します。
- 1 つの無線インタフェースで同時に接続可能なクライアント最大数は、QX-W1200 シリーズは 512、QX-W1100 シリーズは 512、QX-W1000 シリーズは 256 です。
- 無線インタフェースで同時に接続可能なクライアント最大数を超えて接続することはできません。

例

サービステンプレート **service1** で、MAC 認証クライアントの最大接続数を 32 に設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] mac-authentication max-user 32

5.1.24 port-security oui

Syntax

port-security oui index *index-value* **mac-address** *oui-value*

undo port-security oui index *index-value*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

index-value: OUI 値を 1～16 の範囲で設定します。

oui-value: OUI 文字列、すなわち H-H-H フォーマットの 48 ビット MAC アドレスを指定します。システムは、上位 24 ビットのみを OUI 値として使用します。

説明

port-security oui コマンドは OUI 認証用の OUI 値を設定します。

undo port-security oui コマンドは指定した OUI 値を削除します。

OUI（MAC アドレスの最初の 24 バイナリビット）は、IEEE によってデバイスベンダを一意に識別するために割り当てられます。特定の無線デバイスからのパケットが認証を開始できるようにデバイスを設定する場合、このコマンドを使用します。たとえば、企業がイントラネット内のベンダ A の IP 電話だけを許可する場合、このコマンドを使用して、ベンダ A の OUI を指定します。

このコマンドを使用して設定された OUI 値は、認証モードが oui-or-dot1x の場合にのみ適用されます。oui-or-dot1x モードのポートは、1 つの 802.1X 認証ユーザからのフレームと、MAC アドレスが特定の OUI を含む 1 人のユーザからのフレームを許可します。

例

OUI 値 000d2a をセットし、インデックスを 4 に設定します。

<AC> system-view

[AC] port-security oui index 4 mac-address 000d-2a10-003

5.1.25 radius-server test-profile

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.21 を含む以降のソフトウェアからサポートしています。

Syntax

ソフトウェアバージョン 7.2.89 を含む以降のソフトウェア

radius-server test-profile *profile-name* **username** *name* [**interval** [**second**] *interval*]

undo radius-server test-profile *profile-name*

ソフトウェアバージョン 7.2.85a を含む以前のソフトウェア

radius-server test-profile *profile-name* **username** *name* [**interval** *interval*]

undo radius-server test-profile *profile-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

profile-name: テストプロファイルの名前を指定します。大文字と小文字を区別します。文字数は 1～31 文字です。

username *name*: 検出パケット内のユーザ名を指定します。*name* パラメータは大文字と小文字を区別し、1～253 文字で指定します。

interval *interval*: 検出パケットを送信する間隔を分で設定します。*Interval* パラメータの値の範囲は 1～3600 で、デフォルトは 60 です。

second: 検出パケットを送信する間隔を秒で設定します。このパラメータを指定した場合、*interval* パラメータの値の範囲は 10～216000 です。

🕮 **メモ：**

second パラメータはソフトウェアバージョン 7.2.89 を含む以降のソフトウェアからサポートしています。

説明

radius-server test-profile コマンドは RADIUS サーバの状態を検出するためのテストプロファイルを設定します。

undo radius-server test-profile コマンドはテストプロファイルを削除します。

装置は、サーバに対して指定されたテストプロファイルが存在する場合にのみ、RADIUS サーバの状態検出を開始します。存在しないテストプロファイルを RADIUS サーバに対して指定した場合、装置上にテストプロファイルを作成するまで、装置はサーバの状態を検出しません。

テストプロファイルを削除すると、装置は削除したテストプロファイルを使用していた RADIUS サーバの状態の検出を停止します。

このコマンドを複数回実行することで、複数のテストプロファイルを設定できます。

例

RADIUS サーバの状態を検出するためにテストプロファイル **abc** を設定します。ユーザ名 **admin** を使用した検出パケットを 10 分ごとに送信します。

<AC> system-view

[AC] radius-server test-profile abc username admin interval 10

関連コマンド

- **primary authentication**（コマンドマニュアルのセクション 9 *セキュリティ "AAA"*）
- **secondary authentication**（コマンドマニュアルのセクション 9 *セキュリティ "AAA"*）

5.2 Web認証(ポータル認証)設定コマンド

Web 認証(ポータル認証)の設定に関するコンフィグについては、別紙の共通マニュアル"*QX-W シリーズ Web 認証(ポータル認証)コマンドマニュアル*"を参照してください。

目次

このセクションのページは **2-x-x** です。

6 章 WIPS の設定 6-1
6.1 WIPS の設定コマンド 6-1
6.1.1 ap-channel-change 6-1
6.1.2 ap-classification rule 6-2
6.1.3 ap-flood 6-2
6.1.4 ap-impersonation 6-3
6.1.5 apply ap-classification rule 6-4
6.1.6 apply classification policy 6-5
6.1.7 apply countermeasure policy 6-6
6.1.8 apply detect policy 6-7
6.1.9 apply signature policy 6-8
6.1.10 apply signature rule 6-8
6.1.11 ap-rate-limit 6-9
6.1.12 ap-spoofing 6-10
6.1.13 ap-timer 6-11
6.1.14 association-table-overflow 6-12
6.1.15 authentication 6-13
6.1.16 block mac-address 6-14
6.1.17 classification policy 6-15
6.1.18 client-online 6-16
6.1.19 client-rate-limit 6-17
6.1.20 client-spoofing 6-18
6.1.21 client-timer 6-18
6.1.22 countermeasure adhoc 6-20
6.1.23 countermeasure attack all 6-20
6.1.24 countermeasure attack deauth-broadcast 6-21
6.1.25 countermeasure attack disassoc-broadcast 6-22
6.1.26 countermeasure attack honeypot-ap 6-23
6.1.27 countermeasure attack hotspot-attack 6-23
6.1.28 countermeasure attack ht-40-mhz-intolerance 6-24
6.1.29 countermeasure attack malformed-packet 6-25
6.1.30 countermeasure attack man-in-the-middle 6-25
6.1.31 countermeasure attack omerta 6-26
6.1.32 countermeasure attack power-save 6-27
6.1.33 countermeasure attack soft-ap 6-28
6.1.34 countermeasure attack unencrypted-trust-client 6-28

6.1.35 countermeasure attack weak-iv 6-29
6.1.36 countermeasure attack windows-bridge 6-30
6.1.37 countermeasure external-ap 6-30
6.1.38 countermeasure mac-address 6-31
6.1.39 countermeasure misassociation-client 6-32
6.1.40 countermeasure misconfigured-ap 6-33
6.1.41 countermeasure policy 6-33
6.1.42 countermeasure potential-authorized-ap 6-34
6.1.43 countermeasure potential-external-ap 6-35
6.1.44 countermeasure potential-rogue-ap 6-36
6.1.45 countermeasure rogue-ap 6-36
6.1.46 countermeasure unauthorized-client 6-37
6.1.47 countermeasure uncategorized-ap 6-38
6.1.48 countermeasure uncategorized-client 6-38
6.1.49 deauthentication-broadcast 6-39
6.1.50 detect policy 6-40
6.1.51 detect signature 6-41
6.1.52 disassociation-broadcast 6-42
6.1.53 detect dissociate-client enable 6-43
6.1.54 discovered-ap 6-44
6.1.55 display wips sensor 6-45
6.1.56 display wips statistics 6-45
6.1.57 display wips virtual-security-domain countermeasure record 6-51
6.1.58 display wips virtual-security-domain device 6-52
6.1.59 display wlan nat-detect 6-58
6.1.60 flood association-request 6-59
6.1.61 flood authentication 6-60
6.1.62 flood beacon 6-61
6.1.63 flood block-ack 6-62
6.1.64 flood cts 6-63
6.1.65 flood deauthentication 6-64
6.1.66 flood disassociation 6-65
6.1.67 flood eap-failure 6-66
6.1.68 flood eapol-logoff 6-67
6.1.69 flood eapol-start 6-68
6.1.70 flood eap-success 6-69
6.1.71 flood null-data 6-70
6.1.72 flood probe-request 6-71
6.1.73 flood reassociation-request 6-72
6.1.74 flood rts 6-73
6.1.75 frame-type 6-74
6.1.76 honeypot-ap 6-76
6.1.77 hotspot-attack 6-76

6.1.78 ht-40mhz-intolerance 6-77
6.1.79 ht-greenfield 6-78
6.1.80 ignorelist 6-79
6.1.81 import hotspot 6-80
6.1.82 import oui 6-81
6.1.83 invalid-oui-classify illegal 6-82
6.1.84 mac-address 6-82
6.1.85 malformed duplicated-ie 6-83
6.1.86 malformed fata-jack 6-84
6.1.87 malformed illegal-ibss-ess 6-85
6.1.88 malformed invalid-address-combination 6-86
6.1.89 malformed invalid-assoc-req 6-87
6.1.90 malformed invalid-auth 6-88
6.1.91 malformed invalid-deauth-code 6-89
6.1.92 malformed invalid-disassoc-code 6-90
6.1.93 malformed invalid-ht-ie 6-91
6.1.94 malformed invalid-ie-length 6-92
6.1.95 malformed invalid-pkt-length 6-93
6.1.96 malformed large-duration 6-94
6.1.97 malformed null-probe-resp 6-95
6.1.98 malformed overflow-eapol-key 6-96
6.1.99 malformed overflow-ssid 6-97
6.1.100 malformed redundant-ie 6-98
6.1.101 man-in-the-middle 6-98
6.1.102 manual-classify mac-address 6-99
6.1.103 omerta 6-100
6.1.104 oui 6-101
6.1.105 pattern 6-102
6.1.106 permit-channel 6-103
6.1.107 power-save 6-104
6.1.108 prohibited-channel 6-105
6.1.109 report-interval 6-106
6.1.110 reset wips statistics 6-107
6.1.111 reset wips virtual-security-domain 6-108
6.1.112 reset wips virtual-security-domain countermeasure record 6-109
6.1.113 reset wlan nat-detect 6-109
6.1.114 rssi 6-110
6.1.115 rssi-change-threshold 6-111
6.1.116 rssi-threshold 6-111
6.1.117 security 6-112
6.1.118 select sensor all 6-113
6.1.119 seq-number 6-114
6.1.120 signature policy 6-115

6.1.121 signature rule 6-115
6.1.122 soft-ap 6-116
6.1.123 ssid (AP classification rule view) 6-117
6.1.124 ssid (signature view) 6-118
6.1.125 ssid-length 6-119
6.1.126 trust mac-address 6-120
6.1.127 trust oui 6-120
6.1.128 trust ssid 6-121
6.1.129 unencrypted-authorized-ap 6-122
6.1.130 unencrypted-trust-client 6-123
6.1.131 up-duration 6-124
6.1.132 virtual-security-domain 6-125
6.1.133 weak-iv 6-125
6.1.134 windows-bridge 6-126
6.1.135 wips 6-127
6.1.136 wips enable 6-128
6.1.137 wips virtual-security-domain 6-129
6.1.138 wireless-bridge 6-130
6.1.139 wlan nat-detect 6-130

6章 WIPS の設定

6.1 WIPSの設定コマンド

6.1.1 ap-channel-change

Syntax

ap-channel-change [**quiet** *quiet-value*]

undo ap-channel-change

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がチャネル変更のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にチャネル変更を検出してもアラームを引き起こしません。

説明

ap-channel-change コマンドはチャネル変更の設定をします。

undo ap-channel-change コマンドはチャネル変更の検出を無効にします。

例

チャネル変更の検出を有効にし、遅延時間を 5 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ap-channel-change quiet 5

6.1.2 ap-classification rule

Syntax

ap-classification rule *rule-id*

undo ap-classification rule *rule-id*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

rule-id: ID で AP 分類ルールを指定します。値の範囲は 1～65535 です。

説明

ap-classification rule コマンドは AP 分類ルールを作成し、その view に移行します。AP 分類ルールがすでに存在する場合、**ap-classification rule** コマンドで AP classification rule view に移行します。

undo ap-classification rule コマンドは AP 分類ルールを削除します。

例

AP classification rule 1 を作成し、その view に移行します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

6.1.3 ap-flood

Syntax

ap-flood [**apnum** *apnum-value* | **exceed** *exceed-value* | **quiet** *quiet-value*] *

undo ap-flood

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

apnum *apnum-value*: AP 数しきい値を指定します。値の範囲は 10～200 です。デフォルト値は 80 です。

exceed *exceed-value*: 超過を許可された AP の最大数を指定します。*exceed-value* 引数の値の範囲は 10～200 です。デフォルト値は 80 です。AP の数が、AP 数しきい値と、超過を許可された AP の最大数の合計を超える場合、WIPS は AP フラッド攻撃アラームを引き起こします。

quiet *quiet-value*: WIPS が AP フラッド攻撃アラームを引き起こした後、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルト時間は 600 秒です。WIPS は遅延時間内に AP フラッド攻撃を検出してもアラームを引き起こしません。

説明

ap-flood コマンドは AP フラッド攻撃検出を設定します。

undo ap-flood コマンドは AP フラッド攻撃検出を無効にします。

例

AP フラッド攻撃検出を有効にし、*apnum-value*、*exceed-value*、*quiet-value* をそれぞれ 50、50、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ap-flood apnum 50 exceed 50 quiet 100

6.1.4 ap-impersonation

Syntax

ap-impersonation [**quiet** *quiet-value*]

undo ap-impersonation

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が AP なりすまし攻撃アラームを引き起こした後、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルト時間は 600 秒です。WIPS は遅延時間内に AP なりすまし攻撃を検出してもアラームを引き起こしません。

説明

ap-impersonation コマンドは AP なりすまし攻撃検出を設定します。

undo ap-impersonation コマンドはデフォルトに戻します。

例

AP なりすまし攻撃検出を有効にし、遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ap-impersonation quiet 360

6.1.5 apply ap-classification rule

Syntax

apply ap-classification rule *rule-id* { **authorized-ap** | { { **external-ap** | **misconfigured-ap** | **rogue-ap** } [**severity-level** *level*] } }

undo apply ap-classification rule *rule-id*

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

rule-id: ID で AP 分類ルールを指定します。ID の値の範囲は 1～65535 です。

authorized-ap: 許可された AP として AP 分類ルールに一致する AP を指定します。

external-ap: 外部 AP

misconfigured-ap: 不良コンフィグレーション AP として AP 分類ルールに一致する AP を指定します。

rogue-ap: 不正な AP として AP 分類ルールに一致する AP を指定します。

level: AP 分類ルールに一致する AP に対して重大度レベルを指定します。レベルの範囲は 1～100 です。デフォルトレベルは 50 です。

説明

apply ap-classification rule コマンドは分類ポリシに AP 分類ルールを設定します。

undo apply ap-classification rule コマンドはデフォルトに戻します。

例

分類ポリシ **home** に AP classification rule 1 を設定します。不正な AP として AP classification rule 1 に一致する AP を指定します。重大度レベルを 80 に設定します。

<AC> system-view

[AC] wips

[AC-wips] classification policy home

[AC-wips-cls-home] apply ap-classification rule 1 rogue-ap severity-level 80

関連コマンド

ap-classification rule

6.1.6 apply classification policy

Syntax

apply classification policy *policy-name*

undo apply classification policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザロール

network-admin

パラメータ

policy-name: 分類ポリシの名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

apply classification policy コマンドは分類ポリシを VSD（Virtual Security Domain）に適用します。

undo apply classification policy コマンドは VSD から分類ポリシを削除します。

例

分類ポリシ **policy1** を VSD **home** に適用します。

<AC> system-view

[AC] wips

[AC-wips] virtual-security-domain home

[AC-wips-vsd-home] apply classification policy policy1

6.1.7 apply countermeasure policy

Syntax

apply countermeasure policy *policy-name*

undo apply countermeasure policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザロール

network-admin

パラメータ

policy-name: 対策ポリシの名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

apply countermeasure policy コマンドは対策ポリシを VSD（Virtual Security Domain）に適用します。

undo apply countermeasure policy コマンドは VSD から対策ポリシを削除します。

例

対策ポリシ **policy2** を VSD **home** に適用します。

<AC> system-view

[AC] wips

[AC-wips] virtual-security-domain home

[AC-wips-vsd-home] apply countermeasure policy policy2

6.1.8 apply detect policy

Syntax

apply detect policy *policy-name*

undo apply detect policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザロール

network-admin

パラメータ

policy-name: 分類ポリシの名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

apply detect policy コマンドは攻撃検出ポリシを VSD に適用します。

undo apply detect policy コマンドは VSD から攻撃検出ポリシを削除します。

例

攻撃検出ポリシ **policy2** を VSD **home** に適用します。

<AC> system-view

[AC] wips

[AC-wips] virtual-security-domain home

[AC-wips-vsd-home] apply detect policy policy2

6.1.9 apply signature policy

Syntax

apply signature policy *policy-name*

undo apply signature policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザロール

network-admin

パラメータ

policy-name: 分類ポリシの名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

apply signature policy コマンドは署名ポリシを VSD に適用します。

undo apply signature policy コマンドはデフォルトに戻します。

例

署名ポリシ **policy1** を VSD **home** に適用します。

<AC> system-view

[AC] wips

[AC-wips] virtual-security-domain home

[AC-wips-vsd-home] apply signature policy policy1

6.1.10 apply signature rule

Syntax

apply signature rule *rule-id*

undo apply signature rule *rule-id*

デフォルト

設定なし

View

Signature policy view

定義済みユーザロール

network-admin

パラメータ

rule-id: ID で署名を指定します。値の範囲は 1～65535 文字です。

説明

apply signature rule コマンドは署名ポリシに署名を設定します。

undo apply signature rule コマンドはデフォルトに戻します。

例

signature 1 を署名ポリシ **office** に設定します。

<AC> system-view

[AC] wips

[AC-wips] signature policy office

[AC-wips-sig-office] apply signature rule 1

6.1.11 ap-rate-limit

Syntax

ap-rate-limit [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo ap-rate-limit

デフォルト

学習した AP エントリのための統計値収集間隔：60 秒

遅延時間：1200 秒

AP エントリしきい値：64

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 学習した AP エントリのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。

quiet *quiet-value*: WIPS が AP エントリ攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 1200～3600 秒です。WIPS は遅延時間内に AP エントリ攻撃を検出してもアラームを引き起こさず、AP エントリ学習を停止します。

threshold t*hreshold-value*: AP エントリ攻撃アラームを引き起こす AP エントリ数を指定します。*threshold-value* 引数の値の範囲は 1～4096 です。

説明

ap-rate-limit コマンドは AP エントリの学習を制限します。

undo ap-rate-limit コマンドはデフォルトに戻します。

例

AP エントリの学習を制限します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ap-rate-limit interval 60 quiet 1600 threshold 100

6.1.12 ap-spoofing

Syntax

ap-spoofing [**quiet** *quiet-value*]

undo ap-spoofing

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が AP スプーフィング攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトの遅延時

間は 600 秒です。WIPS は遅延時間内に AP エントリ攻撃を検出してもアラームを引き起こしません。

説明

ap-spoofing コマンドは AP スプーフィング攻撃を有効にします。

undo ap-spoofing コマンドは AP スプーフィング攻撃を無効にします。

例

AP スプーフィング検出を有効にし、遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ap-spoofing quiet 360

6.1.13 ap-timer

🕮 **メモ：**

inactive-value 引数と aging-value 引数の下限値が Version 7.1.13 を含む以降のソフトウェアから変更されました。

Syntax

ap-timer [**inactive** *inactive-value* **aging** *aging-value*]

undo ap-timer

デフォルト

非アクティブ時間： 300 秒

エージングタイマ： 600 秒

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

inactive *inactive-value*: 非アクティブ時間を指定します。指定された非アクティブ時間内に AP がフレームを送受信しない場合、WIPS は AP を非アクティブ状態に設定します。

Version 7.1.13 を含む以降のソフトウェア

inactive-value 引数の値の範囲は 1～1200 秒です。

Version 7.1.11 を含む以前のソフトウェア

inactive-value 引数の値の範囲は 60～1200 秒です。

aging *aging-value*: エージングタイマを指定します。指定されたエージングタイマ内に AP がフレームを送受信しない場合、WIPS はエントリを削除します。エージングタイマは非アクティブ時間より大きくなければなりません。

Version 7.1.13 を含む以降のソフトウェア

aging-value 引数の値の範囲は 1～86400 秒です。

Version 7.1.11 を含む以前のソフトウェア

aging-value 引数の値の範囲は 120～86400 秒です。

説明

ap-timer コマンドは AP エントリタイマを設定します。

undo ap-timer コマンドはデフォルトに戻します。

例

非アクティブ時間を 120 秒、エージングタイマを 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ap-timer inactive 120 aging 360

6.1.14 association-table-overflow

Syntax

association-table-overflow [**quiet** *quiet-value*]

undo association-table-overflow

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がアソシエーション/再アソシエーション DoS 攻撃アラームを引き起こした後、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトの遅延時間は 600 秒です。WIPS は遅延時間内にアソシエーション/再アソシエーション DoS 攻撃を検出してもアラームを引き起こしません。

説明

association-table-overflow コマンドはアソシエーション/再アソシエーション DoS 攻撃検出を設定します。

undo association-table-overflow コマンドはアソシエーション/再アソシエーション DoS 攻撃検出を無効にします。

例

アソシエーション/再アソシエーション DoS 攻撃検出を有効にし、遅延時間を 100 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] association-table-overflow quiet 100

6.1.15 authentication

Syntax

authentication { **equal** | **include** } { **802.1x** | **none** | **other** | **psk** }

undo authentication

デフォルト

一致なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

equal: 指定された認証モードと等しい認証モードを整合します。

include: 指定された認証モードを含む認証モードを整合します。

802.1x: 802.1X 認証モードを指定します。

none: 認証モードは指定されません。

other: 802.1X と PSK 以外の認証モードを指定します。

psk: PSK 認証モードを指定します。

説明

authentication コマンドは AP の認証モードを整合するために AP 分類ルールを設定します。

undo authentication コマンドはデフォルトに戻します。

例

PSK 認証モードを使用する AP を整合するために AP classification rule 1 を設定します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

[AC-wips-cls-rule-1] authentication equal psk

6.1.16 block mac-address

Syntax

block mac-address *mac-address*

undo block mac-address { *mac-address* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

mac-address: AP の無線 MAC アドレス(BSSID)もしくはクライアントの MAC アドレスを H-H-H 形式で指定します。

all: すべての MAC アドレスを指定します。

説明

block mac-address コマンドはスタティック禁止装置リストに MAC アドレスを追加します。

undo block mac-address コマンドはスタティック禁止装置リストから 1 つもしくはすべての MAC アドレスを削除します。

例

スタティック禁止装置リストに MAC アドレス **78AC-C0AF-944F** を追加します。

<AC> system-view

[AC] wips

[AC-wips] classification policy home

[AC-wips-cls-home] block mac-address 78AC-C0AF-944F

6.1.17 classification policy

Syntax

classification policy *policy-name*

undo classification policy *policy-name*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

policy-name: 分類ポリシの名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

classification policy コマンドは分類ポリシを作成し、その view に移行します。

undo classification policy コマンドは分類ポリシを削除します。

例

分類ポリシ **home** を作成し、その view に移行します。

<AC> system-view

[AC] wips

[AC-wips] classification policy home

[AC-wips-cls-home]

6.1.18 client-online

Syntax

client-online *value1* [**to** *value2*]

undo client-online

デフォルト

一致なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

value1 **to** *value2*: AP に紐付けられたクライアント数の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、どちらも 0～128 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

説明

client-online コマンドは AP に紐付いたクライアント数を整合するために AP 分類ルールを設定します。

undo client-online コマンドはデフォルトに戻します。

例

20～40 のクライアントに紐付いた AP を整合するために、AP classification rule 1 を設定します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

[AC-wips-cls-rule-1] client-online 20 to 40

6.1.19 client-rate-limit

Syntax

client-rate-limit [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo client-rate-limit

デフォルト

学習したクライアントエントリのための統計値収集間隔：60 秒

遅延時間：1200 秒

クライアントエントリしきい値：512

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 学習したクライアントエントリのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。

quiet *quiet-value*: WIPS がクライアントエントリ攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 1200～3600 秒です。WIPS は遅延時間内にクライアントエントリ攻撃を検出してもアラームを引き起こさず、AP エントリ学習を停止します。

threshold *threshold-value*: クライアントエントリ攻撃アラームを引き起こすクライアントエントリ数を指定します。*threshold-value* 引数の値の範囲は 1～4096 です。

説明

client-rate-limit コマンドはクライアントエントリの学習を制限します。

undo client-rate-limit コマンドはデフォルトに戻します。

例

クライアントエントリの学習を制限します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] client-rate-limit interval 80 quiet 1600 threshold 100

6.1.20 client-spoofing

Syntax

client-spoofing [**quiet** *quiet-value*]

undo client-spoofing

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がクライアントスプーフィング攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトの遅延時間は 600 秒です。WIPS は遅延時間内にクライアントスプーフィング攻撃を検出してもアラームを引き起こしません。

説明

client-spoofing コマンドはクライアントスプーフィング攻撃検出を有効にします。

undo client-spoofing コマンドはクライアントスプーフィング攻撃検出を無効にします。

例

クライアントスプーフィング攻撃検出を有効にし、遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] client-spoofing quiet 360

6.1.21 client-timer

🕮 **メモ：**

inactive-value 引数と aging-value 引数の下限値が Version 7.1.13 を含む以降のソフトウェアから変更されました。

Syntax

client-timer inactive *inactive-value* **aging** *aging-value*

undo client-timer

デフォルト

非アクティブ時間：300 秒

エージングタイマ：600 秒

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

inactive *inactive-value*: 非アクティブ時間を指定します。指定された非アクティブ時間内にクライアントがフレームを送受信しない場合、WIPS はクライアントを非アクティブ状態に設定します。

Version 7.1.13 を含む以降のソフトウェア

inactive-value 引数の値の範囲は 1～1200 秒です。

Version 7.1.11 を含む以前のソフトウェア

inactive-value 引数の値の範囲は 60～1200 秒です。

aging *aging-value*: エージングタイマを指定します。指定されたエージングタイマ内にクライアントがフレームを送受信しない場合、WIPS はエントリを削除します。エージングタイマは非アクティブ時間より大きくなければなりません。

Version 7.1.13 を含む以降のソフトウェア

aging-value 引数の値の範囲は 1～86400 秒です。

Version 7.1.11 を含む以前のソフトウェア

aging-value 引数の値の範囲は 120～86400 秒です。

説明

client-timer コマンドはクライアントエントリタイマを設定します。

undo client-timer コマンドはデフォルトに戻します。

例

非アクティブ時間を 120 秒、エージングタイマを 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] client-timer inactive 120 aging 360

6.1.22 countermeasure adhoc

Syntax

countermeasure adhoc

undo countermeasure adhoc

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure adhoc コマンドはアドホック装置に対策を講じるために WIPS を有効にします。

undo countermeasure adhoc コマンドはデフォルトに戻します。

例

#アドホック装置に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure adhoc

6.1.23 countermeasure attack all

Syntax

countermeasure attack all

undo countermeasure attack all

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack all コマンドはすべての攻撃者に対策を講じるために WIPS を有効にします。

undo countermeasure attack all コマンドはデフォルトに戻します。

例

すべての攻撃者に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack all

6.1.24 countermeasure attack deauth-broadcast

Syntax

countermeasure attack deauth-broadcast

undo countermeasure attack deauth-broadcast

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack deauth-broadcast コマンドは認証取り消しアタックをブロードキャストする装置に対策を講じるために WIPS を有効にします。

undo countermeasure attack deauth-broadcast コマンドはデフォルトに戻します。

例

認証取り消しアタックをブロードキャストする装置に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack deauth-broadcast

6.1.25 countermeasure attack disassoc-broadcast

Syntax

countermeasure attack disassoc-broadcast

undo countermeasure attack disassoc-broadcast

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack disassoc-broadcast コマンドはアソシエーション解除フレームをブロードキャストする装置に対策を講じるために WIPS を有効にします。

undo countermeasure attack disassoc-broadcast コマンドはデフォルトに戻します。

例

#アソシエーション解除フレームをブロードキャストする装置に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack disassoc-broadcast

6.1.26 countermeasure attack honeypot-ap

Syntax

countermeasure attack honeypot-ap

undo countermeasure attack honeypot-ap

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack honeypot-ap コマンドはハニーポット AP に対策を講じるために WIPS を有効にします。

undo countermeasure attack honeypot-ap コマンドはデフォルトに戻します。

例

ハニーポット AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack honeypot-ap

6.1.27 countermeasure attack hotspot-attack

Syntax

countermeasure attack hotspot-attack

undo countermeasure attack hotspot-attack

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack hotspot-attack コマンドはホットスポット攻撃に対策を講じるために WIPS を有効にします。

undo countermeasure attack hotspot-attack コマンドはデフォルトに戻します。

例

ホットスポット攻撃に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack hotspot-attack

6.1.28 countermeasure attack ht-40-mhz-intolerance

Syntax

countermeasure attack ht-40-mhz-intolerance

undo countermeasure attack ht-40-mhz-intolerance

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack ht-40-mhz-intolerance コマンドは 40MHz 帯域幅モードが無効の装置に対策を講じるために WIPS を有効にします。

undo countermeasure attack ht-40-mhz-intolerance コマンドはデフォルトに戻します。

例

#アドホック装置に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack ht-40-mhz-intolerance

6.1.29 countermeasure attack malformed-packet

Syntax

countermeasure attack malformed-packet

undo countermeasure attack malformed-packet

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack malformed-packet コマンドは不正パケットを送信する装置に対策を講じるために WIPS を有効にします。

undo countermeasure attack malformed-packet コマンドはデフォルトに戻します。

例

不正パケットを送信する装置に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack malformed-packet

6.1.30 countermeasure attack man-in-the-middle

Syntax

countermeasure attack man-in-the-middle

undo countermeasure attack man-in-the-middle

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack man-in-the-middle コマンドは MITM 攻撃に対策を講じるために WIPS を有効にします。

undo countermeasure attack man-in-the-middle コマンドはデフォルトに戻します。

例

MITM 攻撃に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack man-in-the-middle

6.1.31 countermeasure attack omerta

Syntax

countermeasure attack omerta

undo countermeasure attack omerta

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack omerta コマンドは Omerta 攻撃に対策を講じるために WIPS を有効にします。

undo countermeasure attack omerta コマンドはデフォルトに戻します。

例

Omerta 攻撃に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack omerta

6.1.32 countermeasure attack power-save

Syntax

countermeasure attack power-save

undo countermeasure attack power-save

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack power-save コマンドはパワーセーブ攻撃に対策を講じるために WIPS を有効にします。

undo countermeasure attack power-save コマンドはデフォルトに戻します。

例

パワーセーブ攻撃に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack power-save

6.1.33 countermeasure attack soft-ap

Syntax

countermeasure attack soft-ap

undo countermeasure attack soft-ap

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack soft-ap コマンドはソフト AP に対策を講じるために WIPS を有効にします。

undo countermeasure attack soft-ap コマンドはデフォルトに戻します。

例

ソフト AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack soft-ap

6.1.34 countermeasure attack unencrypted-trust-client

Syntax

countermeasure attack unencrypted-trust-client

undo countermeasure attack unencrypted-trust-client

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack unencrypted-trust-client コマンドは未暗号化のフレームを送信する許可クライアントに対策を講じるために WIPS を有効にします。

undo countermeasure attack unencrypted-trust-client コマンドはデフォルトに戻します。

例

未暗号化フレームを送信する許可クライアントに対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack unencrypted-trust-client

6.1.35 countermeasure attack weak-iv

Syntax

countermeasure attack weak-iv

undo countermeasure attack weak-iv

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack weak-iv コマンドは Weak IV を使用する装置に対策を講じるために WIPS を有効にします。

undo countermeasure attack weak-iv コマンドはデフォルトに戻します。

例

#アドホック装置に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack weak-iv

6.1.36 countermeasure attack windows-bridge

Syntax

countermeasure attack windows-bridge

undo countermeasure attack windows-bridge

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack windows-bridge コマンドは Windows ブリッジ攻撃に対策を講じるために WIPS を有効にします。

undo countermeasure attack windows-bridge コマンドはデフォルトに戻します。

例

Windws ブリッジ攻撃に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack windows-bridge

6.1.37 countermeasure external-ap

Syntax

countermeasure external-ap

undo countermeasure external-ap

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure external-ap コマンドは外部の AP に対策を講じるために WIPS を有効にします。

undo countermeasure external-ap コマンドはデフォルトに戻します。

例

#外部の AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure external-ap

6.1.38 countermeasure mac-address

Syntax

countermeasure mac-address *mac-address*

undo countermeasure mac-address { *mac-address* | **all** }

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

パラメータ

mac-address: AP の無線 MAC アドレス(BSSID)もしくはクライアントの MAC アドレスを H-H-H 形式で指定します。

all: すべての AP とクライアントを指定します。

説明

countermeasure mac-address コマンドは指定された MAC アドレスを持つ装置に対策を講じるために WIPS を有効にします。

undo countermeasure mac-address コマンドは設定を削除します。

countermeasure mac-address コマンドを複数回設定することで、複数の装置に対策を講じるように WIPS を有効化できます。

例

MAC アドレス **2a11-1fa1-141f** を持つ装置に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure mac-address 2a11-1fa1-141f

6.1.39 countermeasure misassociation-client

Syntax

countermeasure misassociation-client

undo countermeasure misassociation-client

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure misassociation-client コマンドは間違って紐付いたクライアントに対策を講じるために WIPS を有効にします。

undo countermeasure misassociation-client コマンドはデフォルトに戻します。

例

間違って紐付いたクライアントに対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure misassociation-client

6.1.40 countermeasure misconfigured-ap

Syntax

countermeasure misconfigured-ap

undo countermeasure misconfigured-ap

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure misconfigured-ap コマンドは未設定 AP に対策を講じるために WIPS を有効にします。

undo countermeasure misconfigured-ap コマンドはデフォルトに戻します。

例

未設定 AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure misconfigured-ap

6.1.41 countermeasure policy

Syntax

countermeasure policy *policy-name*

undo countermeasure policy *policy-name*

Default

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

policy-name: 対策ポリシの名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

countermeasure policy コマンドは対策ポリシを作成し、その view に移行します。

undo countermeasure policy コマンドは対策ポリシを削除します。

例

対策ポリシ **home** を作成し、その view に移行します。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home]

6.1.42 countermeasure potential-authorized-ap

Syntax

countermeasure potential-authorized-ap

undo countermeasure potential-authorized-ap

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure potential-authorized-ap コマンドは潜在的許可 AP に対策を講じるために WIPS を有効にします。

undo countermeasure potential-authorized-ap コマンドはデフォルトに戻します。

例

潜在的許可 AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure potential-authorized-ap

6.1.43 countermeasure potential-external-ap

Syntax

countermeasure potential-external-ap

undo countermeasure potential-external-ap

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure potential-external-ap コマンドは潜在的外部 AP に対策を講じるために WIPS を有効にします。

undo countermeasure potential-external-ap コマンドはデフォルトに戻します。

例

潜在的外部 AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure potential-external-ap

6.1.44 countermeasure potential-rogue-ap

Syntax

countermeasure potential-rogue-ap

undo countermeasure potential-rogue-ap

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure potential-rogue-ap コマンドは潜在的不正 AP に対策を講じるために WIPS を有効にします。

undo countermeasure potential-rogue-ap コマンドはデフォルトに戻します。

例

潜在的不正 AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure potential-rogue-ap

6.1.45 countermeasure rogue-ap

Syntax

countermeasure rogue-ap

undo countermeasure rogue-ap

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure rogue-ap コマンドは不正 AP に対策を講じるために WIPS を有効にします。

undo countermeasure rogue-ap コマンドはデフォルトに戻します。

例

不正 AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure rogue-ap

6.1.46 countermeasure unauthorized-client

Syntax

countermeasure unauthorized-client

undo countermeasure unauthorized-client

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure unauthorized-client コマンドは無許可クライアントに対策を講じるために WIPS を有効にします。

undo countermeasure unauthorized-client コマンドはデフォルトに戻します。

例

無許可クライアントに対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure unauthorized-client

6.1.47 countermeasure uncategorized-ap

Syntax

countermeasure uncategorized-ap

undo countermeasure uncategorized-ap

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure uncategorized-ap コマンドは未分類 AP に対策を講じるために WIPS を有効にします。

undo countermeasure uncategorized-ap コマンドはデフォルトに戻します。

例

未分類 AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure uncategorized-ap

6.1.48 countermeasure uncategorized-client

Syntax

countermeasure uncategorized-client

undo countermeasure uncategorized-client

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure uncategorized-client コマンドは未分類クライアントに対策を講じるために WIPS を有効にします。

undo countermeasure uncategorized-client コマンドはデフォルトに戻します。

例

未分類クライアントに対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure uncategorized-client

6.1.49 deauthentication-broadcast

Syntax

deauthentication-broadcast [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo deauthentication-broadcast

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: ブロードキャスト認証取り消しフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの統計値収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がブロードキャスト認証取り消し攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。WIPS は遅延時間内にブロードキャスト認証取り消し攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ブロードキャスト認証取り消し攻撃アラームを引き起こすブロードキャスト認証取り消しの数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

deauthentication-broadcast コマンドはブロードキャスト認証取り消し攻撃検出を設定します。

undo deauthentication-broadcast コマンドはブロードキャスト認証取り消し攻撃検出を無効にします。

例

ブロードキャスト認証取り消し攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] deauthentication-broadcast interval 100 threshold 100 quiet 360

6.1.50 detect policy

Syntax

detect policy *policy-name*

undo detect policy *policy-name*

デフォルト

設定なし

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

policy-name: 攻撃検出ポリシの名前を指定します。大文字と小文字を区別します。設定範囲は 1～63 文字です。

説明

detect policy コマンドは攻撃検出ポリシを作成し、その view に移行します。

undo detect policy コマンドは攻撃検出ポリシを削除します。

例

攻撃検出ポリシ **home** を作成し、その view に移行します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home]

6.1.51 detect signature

Syntax

detect signature [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo detect

デフォルト

有効

View

Signature policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 署名に一致するパケットのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの統計値収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が user-defined 攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルト値は 600 秒です。WIPS は遅延時間内に user-defined 攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: user-defined 攻撃アラームを引き起こす、署名に一致したパケット数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

detect signature コマンドは署名に基づく user-define 攻撃検出を有効にします。

undo detect signature コマンドは署名に基づく user-define 攻撃検出を無効にします。

例

署名に基づく user-define 攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、60、100、360 に設定します。

<AC> system-view

[AC] wips

[AC-wips] signature policy home

[AC-wips-sig-home] detect signature interval 60 threshold 100 quiet 360

6.1.52 disassociation-broadcast

Syntax

disassociation-broadcast [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo disassociation-broadcast

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: ブロードキャスト認証取り消しフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの統計値収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がブロードキャスト認証取り消し攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルト値は 600 秒です。WIPS は遅延時間内にブロードキャスト認証取り消し攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ブロードキャスト認証取り消し攻撃アラームを引き起こす、ブロードキャスト認証取り消しフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

disassociation-broadcast コマンドはブロードキャスト認証取り消し攻撃検出を有効にします。

undo disassociation-broadcast コマンドはブロードキャスト認証取り消し攻撃検出を無効にします。

例

ブロードキャスト認証取り消し攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] disassociation-broadcast interval 100 threshold 100 quiet 360

6.1.53 detect dissociate-client enable

Syntax

detect dissociate-client enable

undo detect dissociate-client enable

デフォルト

設定なし

View

Attack detection policy view

定義済みユーザロール

network-admin

説明

detect dissociate-client enable コマンドは関連付けられていないクライアントの検出を有効にします。

undo detect dissociate-client enable コマンドは関連付けられていないクライアントの検出を有効にします。

例

関連付けられていないクライアントの検出を有効にします。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] detect dissociate-client enable

6.1.54 discovered-ap

Syntax

discovered-ap *value1* [**to** *value2*]

undo discovered-ap

デフォルト

一致なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

value1 **to** *value2*: AP を検出するセンサの数の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、どちらも 1～128 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

説明

discovered-ap コマンドを使用して、AP を検出するセンサの数を整合するために AP 分類ルールを設定します。

undo discovered-ap コマンドでデフォルトに戻ります。

例

10～128 のセンサに検出された AP を整合するために、AP classification rule 1 を設定します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

[AC-wips-cls-rule-1] discovered-ap 10 to 128

6.1.55 display wips sensor

Syntax

display wips sensor

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wips sensor コマンドはすべてのセンサに関する情報を表示します。

例

すべてのセンサに関する情報を表示します。

<AC> display wips sensor

```
Total number of sensors: 1
Sensor ID   Sensor name             VSD name            Radio ID   Status
3           ap1                    aaa                 1          Active
```

表 6-1 コマンド出力

フィールド	説明
VSD name	APが属するVSDの名前
Radio ID	WIPSで有効化された無線の名前
Status	センサの状態 • **Active**－センサはWIPSで有効にされます。 • **Inactive**－センサはWIPSで有効にされません。

6.1.56 display wips statistics

Syntax

display wips statistics [**receive** | **virtual-security-domain** *vsd-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

receive: すべての VSD のセンサから AC が受信する攻撃検出統計値情報を表示します。

virtual-security-domain *vsd-name*: 指定された VSD のセンサから AC が受信する攻撃検出統計値情報を表示します。

説明

display wips statistics コマンドはセンサから収集した攻撃検出情報を表示します。

例

すべての VSD のセンサから収集した攻撃検出統計値情報を表示します。

<AC> display wips statistics receive

```
Information from sensor 3
 Information about attack statistics:
   Detected association-request flood messages: 0
   Detected authentication flood messages: 0
   Detected beacon flood messages: 0
   Detected block-ack flood messages: 0
   Detected cts flood messages: 0
   Detected deauthentication flood messages: 0
   Detected disassociation flood messages: 0
   Detected eapol-start flood messages: 0
   Detected null-data flood messages: 0
   Detected probe-request flood messages: 0
   Detected reassociation-request flood messages: 0
   Detected rts flood messages: 0
   Detected eapol-logoff flood messages: 0
   Detected eap-failure flood messages: 0
   Detected eap-success flood messages: 0
   Detected duplicated-ie messages: 0
   Detected fata-jack messages: 0
   Detected illegal-ibss-ess messages: 0
   Detected invalid-address-combination messages: 0
   Detected invalid-assoc-req messages: 0
   Detected invalid-auth messages: 0
   Detected invalid-deauth-code messages: 0
   Detected invalid-disassoc-code messages: 0
   Detected invalid-ht-ie messages: 0
   Detected invalid-ie-length messages: 0
```

```
Detected invalid-pkt-length messages: 0
Detected large-duration messages: 0
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 0
Detected overflow-ssid messages: 0
Detected redundant-ie messages: 0
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0
Detected AP spoof ad-hoc messages: 0
Detected ad-hoc spoof AP messages: 0
Detected client spoof AP messages: 0
Detected weak IV messages: 0
Detected excess AP messages: 0
Detected excess client messages: 0
Detected signature rule messages: 0
Detected 40MHZ messages: 0
Detected power save messages: 0
Detected omerta messages: 0
Detected windows bridge messages: 0
Detected soft AP messages: 0
Detected broadcast disassoc messages: 2
Detected broadcast deauth messages: 0
Detected AP impersonate messages: 0
Detected HT greenfield messages: 0
Detected association table overflow messages: 0
Detected wireless bridge messages: 0
Detected AP flood messages: 11
```

表 6-2 コマンド出力

フィールド	説明
Information from sensor n	センサnから収集した情報。nはセンサのIDをあらわします。
Detected association-request flood messages	紐付け要求フラッドアタック攻撃に対して検出したメッセージの数。
Detected authentication flood messages	認証要求フラッド攻撃に対して検出したメッセージの数。
Detected beacon flood messages	ビーコンフラッド攻撃に対して検出したメッセージの数。
Detected block-ack flood messages	ブロックアクトフラッド攻撃に対して検出したメッセージの数。
Detected cts flood messages	CTSフラッド攻撃に対して検出したメッセージの数。

フィールド	説明
Detected deauthentication flood messages	認証取り消しフラッド攻撃に対して検出したメッセージの数。
Detected disassociation flood messages	紐付け取り消しフラッド攻撃に対して検出したメッセージの数。
Detected eapol-start flood messages	EAPOLスタートフラッド攻撃に対して検出したメッセージの数。
Detected null-data flood messages	nullデータフラッド攻撃に対して検出したメッセージの数。
Detected probe-request flood messages	プローブ要求フラッド攻撃に対して検出したメッセージの数。
Detected reassociation-request flood messages	再紐付け要求フラッド攻撃に対して検出したメッセージの数。
Detected rts flood messages	RTSフラッド攻撃に対して検出したメッセージの数。
Detected eapol-logoff flood messages	EAPOLログオフフラッド攻撃に対して検出したメッセージの数。
Detected eap-failure flood messages	EAPOL失敗フラッド攻撃に対して検出したメッセージの数。
Detected eap-success flood messages	EAPOL成功フラッド攻撃に対して検出したメッセージの数。
Detected duplicated-ie messages	複製されたIEをもつ異常パケットに対して検出したメッセージの数。
Detected fata-jack messages	FATAジャック異常パケットに対して検出したメッセージの数。
Detected illegal-ibss-ess messages	異常なIBSSとESS設定をもつ異常パケットに対して検出したメッセージの数。
Detected invalid-address-combination messages	無効な送信元アドレスをもつ異常パケットに対して検出したメッセージの数。
Detected invalid-assoc-req messages	異常な紐付け要求に対して検出したメッセージの数。
Detected invalid-auth messages	異常な認証要求に対して検出したメッセージの数。
Detected invalid-deauth-code messages	無効な認証取り消しコードをもつ異常パケットに対して検出したメッセージの数。
Detected invalid-disassoc-code messages	無効な紐付け取り消しコードをもつ異常パケットに対して検出したメッセージの数。
Detected invalid-ht-ie messages	異常なHT IEをもつ異常パケットに対して検出したメッセージの数。
Detected invalid-ie-length messages	無効なIE長をもつ異常パケットに対して検出したメッセージの数。

フィールド	説明
Detected invalid-pkt-length messages	無効なパケット長をもつ異常パケットに対して検出したメッセージの数。
Detected large-duration messages	オーバーサイズの期間をもつ異常パケットに対して検出したメッセージの数。
Detected null-probe-resp messages	異常なプローブ要求フレームに対して検出したメッセージの数。
Detected overflow-eapol-key messages	オーバーサイズのEAPOL鍵をもつ異常パケットに対して検出したメッセージの数。
Detected overflow-ssid messages	オーバーサイズなSSIDをもつ異常パケットに対して検出したメッセージの数。
Detected redundant-ie messages	冗長なIEをもつ異常パケットに対して検出したメッセージの数。
Detected AP spoof AP messages	APスプーフィング攻撃に対して検出したメッセージの数。(AP spoofs AP)
Detected AP spoof client messages	クライアントスプーフィング攻撃に対して検出したメッセージの数。(AP spoofs client)
Detected AP spoof ad-hoc messages	アドホックスプーフィング攻撃に対して検出したメッセージの数。(AP spoofs Ad hoc)
Detected ad-hoc spoof AP messages	APスプーフィング攻撃に対して検出したメッセージの数。(Ad hoc spoofs AP)
Detected client spoof AP messages	APスプーフィング攻撃に対して検出したメッセージの数。(client spoofs AP)
Detected weak IV messages	ウィークIVに対して検出したメッセージの数。
Detected excess AP messages	APエントリ攻撃に対して検出したメッセージの数。
Detected excess client messages	クライアントエントリ攻撃に対して検出したメッセージの数。
Detected 40MHZ messages	40Hz帯モードで無効化されるクライアントに対して検出したメッセージの数。
Detected power save messages	電力節約攻撃に対して検出したメッセージの数。
Detected omerta messages	Omerta攻撃に対して検出したメッセージの数。
Detected windows bridge messages	Windowsブリッジに対して検出したメッセージの数。
Detected soft AP messages	ソフトAPに対して検出したメッセージの数。
Detected broadcast disassoc messages	ブロードキャスト紐付け取り消し攻撃に対して検出したメッセージの数。
Detected broadcast deauth messages	ブロードキャスト認証取り消し攻撃に対して検出したメッセージの数。

フィールド	説明
Detected AP impersonate messages	APなりすまし攻撃に対して検出したメッセージの数。
Detected HT greenfield messages:	HTグリーンフィールドAPの検出メッセージ数
Detected association table overflow messages	アソシエーション/再アソシエーションのDoS攻撃に対する検出メッセージ数
Detected wireless bridge messages	無線ブリッジの検出メッセージ数。
Detected AP flood messages	APフラッドアタックの検出メッセージ数

指定された VSD のセンサから収集された攻撃検出情報を表示します。

<AC> display wips statistics virtual-security-domain 111

```
Information from VSD 111
Information about attack statistics:
  Detected hotspot attack messages: 1
  Detected unencrypted authorized AP messages: 0
  Detected unencrypted trust client messages: 0
  Detected honeypot AP messages: 1
  Detected man in the middle messages: 1
  Detected AP channel change messages: 0
```

表 6-3 コマンド出力

フィールド	説明
Detected hotspot attack messages	ホットスポット攻撃の検出メッセージ数。
Detected unencrypted authorized AP messages	暗号化されていない許可APの検出メッセージ数。
Detected unencrypted trust client messages	暗号化されていない許可クライアントの検出メッセージ数。
Detected honeypot AP messages	ハニーポットAPの検出メッセージ数。
Detected man in the middle messages	MITM攻撃の検出されたメッセージ数
Detected AP channel change messages	チャネル変更のために検出されたメッセージの数。

関連コマンド

reset wips statistics

6.1.57 display wips virtual-security-domain countermeasure record

Syntax

display wips virtual-security-domain *vsd-name* **countermeasure record**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

display wips virtual-security-domain countermeasure record コマンドは WIPS が不正な装置に実行している対策の情報を表示します。

例

VSD **office** で WIPS が対策を実行している不正な装置に関する情報を表示します。

<AC> display wips virtual-security-domain office countermeasure record

```
Total 3 times countermeasure, current 3 countermeasure record in virtual-
security-domain office

Reason: Attack; Ass - associated; Black - blacklist;
       Class - classification; Manu - manual;

MAC address    Type   Reason   Countermeasure AP    Radio ID   Time
1000-0000-00e3 AP      Manu      ap1                      1          2016-05-
03/09:32:01
1000-0000-00e4 AP      Manu      ap2                      1          2016-05-
03/09:32:11
2000-0000-f282 Client Black     ap3                      1          2016-05-
03/09:31:56
```

表 6-4 コマンド出力

フィールド	説明
Total 3 times countermeasure, current 3 countermeasure record in virtual-security-domain office	成功した対策の数。このフィールドは1024まで表示できます。
MAC Address	WIPSが対策した無線装置のMACアドレス。
Type	無線装置のタイプ：APもしくはクライアント
Reason	WIPSが無線装置に対策した理由。 • **Attack**－無線装置がアタッカーです。 • **Ass**－無線装置が関連付いたAPに対して対策します。 • **Black**－クライアントに対策後にAPに関連付くと、クライアントをブラックリストに追加します。 • **Class**－装置のタイプに基づいて対策を実施します。 • **Manu**－MACアドレスに基づいて対策を実施します。
Countermeasure AP	無線装置に対策を実行したセンサの名前。
Radio ID	無線装置に対策を実行したセンサのラジオID。
Time	無線装置に対策を実行した時間。

6.1.58 display wips virtual-security-domain device

Syntax

display wips virtual-security-domain *vsd-name* **device** [**ap** [**ad-hoc** | **authorized** | **external** | **misconfigured** | **potential-authorized** | **potential-external** | **potential-rogue** | **rogue**] | **client** [[**dissociative-client**] | [**authorized** | **misassociation** | **unauthorized** | **uncategorized**]] | **mac-address** *mac-address*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

device: 無線装置の情報を表示します。

ap: AP の情報を表示します。

ad-hoc: アドホックモードで動作する AP に関する情報を表示します。

authorized: 許可 AP に関する情報を表示します。

external: 外部 AP に関する情報を表示します。

misconfigured: 間違って設定された AP に関する情報を表示します。

potential-authorized: 潜在的に許可された AP に関する情報を表示します。

potential-external: 潜在的外部 AP に関する情報を表示します。

potential-rogue: 潜在的な不正 AP に関する情報を表示します。

rogue: 不正な AP に関する情報を表示します。

client: クライアント情報を表示します。

dissociative-client: 紐付けられていないクライアント情報を表示します。

authorized: 許可クライアントに関する情報を表示します。

misassociation: 間違って紐付けられたクライアントに関する情報を表示します。

unauthorized: 未許可クライアントに関する情報を表示します。

uncategorized: 分類されていないクライアントに関する情報を表示します。

mac-address *mac-address*: 特定の無線装置に関する情報を表示します。*mac-address* 引数は無線装置の MAC アドレスを表し、H-H-H 形式です。

verbose: 詳細な装置情報を表示します。

説明

display wips virtual-security-domain device コマンドは VSD で検出された無線装置に関する情報を表示します。

例

VSD **office** で検出された無線装置に関する情報を表示します。

<AC> display wips virtual-security-domain office device

```
Total 200 detected devices in virtual-security-domain office

Class: Auth - authorization; Ext - external; Mis - mistake;
      Unauth - unauthorized; Uncate - uncategorized;
      (A) - associate; (C) - config; (P) - potential

MAC address    Type   Class    Duration    Sensors Channel Status
1000-0000-0000 AP     Ext(P)   00h 10m 46s 1       11      Active
1000-0000-0001 AP     Ext(P)   00h 10m 46s 1       6       Active
1000-0000-0002 AP     Ext(P)   00h 10m 46s 1       1       Active
```

表 6-5 コマンド出力

フィールド	説明
Type	無線装置タイプ： AP、Client、またはMesh
Class	無線装置のカテゴリ
Duration	無線装置が現在の状態に移行してからの期間
Sensors	無線装置を検出したセンサの数
Channel	直近で無線装置が検出されたチャネル
Status	APもしくはクライアントの状態 ● **Active**－APもしくはクライアントはアクティブです。 ● **Inactive**－APもしくはクライアントは非アクティブです。

VSD **a** で検出された無線装置に関する詳細な情報を表示します。

<AC> display wips virtual-security-domain a device verbose

```
Total 2 detected devices in virtual-security-domain a

 AP: 1000-0000-0000
   Mesh Neighbor: None
   Classification: Mis(C)
   Severity level: 0
   Classify way: Auto
   Status: Active
   Status duration: 00h 27m 57s
   Vendor: Not found
   SSID: service
   Radio type: 802.11g
   Countermeasuring: No
   Security: None
   Encryption method: None
   Authentication method: None
   Broadcast SSID: Yes
   QoS supported: No
   Ad-hoc: No
   Beacon interval: 100 TU
   Up duration: 00h 27m 57s
Channel band-width supported: 20MHZ
   Hotspot AP: No
```

```
    Soft AP: No
    Honeypot AP: No
    Total number of reported sensors: 1
      Sensor 1:
        Sensor ID: 3
        Sensor name: 1
        Radio ID: 1
        RSSI: 15
        Channel: 149
        First reported time: 2014-06-03/09:05:51
        Last reported time: 2014-06-03/09:05:51
    Total number of associated clients: 1
      01: 2000-0000-0000
Client: 2000-0000-0000
  Last reported associated AP: 1000-0000-0000
  Classification: Uncate
  Severity level: 0
  Classify way: Auto
  Dissociative status: No
  Status: Active
  Status duration: 00h 00m 02s
  Vendor: Not found
  Radio type: 802.11a
  40mhz intolerance: No
  Countermeasuring: No
  Man in the middle: No
  Total number of reported sensors: 1
     Sensor 1:
       Sensor ID: 2
       Sensor name: 1
       Radio ID: 1
       RSSI: 50
       Channel: 149
       First reported time: 2014-06-03/14:52:56
       Last reported time: 2014-06-03/14:52:56
       Reported associated AP: 1000-0000-0000
```

表 6-6 コマンド出力

フィールド	説明
AP	APのMACアドレス
Mesh Neighbor	メッシュAPのネイバのMACアドレス

フィールド	説明
Client	クライアントのMACアドレス
Last reported associated AP	クライアントが直近で報告した、紐付けられたAPのMACアドレス

Classification	APもしくはクライアントのカテゴリ
	• APカテゴリオプション
	  • ad_hoc
	  • authorized
	  • rogue
	  • misconfigured
	  • external
	  • potential-authorized
	  • potential-rogue
	  • potential-external
	  • uncategorized
	• クライアントカテゴリオプション
	  • authorized
	  • unauthorized
	  • misassociated
	  • uncategorized

Severity level	装置の重大度レベル
Classify way	APもしくはクライアント分類方法 • **Manual**－手動分類 • **Invalid OUI**－無効なOUIリストに追加 • **Block List**－禁止装置リストに追加 • **Associated**－ACに接続されたAP • **Trust List**－許可装置リストに追加 • **User Define**－ユーザが定義した分類 • **Auto**－自動分類
Dissociative status	クライアントが紐付けられたものではないかどうかをあらわします。
Status	APもしくはクライアントの状態 • **Active**－APもしくはクライアントはアクティブです。 • **Inactive**－APもしくはクライアントは非アクティブです。

フィールド	説明
Status duration	無線装置が現在の状態に移行してからの期間
Vendor	装置のOUI。装置のOUIが、インポートされたOUIと一致する場合、このフィールドは装置のOUIを表示します。装置にOUIが設定されていない場合、あるいは装置のOUIが、インポートされたいずれのOUIとも一致しない場合、このフィールドは**Not found**を表示します。
SSID	APに提供された無線装置のSSID
Radio Type	無線装置の無線モード
40mhz intolerance	クライアントが40MHz帯をサポートするかどうかをあらわします。
Countermeasuring	WIPSが無線装置に対策を講じるかをあらわします。 • **No** • **Yes**
Man in the middle	MITM攻撃を検出するかどうかをあらわします。
Security	セキュリティ方式。 • **None** • **WEP** • **WPA** • **WPA 2**
Encryption method	データ暗号方式。 • **TKIP** • **CCMP** • **WEP** • **None**
Authentication method	認証方式。 • **None** • **PSK** • **802.1X** • **Others**－PSK認証と802.1X認証以外の認証方式
Broadcast SSID	APがSSIDをブロードキャストするかどうかをあらわします。APがSSIDをブロードキャストしない場合、このフィールドは何も表示しません。
QoS supported	無線装置がQoSをサポートするかどうかをあらわします。
Ad-hoc	無線装置がアドホックモードかどうかをあらわします。

フィールド	説明
Beacon interval	TUにおけるビーコン間隔です。1つのTUは1024マイクロ秒に等しいです。
Channel band-width supported	サポートされたチャネル帯域幅モード ● 20/40/80MHZ ● 20/40MHz ● 20MHz
Hotspot AP	APがホットスポット攻撃APであるかどうかをあらわします。
Soft AP	APがソフトAPであるかどうかをあらわします。
Honeypot AP	APがハニーポットAPであるかどうかをあらわします。
Sensor n	無線装置を検出したセンサです。n はシステムに割り当てられたIDをあらわします。
Channel	センサが直近で無線装置を検出したチャネルです。
First reported time	センサが最初に無線装置を検出した時間です。
Last reported time	センサが直近で無線装置を検出した時間です。
n: H-H-H	APに紐付けられたMACアドレスです。n はシステムに割り当てられたIDをあらわします。
Reported associated AP	センサが報告した、紐付けられたAPのMACアドレスです。

関連コマンド

reset wips virtual-security-domain device

6.1.59 display wlan nat-detect

Syntax

display wlan nat-detect [**mac-address** *mac-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address *mac-address*: クライアントを MAC アドレスで指定します。このオプションを指定しない場合、検出されたすべての NAT 構成クライアントに関する情報が表示されます。

説明

display wlan nat-detect コマンドは NAT が設定されたクライアントに関する情報を表示します。

例

検出されたすべての NAT 構成クライアントに関する情報を表示します。

<AC> display wlan nat-detect

```
Total 1 detected clients with NAT configured

MAC address    Last report        First report        Duration
0a98-2044-0000 2015-08-24/11:05:23 2015-08-24/10:05:23  01h 15m 00s
```

表 6-7 コマンド出力

フィールド	説明
Total number detected clients with NAT configured	検出されたNAT構成クライアントの数
MAC address	検出されたクライアントのMACアドレス
Last report	クライアントが直近に検出された時刻
First report	クライアントが最初に検出された時刻
Duration	クライアントがNAT設定されてからの期間

関連コマンド

reset wlan nat-detect

6.1.60 flood association-request

Syntax

flood association-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood association-request

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 紐付け要求フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が紐付け要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に紐付け要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 紐付け要求フラッド攻撃アラームを引き起こす紐付け要求フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood association-request コマンドは紐付け要求フラッド攻撃検出を設定します。

undo flood a**ssociation-request** コマンドはデフォルトに戻します。

例

紐付け要求フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood association-request interval 100 threshold 100 quiet 360

6.1.61 flood authentication

Syntax

flood authentication [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood authentication

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 認証要求フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が認証要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に認証要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 認証要求フラッド攻撃アラームを引き起こす認証要求フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood authentication コマンドは認証要求フラッド攻撃検出を設定します。

undo flood authentication コマンドはデフォルトに戻します。

例

認証要求フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood authentication interval 100 threshold 100 quiet 360

6.1.62 flood beacon

Syntax

flood beacon [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood beacon

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: ビーコンフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がビーコンフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にビーコンフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ビーコンフラッド攻撃アラームを引き起こすビーコンフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood beacon コマンドはビーコンフラッド攻撃検出を設定します。

undo flood beacon コマンドはデフォルトに戻します。

例

ビーコンフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood beacon interval 100 threshold 100 quiet 360

6.1.63 flood block-ack

Syntax

flood block-ack [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood block-ack

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: ブロックアクトフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がブロックアクトフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にブロックアクトフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ブロックアクトフラッド攻撃アラームを引き起こすブロックアクトフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood block-ack コマンドはブロックアクトフラッド攻撃検出を設定します。

undo flood block-ack コマンドはデフォルトに戻します。

例

ブロックアクトフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood block-ack interval 100 threshold 100 quiet 360

6.1.64 flood cts

Syntax

flood cts [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood cts

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: CTS フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が CTS フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に CTS フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: CTS フラッド攻撃アラームを引き起こす CTS フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood cts コマンドは CTS フラッド攻撃検出を設定します。

undo flood cts コマンドはデフォルトに戻します。

例

CTS フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood cts interval 100 threshold 100 quiet 360

6.1.65 flood deauthentication

Syntax

flood deauthentication [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood deauthentication

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 認証取り消しフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が認証取り消しフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に認証取り消しフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 認証取り消しフラッド攻撃アラームを引き起こす認証取り消しフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood deauthentication コマンドは認証取り消しフラッド攻撃検出を設定します。

undo flood deauthentication コマンドはデフォルトに戻します。

例

認証取り消しフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood deauthentication interval 100 threshold 100 quiet 360

6.1.66 flood disassociation

Syntax

flood disassociation [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood disassociation

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 紐付け取り消しフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が紐付け取り消しフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に紐付け取り消しフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 紐付け取り消しフラッド攻撃アラームを引き起こす紐付け取り消しフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood disassociation コマンドは紐付け取り消しフラッド攻撃検出を設定します。

undo flood disassociation コマンドはデフォルトに戻します。

例

紐付け取り消しフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood disassociation interval 100 threshold 100 quiet 360

6.1.67 flood eap-failure

Syntax

flood eap-failure [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eap-failure

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: EAP 失敗フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が EAP 失敗フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に EAP 失敗フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: EAP 失敗フラッド攻撃アラームを引き起こす EAP 失敗フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood eap-failure コマンドは EAP 失敗フラッド攻撃検出を設定します。

undo flood eap-failure コマンドはデフォルトに戻します。

例

EAP 失敗フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood eap-failure interval 100 threshold 100 quiet 360

6.1.68 flood eapol-logoff

Syntax

flood eapol-logoff [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eapol-logoff

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: EAPOL ログオフフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が EAPOL ログオフフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に EAPOL ログオフフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: EAPOL ログオフフラッド攻撃アラームを引き起こす EAPOL ログオフフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood eapol-logoff コマンドは EAPOL ログオフフラッド攻撃検出を設定します。

undo flood eapol-logoff コマンドはデフォルトに戻します。

例

EAPOL ログオフフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood eapol-logoff interval 100 threshold 100 quiet 360

6.1.69 flood eapol-start

Syntax

flood eapol-start [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eapol-start

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: EAPOL スタートフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が EAPOL スタートフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に EAPOL スタートフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: EAPOL スタートフラッド攻撃アラームを引き起こす EAPOL スタートフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood eapol-start コマンドは EAPOL スタートフラッド攻撃検出を設定します。

undo flood eapol-start コマンドはデフォルトに戻します。

例

EAPOL スタートフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood eapol-start interval 100 threshold 100 quiet 360

6.1.70 flood eap-success

Syntax

flood eap-success [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eap-success

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: EAP 成功フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が EAP 成功フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に EAP 成功フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: EAP 成功フラッド攻撃アラームを引き起こす EAP 成功フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood eap-success コマンドは EAP 成功フラッド攻撃検出を設定します。

undo flood eap-success コマンドはデフォルトに戻します。

例

EAP 成功フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood eap-success interval 100 threshold 100 quiet 360

6.1.71 flood null-data

Syntax

flood null-data [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood null-data

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: null データフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が null データフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に null データフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: null データフラッド攻撃アラームを引き起こす null データフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood null-data コマンドは null データフラッド攻撃検出を設定します。

undo flood null-data コマンドはデフォルトに戻します。

例

null データフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood null-data interval 100 threshold 100 quiet 360

6.1.72 flood probe-request

Syntax

flood probe-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood probe-request

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: プローブ要求フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がプローブ要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にプローブ要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: プローブ要求フラッド攻撃アラームを引き起こすプローブ要求フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood probe-request コマンドはプローブ要求フラッド攻撃検出を設定します。

undo flood probe-request コマンドはデフォルトに戻します。

例

プローブ要求フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood probe-request interval 100 threshold 100 quiet 360

6.1.73 flood reassociation-request

Syntax

flood reassociation-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood reassociation-request

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 再紐付け要求フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が再紐付け要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に再紐付け要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 再紐付け要求フラッド攻撃アラームを引き起こす再紐付け要求フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood reassociation-request コマンドは再紐付け要求フラッド攻撃検出を設定します。

undo flood reassociation-request コマンドはデフォルトに戻します。

例

再紐付け要求フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood reassociation-request interval 100 threshold 100 quiet 360

6.1.74 flood rts

Syntax

flood rts [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood rts

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: RTS フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が RTS フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に RTS フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: RTS フラッド攻撃アラームを引き起こす RTS フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood rts コマンドは RTS フラッド攻撃検出を設定します。

undo flood rts コマンドはデフォルトに戻します。

例

RTS フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood rts interval 100 threshold 100 quiet 360

6.1.75 frame-type

Syntax

frame-type { **control** | **data** | **management** [**frame-subtype** { **association-request** | **association-response** | **authentication** | **beacon** | **deauthentication** | **disassociation** | **probe-request** }] }

undo frame-type

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

control: 制御フレームと整合します。

data: データフレームと整合します。

management: 管理フレームと整合します。

frame-subtype: フレームサブタイプを指定します。

association-request: 紐付け要求フレームと整合します。

association-response: 紐付け応答フレームと整合します。

authentication: 認証フレームと整合します。

beacon: ビーコンフレームと整合します。

deauthentication: 認証取り消しフレームと整合します。

disassociation: 紐付け取り消しフレームと整合します。

probe-request: プローブ要求フレームと整合します。

説明

frame-type コマンドはフレームのフレームタイプと整合するためにサブ署名を設定します。

undo frame-type コマンドはデフォルトに戻します。

例

データフレームと一致するように signature 1 に対してサブ署名を設定します。

<AC> system-view

[AC] wips

[AC-wips] signature rule 1

[AC-wips-sig-rule-1] frame-type data

6.1.76 honeypot-ap

Syntax

honeypot-ap [**similarity** *similarity-value* | **quiet** *quiet-value*] *

undo honeypot-ap

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

similarity *similarity-value*: ハニーポット AP アラームを引き起こす類似のしきい値を指定します。値の範囲は 70～100%です。デフォルト値は 80%です。AP の SSID と適合 AP の SSID との間の類似点がしきい値に達すると、AP はハニーポット AP とみなされます。

quiet *quiet-value*: WIPS がハニーポット AP 検出アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にハニーポット AP を検出してもアラームを引き起こしません。

説明

honeypot-ap コマンドはハニーポット AP 検出を設定します。

undo honeypot-ap コマンドはハニーポット AP 検出を無効にします。

例

ハニーポット AP 検出を有効にします。類似のしきい値と遅延時間をそれぞれ、90%、10 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] honeypot-ap similarity 90 quiet 10

6.1.77 hotspot-attack

Syntax

hotspot-attack [**quiet** *quiet-value*]

undo hotspot-attack

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がハニーポット攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にハニーポット攻撃を検出してもアラームを引き起こしません。

説明

hotspot-attack コマンドはハニーポット攻撃検出を設定します。

undo hotspot-attack コマンドはハニーポット攻撃検出を無効にします。

例

ハニーポット攻撃検出を有効にします。遅延時間を 100 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] hotspot-attack quiet 100

6.1.78 ht-40mhz-intolerance

Syntax

ht-40mhz-intolerance [**quiet** *quiet-value*]

undo ht-greenfield

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が 40MHz の帯域幅モードを使用禁止にしたクライアントを検出するアラームを開始した後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に HT グリーンフィールド AP を検出してもアラームを引き起こしません。

説明

ht-40mhz-intolerance コマンドは 40MHz の帯域幅モードを使用禁止にしたクライアントの検出を設定します。

undo ht-40mhz-intolerance コマンドは 40MHz の帯域幅モードを使用禁止にしたクライアントの検出を無効にします。

例

40MHz の帯域幅モードを使用禁止にしたクライアント検出を有効にします。遅延時間を 100 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ht-40mhz-intolerance quiet 100

6.1.79 ht-greenfield

Syntax

ht-greenfield [**quiet** *quiet-value*]

undo ht-greenfield

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が HT グリーンフィールド AP 検出アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に HT グリーンフィールド AP を検出してもアラームを引き起こしません。

説明

ht-greenfield コマンドは HT グリーンフィールド検出を設定します。

undo ht-greenfield コマンドは HT グリーンフィールド検出を無効にします。

例

HT グリーンフィールド AP 検出を有効にします。遅延時間を 100 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ht-greenfield quiet 100

6.1.80 ignorelist

Syntax

ignorelist mac-address *mac-address*

undo i**gnorelist mac-address** { *mac-address* | **all** }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-address: MAC アドレスを H-H-H 形式で指定します。

all: アラームを無視する装置リスト内のすべてのすべての MAC アドレスを指定します。

説明

ignorelist コマンドはアラームを無視する装置リストに MAC アドレスを追加します。

undo ignorelist コマンドはアラームを無視する装置リストから特定の、もしくはすべての MAC アドレスを削除します。

WIPS は、アラームを無視する装置リスト内の無線装置のみを監視しますが、アラームはあげません。

例

アラームを無視する装置リストに MAC アドレス **2a11-1fa1-1311** を追加します。

<AC> system-view

[AC] wips

[AC-wips] ignorelist mac-address 2a11-1fa1-1311

6.1.81 import hotspot

Syntax

import hotspot *file-name*

undo import hotspot

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

file-name: コンフィグレーションファイルの名前を指定します。大文字と小文字は区別しません。文字数は 1～255 文字です。バックスラッシュ、スラッシュ（/）、コロン（:）、アスタリスク（*）、クエスチョンマーク（?）、クォーテーションマーク（"）、左括弧（<）、右括弧（>）、縦棒（|）は使用できません。

説明

import hotspot コマンドはコンフィグレーションファイルからホットスポットをインポートします。

undo import hotspot コマンドはコンフィグレーションファイルを削除します。

1 つのコンフィグレーションファイルからのみホットスポットをインポートできます。

例

コンフィグレーションファイル **hotspot_cfg** からホットスポットをインポートします。

<AC> system-view

[AC] wips

[AC-wips] import hotspot hotspot_cfg

6.1.82 import oui

Syntax

import oui *file-name*

undo import oui

デフォルト

インポートなし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

file-name: コンフィグレーションファイルの名前を指定します。大文字と小文字は区別しません。文字数は 1～255 文字です。バックスラッシュ、スラッシュ（/）、コロン（:）、アスタリスク（*）、クエスチョンマーク（?）、クォーテーションマーク（"）、左括弧（<）、右括弧（>）、縦棒（|）は使用できません。

説明

import oui コマンドはコンフィグレーションファイルから OUI をインポートします。

undo import oui コマンドはコンフィグレーションを削除します。

IEEE ウェブサイトからコンフィグレーションファイルをダウンロードできます。

1 つのコンフィグレーションファイルからのみ OUI をインポートできます。

例

コンフィグレーションファイル **oui_import_cfg** から OUI をインポートします。

<AC> system-view

[AC] wips

[AC-wips] import oui oui_import_cfg

関連コマンド

invalid-oui-classify illegal

6.1.83 invalid-oui-classify illegal

Syntax

invalid-oui-classify illegal

undo invalid-oui-classify

デフォルト

無効

View

Classification policy view

定義済みユーザロール

network-admin

説明

invalid-oui-classify illegal コマンドは無効な OUI で装置を不正な装置として分類するように WIPS を有効にします

undo invalid-oui-classify コマンドはデフォルトに戻します。

例

無効な OUI で装置を不正な装置として分類するように WIPS を設定します。

<AC> system-view

[AC] wips

[AC-wips] classification policy home

[AC-wips-cls-home] invalid-oui-classify illegal

関連コマンド

import oui

6.1.84 mac-address

Syntax

mac-address { **bssid** | **destination** | **source** } *mac-address*

undo mac-address

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

bssid: 指定された BSSID と整合します。

destination: 指定された送信元 MAC アドレスと整合します。

source: 指定された送信元 MAC アドレスと整合します。

mac-address: MAC アドレスを H-H-H 形式で指定します。

説明

mac-address コマンドはフレームが送信元 MAC アドレスと整合するようにサブ署名を設定します。

undo mac-address コマンドはデフォルトに戻します。

例

フレームが送信元 MAC アドレス **000f-e201-0101** と整合するように signature 1 に対してサブ署名を設定します。

<AC> system-view

[AC] wips

[AC-wips] signature rule 1

[AC-wips-sig-rule-1] mac-address source 000f-e201-0101

6.1.85 malformed duplicated-ie

Syntax

malformed duplicated-ie [**quiet** *quiet-value*]

undo malformed duplicated-ie

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が複製された IE のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に複製された IE を検出してもアラームを引き起こしません。

説明

malformed duplicated-ie コマンドは複製された IE を伴った異常パケットを検出するように、WIPS を有効にします。

undo malformed duplicated-ie コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。複製された IE をパケットが持つ場合、WIPS はパケットを異常とみなします。この検出はベンダに定義された IE には適用できません。

例

複製された IE を伴った異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed duplicated-ie quiet 360

6.1.86 malformed fata-jack

Syntax

malformed fata-jack [**quiet** *quiet-value*]

undo malformed fata-jack

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が FATA ジャック異常パケットアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600

秒です。WIPS は遅延時間内に FATA ジャック異常パケットを検出してもアラームを引き起こしません。

説明

malformed fata-jack コマンドは FATA ジャック異常パケットを検出するように、WIPS を有効にします。

undo malformed fata-jack コマンドはデフォルトに戻します。

この機能は認証フレームに適用できます。認証アルゴリズム番号の値が 2 である場合、WIPS は認証フレームを異常とみなします。

例

複製された IE を伴った異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed fata-jack quiet 360

6.1.87 malformed illegal-ibss-ess

Syntax

malformed illegal-ibss-ess [**quiet** *quiet-value*]

undo malformed illegal-ibss-ess

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常 IBSS および ESS 設定のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常 IBSS および ESS 設定を検出してもアラームを引き起こしません。

説明

malformed illegal-ibss-ess コマンドは異常 IBSS および ESS 設定をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed illegal-ibss-ess コマンドはデフォルトに戻します。

この機能はビーコンフレームおよびプローブ応答フレームに適用できます。IBSS と ESS がフレーム内でともに 1 に設定されている場合、WIPS はフレームを異常とみなします。

例

異常 IBSS および ESS 設定をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed illegal-ibss-ess quiet 360

6.1.88 malformed invalid-address-combination

Syntax

malformed invalid-address-combination [**quiet** *quiet-value*]

undo malformed invalid-address-combination

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な送信元アドレスのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な送信元アドレスを検出してもアラームを引き起こしません。

説明

malformed invalid-address-combination コマンドは無効な送信元アドレスをもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-address-combination コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。WIPS は以下の条件において、フレームを異常とみなします。

- フレームの TO DS が 1 の場合。（フレームがクライアントにより AP に送信されたことを示します）
- フレームの送信元 MAC アドレスがマルチキャストアドレスもしくはブロードキャストアドレスの場合。

例

無効な送信元アドレスをもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed invalid-address-combination quiet 360

6.1.89 malformed invalid-assoc-req

Syntax

malformed invalid-assoc-req [**quiet** *quiet-value*]

undo malformed invalid-assoc-req

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常紐付け要求フレームのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常紐付け要求フレームを検出してもアラームを引き起こしません。

説明

malformed invalid-assoc-req コマンドは異常紐付け要求フレームを検出するように、WIPS を有効にします。

undo malformed invalid-assoc-req コマンドはデフォルトに戻します。

この機能は紐付け要求フレームに適用できます。フレーム内の SSID 長が 0 である場合、WIPS はフレームを異常とみなします。

例

異常紐付け要求フレームを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed invalid-assoc-req quiet 360

6.1.90 malformed invalid-auth

Syntax

malformed invalid-auth [**quiet** *quiet-value*]

undo malformed invalid-auth

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常認証要求フレームのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常認証要求フレームを検出してもアラームを引き起こしません。

説明

malformed invalid-auth コマンドは異常認証要求フレームを検出するように、WIPS を有効にします。

undo malformed invalid-auth コマンドはデフォルトに戻します。

この機能は認証要求フレームに適用できます。WIPS は以下の条件において、フレームを異常とみなします。

- 認証アルゴリズム番号が 802.11 プロトコルと一致せず、3 より大きい場合。
- 認証トランザクションシーケンス番号が 1 であり、状態コードが 0 で無い場合。（認証トランザクションシーケンス番号は、クライアントと AP 間の認証処理を示します。）
- 認証トランザクションシーケンス番号が 4 より大きい場合。

例

異常認証要求フレームを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed invalid-auth quiet 360

6.1.91 malformed invalid-deauth-code

Syntax

malformed invalid-deauth-code [**quiet** *quiet-value*]

undo malformed invalid-deauth-code

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な認証取り消しコードのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な認証取り消しコードを検出してもアラームを引き起こしません。

説明

malformed invalid-deauth-code コマンドは無効な認証取り消しコードをもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-deauth-code コマンドはデフォルトに戻します。

この機能は認証取り消しフレームに適用できます。フレーム内の原因コードが 0、もしくは 67～65535 の範囲内である場合、WIPS はフレームを異常とみなします。

例

無効な認証取り消しコードをもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed invalid-deauth-code quiet 360

6.1.92 malformed invalid-disassoc-code

Syntax

malformed invalid-disassoc-code [**quiet** *quiet-value*]

undo malformed invalid-disassoc-code

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な紐付け取り消しコードのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な紐付け取り消しコードを検出してもアラームを引き起こしません。

説明

malformed invalid-disassoc-code コマンドは無効な紐付け取り消しコードをもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-disassoc-code コマンドはデフォルトに戻します。

この機能は紐付け取り消しフレームに適用できます。フレーム内の原因コードが 0、もしくは 67～65535 の範囲内である場合、WIPS はフレームを異常とみなします。

例

無効な紐付け取り消しコードをもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed invalid-disassoc-code quiet 360

6.1.93 malformed invalid-ht-ie

Syntax

malformed invalid-ht-ie [**quiet** *quiet-value*]

undo malformed invalid-ht-ie

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常 HT IE のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常 HT IE を検出してもアラームを引き起こしません。

説明

malformed invalid-ht-ie コマンドは異常 HT IE をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-ht-ie コマンドはデフォルトに戻します。

この機能はビーコンフレーム、プローブ応答フレーム、紐付け応答フレーム、再紐付け応答フレームに適用できます。WIPS は以下の条件において、フレームを異常とみなします。

- HT ケーパビリティ IE の SM 電力節約値が 2 である場合。
- HT オペレーション IE のセカンダリチャネルオフセット値が 2 である場合。

例

異常 HT IE をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed invalid-ht-ie quiet 360

6.1.94 malformed invalid-ie-length

Syntax

malformed invalid-ie-length [**quiet** *quiet-value*]

undo malformed invalid-ie-length

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な IE 長のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な IE 長を検出してもアラームを引き起こしません。

説明

malformed invalid-ie-length コマンドは無効な IE 長をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-ie-length コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。フレーム内の IE 長が 802.11 プロトコルと一致しない場合、WIPS はフレームを異常とみなします。

例

無効な IE 長をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed invalid-ie-length quiet 360

6.1.95 malformed invalid-pkt-length

Syntax

malformed invalid-pkt-length [**quiet** *quiet-value*]

undo malformed invalid-pkt-length

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効なパケット長のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効なパケット長を検出してもアラームを引き起こしません。

説明

malformed invalid-pkt-length コマンドは無効なパケット長をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-pkt-length コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。パケットペイロード解析後に IE の残存長が 0 で無い場合、WIPS はフレームを異常とみなします。

例

無効なパケット長をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed invalid-pkt-length quiet 360

6.1.96 malformed large-duration

Syntax

malformed large-duration [**quiet** *quiet-value* | **threshold** *value*]

undo malformed large-duration

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がオーバーサイズな期間のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にオーバーサイズな期間を検出してもアラームを引き起こしません。

threshold *threshold-value*: WIPS がオーバーサイズな期間を判断し、アラームをあげるために、期間のサイズを指定します。*value* 引数の値の範囲は 1～32767 です。デフォルト値は 5000 です。

説明

malformed large-duration コマンドはオーバーサイズな期間をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed large-duration コマンドはデフォルトに戻します。

この機能はユニキャスト管理フレーム、ユニキャストデータフレーム、RTS フレーム、CTS フレーム、ACK フレームに適用できます。フレーム内の期間の値が指定されたしきい値より大きい場合、WIPS はフレームを異常とみなします。

例

オーバーサイズな期間をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed large-duration quiet 360

6.1.97 malformed null-probe-resp

Syntax

malformed null-probe-resp [**quiet** *quiet-value*]

undo malformed null-probe-resp

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常プローブ応答フレームのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常プローブ応答フレームを検出してもアラームを引き起こしません。

説明

malformed null-probe-resp コマンドは異常プローブ応答フレームを検出するように、WIPS を有効にします。

undo malformed null-probe-resp コマンドはデフォルトに戻します。

この機能はプローブ応答フレームに適用できます。フレームがメッシュフレームでなく、SSID 長が 0 である場合、WIPS はフレームを異常とみなし、パケットは異常パケットとみなします。

例

異常プローブ応答フレームを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed null-probe-resp quiet 360

6.1.98 malformed overflow-eapol-key

Syntax

malformed overflow-eapol-key [**quiet** *quiet-value*]

undo malformed overflow-eapol-key

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がオーバーサイズな EAPOL 鍵のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にオーバーサイズな EAPOL 鍵を検出してもアラームを引き起こしません。

説明

malformed overflow-eapol-key コマンドはオーバーサイズな EAPOL 鍵をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed overflow-eapol-key コマンドはデフォルトに戻します。

この機能は EAPOL 鍵フレームに適用できます。フレーム内の TO DS が 1 で、鍵長が 0 より大きい場合、WIPS はフレームを異常とみなします。悪意ある EAPOL 鍵フレームにより DOS 攻撃を受ける恐れがあります。

例

オーバーサイズな EAPOL 鍵をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed overflow-eapol-key quiet 360

6.1.99 malformed overflow-ssid

Syntax

malformed overflow-ssid [**quiet** *quiet-value*]

undo malformed overflow-ssid

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がオーバーサイズな SSID のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にオーバーサイズな SSID 鍵を検出してもアラームを引き起こしません。

説明

malformed overflow-ssid コマンドはオーバーサイズな SSID をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed overflow-ssid コマンドはデフォルトに戻します。

この機能はビーコンフレーム、プローブ要求フレーム、プローブ応答フレーム、紐付け要求フレームに適用できます。フレーム内の SSID 長が 32 より大きく、802.11 プロトコルに一致していない場合、WIPS はフレームを異常とみなします。

例

オーバーサイズな SSID をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed overflow-ssid quiet 360

6.1.100 malformed redundant-ie

Syntax

malformed redundant-ie [**quiet** *quiet-value*]

undo malformed redundant-ie

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が冗長な IE のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に冗長な IE を検出してもアラームを引き起こしません。

説明

malformed redundant-ie コマンドは冗長な IE をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed redundant-ie コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。フレーム内の IE がフレームにとって必要な IE でも予備の IE でもない場合、WIPS はフレームを異常とみなします。

例

冗長な IE をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed redundant-ie quiet 360

6.1.101 man-in-the-middle

Syntax

man-in-the-middle [**quiet** *quiet-value*]

undo man-in-the-middle

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が MITM（Man-In-The-Middle）攻撃のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に MITM 攻撃を検出してもアラームを引き起こしません。

説明

man-in-the-middle コマンドは MITM 攻撃検出を有効にします。

undo man-in-the-middle コマンドは MITM 攻撃検出を無効にします。

MITM 攻撃検出を有効にする前にハニーポット AP 検出を有効にしてください。

例

MITM 攻撃検出を有効にします。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] honeypot-ap

[AC-wips-dtc-home] man-in-the-middle

6.1.102 manual-classify mac-address

Syntax

manual-classify mac-address *mac-address* { **authorized-ap** | **external-ap** | **misconfigured-ap** | **rogue-ap** }

undo manual-classify mac-address { *mac-address* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

mac-address: AP の MAC アドレスを H-H-H 形式で指定します。

authorized-ap: AP を許可された AP として指定します。

external-ap: AP を外部 AP として指定します。

misconfigured-ap: AP を間違って設定された AP として指定します。

rogue-ap: AP を不正な AP として指定します。

all: すべての AP を指定します。

説明

manual-classify mac-address コマンドは AP に対してカテゴリを設定します。

undo manual-classify mac-address コマンドはデフォルトに戻します。

例

MAC アドレスが 000f-00e2-0001 の AP を許可された AP として設定します。

<AC> system-view

[AC] wips

[AC-wips] classification policy home

[AC-wips-cls-home] manual-classify mac-address 000f-00e2-0001 authorized-ap

6.1.103 omerta

Syntax

omerta [**quiet** *quiet-value*]

undo omerta

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が Omerta 攻撃のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に Omerta 攻撃を検出してもアラームを引き起こしません。

説明

omerta コマンドは Omerta 攻撃検出を有効にします。

undo omerta コマンドは Omerta 攻撃検出を無効にします。

例

Omerta 攻撃検出を有効にします。遅延時間を 100 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] omerta quiet 100

6.1.104 oui

Syntax

oui *oui-info*

undo oui

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

oui-info: OUI 情報を XXXXXX 形式で指定します。大文字と小文字を区別しません。16 進数で指定します。

説明

oui コマンドは AP の OUI 情報と整合するように AP 分類ルールを設定します。

undo oui コマンドはデフォルトに戻します。

例

AP を OUI **000fe4** と整合するために AP classification rule 1 を設定します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

[AC-wips-cls-rule-1] oui 000fe4

6.1.105 pattern

Syntax

pattern *pattern-number* **offset** *offset-value* **mask** *mask value1* [**to** *value2*] [**from-payload**]

undo pattern { *pattern-number* | **all** }

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

pattern-number: 0～65535 の範囲の数字で指定されたフレームのビットと一致するサブ署名を指定します。

offset *offset-value*: 指定されたビットから参照ビットまでのオフセットを指定します。*offset-value* 引数の値の範囲は 0～2346 ビットです。参照ビットは、フレームヘッド（デフォルト）もしくはフレームペイロードの最初のビットになることができます。

mask *mask*: 指定されたビットで AND 演算に使用される 2 バイトマスクを指定します。マスクは 16 進数形式です。マスクの値の範囲は 0～ffff です。

value1 [**to** *value2*]: ビット数の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、どちらも 0～65535 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

from-payload: 参照ビットとしてフレームペイロードの最初のビットを指定します。このキーワードを指定しない場合、フレームヘッドの最初のビットは参照ビットになります。

説明

pattern コマンドは指定されたフレームのビットと整合するようにサブ署名を設定します。

undo pattern コマンドはデフォルトに戻します。

例

フレームヘッドの第 2 ビットと第 3 ビットが整合するようにサブ署名を設定します。フレームの第 2 ビットと第 3 ビットの値が 0x0015～0x0020 の範囲内の場合、フレームはサブ署名と整合します。

<AC> system-view

[AC] wips

[AC-wips] signature rule 1

[AC-wips-sig-rule-1] pattern 1 offset 8 mask ffff 15 to 20

6.1.106 permit-channel

Syntax

permit-channel *channel-id-list*

undo permit-channel { *channel-id-list* | **all** }

デフォルト

設定なし

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

channel-id-list: 許可された 10 個までのチャネルアイテムの空間分離リストを指定します。各アイテムは、*value1* **to** *value2* の形式でチャネル番号もしくはチャネル番号の範囲を指定します。チャネル番号の範囲は 1～224 です。*value2* 引数の値は *value1* 引数の値以上でなければなりません。

all: 許可されたすべてのチャネルを指定します。

説明

permit-channel コマンドは許可されたチャネルリストに 1 つあるいは複数のチャネルを追加します。

undo permit-channel コマンドは許可されたチャネルリストから指定されたチャネルあるいはすべてのチャネルを削除します。

WIPS がすべてのチャネルを禁止されたチャネルとして扱うことを防ぐため、禁止されたチャネル検出を設定する前に、このコマンドを使用して許可されたチャネルリストを設定します。

例

チャネル 1 を許可されたチャネルリストに追加します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] permit-channel 1

関連コマンド

prohibited-channel

6.1.107 power-save

Syntax

power-save [**interval** *interval-value* | **minoffpacket** *packet-value* | **onoffpercent** *percent-value* | **quiet** *quiet-value*] *

undo power-save

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: パワーセーブフレームのための統計値収集間隔を指定します。*interval-value* 引数の値は 1～3600 秒です。デフォルト値は 10 秒です。

minoffpacket *packet-value*: パワーセーブ攻撃分析を引き起こすパワーセーブ off フレームの数のしきい値を指定します。クライアントからの off フレームの数がしきい値の達すると、WIPS はパワーセーブ攻撃が発生したかどうか判断するために、パワーセーブフレームを分析します。値の範囲は 10～150 です。デフォルト値は 50 です。

onoffpercent *percent-value*: クライアントからのパワーセーブ on フレームと off フレームの比率のしきい値を指定します。しきい値に達すると WIPS はパワーセーブ攻撃のアラームを引き起こします。値の範囲は 0～100 です。デフォルト値は 80 です。

quiet *quiet-value*: WIPS がパワーセーブ攻撃のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にパワーセーブ攻撃を検出してもアラームを引き起こしません。

説明

power-save コマンドはパワーセーブ攻撃検出を有効にします。

undo power-save コマンドはパワーセーブ攻撃検出を無効にします。

例

パワーセーブ攻撃検出を有効にします。*interval-value*、*packet-value*、*percent-value*、*quiet-value* の値をそれぞれ、20、20、90、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] power-save interval 20 minoffpacket 20 onoffpercent 90 quiet 100

6.1.108 prohibited-channel

Syntax

prohibited-channel [**quiet** *quiet-value*]

undo prohibited-channel

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が禁止されたチャネルのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に禁止されたチャネルを検出してもアラームを引き起こしません。

説明

prohibited-channel コマンドは禁止されたチャネル検出を有効にします。

undo prohibited-channel コマンドは禁止されたチャネル検出を無効にします。

WIPS がすべてのチャネルを禁止されたチャネルとして扱うことを防ぐため、禁止されたチャネル検出を設定する前に、**permit-channel** コマンドを使用して許可されたチャネルリストを設定します。

例

禁止されたチャネル検出を有効にします。遅延時間を 100 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] prohibited-channel quiet 100

関連コマンド

permit-channel

6.1.109 report-interval

Syntax

report-interval *interval*

undo report-interval

デフォルト

30000 ミリ秒

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval: センサが AC に検出した装置の情報を通知する間隔を指定します。設定範囲は 1000～300000 ミリ秒です。

説明

report-interval コマンドはセンサが AC に検出した装置の情報を通知する間隔を設定します。

undo report-interval コマンドはデフォルトに戻します。

例

センサが AC に検出した装置の情報を通知する間隔を 10000 ミリ秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] report-interval 10000

6.1.110 reset wips statistics

Syntax

reset wips statistics

View

User view

定義済みユーザロール

network-admin

説明

reset wips statistics コマンドはすべてのセンサから収集した情報を削除します。

例

すべてのセンサから収集した情報を消去します。

<AC> reset wips statistics

関連コマンド

display wips statistics receive

6.1.111 reset wips virtual-security-domain

Syntax

reset wips virtual-security-domain *vsd-name* **device** { **ap** { **all** | **mac-address** *mac-address* } | **client** { **all** | **mac-address** *mac-address* } | **all** }

View

User view

定義済みユーザロール

network-admin

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

device: 装置のエントリを消去します。

ap: AP のエントリを消去します。

all: すべての AP のエントリを消去します。

mac-address *mac-address*: AP のエントリを消去します。*mac-address* 引数は AP の MAC アドレスをあらわします。

client: クライアントのエントリを消去します。

all: すべてのクライアントのエントリを消去します。

mac-address *mac-address*: クライアントのエントリを消去します。*mac-address* 引数はクライアントの MAC アドレスをあらわします。

all: すべての AP とクライアントのエントリを消去します。

説明

reset wips virtual-security-domain コマンドは VSD にある学習した AP もしくはクライアントのエントリを削除します。

例

VSD **aaa** にある学習した AP とクライアントのエントリを消去します。

<AC> reset wips virtual-security-domain aaa device all

関連コマンド

display wips virtual-security-domain device

6.1.112 reset wips virtual-security-domain countermeasure record

Syntax

reset wips virtual-security-domain *vsd-name* **countermeasure record**

View

User view

定義済みユーザロール

network-admin

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

reset wips virtual-security-domain countermeasure record コマンドは WIPS が不正な装置に対して講じた対策に関する情報を消去します。

例

VSD **aaa** のために WIPS が不正な装置に対して講じた対策に関する情報を消去します。

<AC> reset wips virtual-security-domain aaa countermeasure record

関連コマンド

display wips virtual-security-domain countermeasure record

6.1.113 reset wlan nat-detect

Syntax

reset wlan nat-detect

View

User view

定義済みユーザロール

network-admin

network-operator

説明

reset wlan nat-detect コマンドは NAT を設定したクライアントに関する情報を削除します。

例

NAT を構成したクライアントに関する情報をクリアします。

<AC> reset wlan nat-detect

関連コマンド

display wlan nat-detect

6.1.114 rssi

Syntax

rssi *value1* [**to** *value2*]

undo rssi

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

value1 [**to** *value2*]: AP の RSSI の値の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、どちらも 0～100 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

説明

rssi コマンドは AP の RSSI と整合するように AP 分類ルールを設定します。

undo rssi コマンドはデフォルトに戻します。

例

AP が 20～40 の RSSI と整合するように AP classification rule 1 を設定します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

[AC-wips-cls-rule-1] rssi 20 to 40

6.1.115 rssi-change-threshold

Syntax

rssi-change-threshold *threshold-value*

undo rssi-change-threshold

デフォルト

20

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

threshold-value: 装置検出の RSSI 相違のしきい値を指定します。設定範囲は 1～100 です。

説明

rssi-change-threshold コマンドは装置検出の RSSI 相違のしきい値を設定します。

undo rssi-change-threshold コマンドはデフォルトに戻します。

例

装置検出の RSSI 相違のしきい値を 80 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] rssi-change-threshold 80

6.1.116 rssi-threshold

Syntax

rssi-threshold { **ap** *ap-rssi-value* | **client** *client-rssi-value* }

undo rssi-threshold { **ap** | **client** }

デフォルト

設定なし

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

ap *ap-rssi-value*: AP の RSSI しきい値を指定します。設定範囲は 1～100 です。

client *client-rssi-value*: クライアントの RSSI しきい値を指定します。設定範囲は 1～100 です。

説明

rssi-threshold コマンドは装置検出の RSSI しきい値を設定します。

undo rssi-threshold コマンドはデフォルトに戻します。

例

信号強度が 80 を超過している AP を検出するために WIPS を設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] rssi-threshold ap 80

6.1.117 security

Syntax

security { **equal** | **include** } { **clear** | **wep** | **wpa** | **wpa2** }

undo security

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

equal: 指定されたセキュリティモードと等しいセキュリティモードと整合します。

include: 指定されたセキュリティモードを含むセキュリティモードと整合します。

clear: 消去するセキュリティモードを指定します。

wep: WEP セキュリティモードを指定します。

wpa: WPA セキュリティモードを指定します。

wpa2: WPA 2 セキュリティモードを指定します。

説明

security コマンドは AP に使用されるセキュリティモードと整合するように AP 分類ルールを設定します。

undo security コマンドはデフォルトに戻します。

例

WEP セキュリティモードを使用する AP と整合するように AP classification rule 1 を設定します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

[AC-wips-cls-rule-1] security equal wep

6.1.118 select sensor all

Syntax

select sensor all

undo select sensor all

デフォルト

直近で攻撃者を検出したセンサのみ、その攻撃者に対して対策を講じます。

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

select sensor all コマンドは攻撃者を検出するすべてのセンサを有効にします。

undo select sensor all コマンドは設定を削除します。

例

攻撃者に対して対策を講じるために、攻撃者を検出するすべてのセンサを有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-ctm-home] select sensor all

6.1.119 seq-number

Syntax

seq-number *seq-value1* [**to** *seq-value2*]

undo seq-number

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

seq-value1 [**to** *seq-value2*]: フレームのシーケンス番号の範囲を指定します。*seq-value1* 引数と *seq-value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*seq-value1* 引数と *seq-value2* 引数の値の範囲は、どちらも 0～4095 です。ただし、*seq-value2* 引数の値は *seq-value1* 引数の値より大きくなければなりません。

説明

seq-number コマンドはシーケンス番号をもつフレームと整合するサブ署名を設定します。

undo seq-number コマンドはデフォルトに戻します。

例

シーケンス番号 100 をもつフレームと整合するサブ署名を設定します。

<AC> system-view

[AC] wips

[AC-wips] signature rule 1

[AC-wips-sig-rule-1] seq-number 100

6.1.120 signature policy

Syntax

signature policy *policy-name*

undo signature policy *policy-name*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

policy-name: 署名ポリシの名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

signature policy コマンドは署名ポリシを作成し、その view に移行します。指定された署名ポリシがすでに存在する場合、signature policy view に移行します。

undo signature policy コマンドは署名ポリシを削除します。

例

署名ポリシ **home** を作成し、その view に移行します。

<AC> system-view

[AC] wips

[AC-wips] signature policy home

6.1.121 signature rule

Syntax

signature rule *rule-id*

undo signature rule *rule-id*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

rule-id: 署名の ID を指定します。範囲は 1～65535 です。

説明

signature rule コマンドは署名を作成し、その view に移行します。指定された署名がすでに存在する場合、signature view に移行します。

undo signature rule コマンドは署名を削除します。

例

signature 1 を作成し、その view に移行します。

<AC> system-view

[AC] wips

[AC-wips] signature rule 1

6.1.122 soft-ap

Syntax

soft-ap [**convert-time** *time-value*]

undo soft-ap

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

convert-time *time-value*: ソフト AP がクライアントと AP の役割を切り替える間隔を指定します。*time-value* 引数の値の範囲は 5～600 秒です。デフォルト値は 10 秒です。

説明

soft-ap コマンドはソフト AP 検出を有効にします。

undo soft-ap コマンドはソフト AP 検出を無効にします。

例

ソフト AP 検出を有効にします。*time-value* 引数の値を 100 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] soft-ap convert-time 100

6.1.123 ssid (AP classification rule view)

Syntax

ssid [**case-sensitive**] [**not**] { **equal** | **include** } *ssid-string*

undo ssid

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

case-sensitive: SSID の大文字、小文字を区別します。

not: 指定された SSID と一致しない SSID、もしくは指定された SSID を含まない SSID を整合します。

equal: 指定された SSID と一致する SSID を整合します。

include: 指定された SSID を含む SSID を整合します。

ssid-string: SSID を指定します。大文字と小文字を区別します。文字数は 1～32 文字です。

説明

ssid コマンドは AP に対して無線装置の SSID を整合するように AP 分類ルールを設定します。

undo ssid コマンドはデフォルトに戻します。

例

SSID **abc** の無線サービスを使用した AP を整合するために AP classification rule 1 を設定します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

[AC-wips-cls-rule-1] ssid equal abc

6.1.124 ssid (signature view)

Syntax

ssid [**case-sensitive**] [**not**] { **equal** | **include** } *string*

undo ssid

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

case-sensitive: SSID の大文字、小文字を区別します。

not: 指定された SSID と一致しない SSID、もしくは指定された SSID を含まない SSID を整合します。

equal: 指定された SSID と一致する SSID を整合します。

include: 指定された SSID を含む SSID を整合します。

string: SSID を指定します。大文字と小文字を区別します。文字数は 1～32 文字です。

説明

ssid コマンドはフレームの SSID を整合するためにサブ署名を設定します。

undo ssid コマンドはデフォルトに戻します。

例

signature 1 に対して SSID **office** のフレームを整合するためにサブ署名を設定します。

<AC> system-view

[AC] wips

[AC-wips] signature rule 1

[AC-wips-sig-rule-1] ssid equal office

6.1.125 ssid-length

Syntax

ssid-length *length-value1* [**to** *length-value2*]

undo ssid-length

デフォルト

設定なし

View

Signature rule

定義済みユーザロール

network-admin

パラメータ

length-value1 [**to** *length-value2*]: SSID 長の値の範囲を指定します。*length-value1* 引数と *length-value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*length-value1* 引数と *length-value2* 引数の値の範囲は、どちらも 1～32 です。ただし、*length-value2* 引数の値は *length-value1* 引数の値より大きくなければなりません。

説明

ssid-length コマンドはフレームの SSID 長を整合するためにサブ署名を設定します。

undo ssid-length コマンドはデフォルトに戻します。

例

SSID 長が 10 のフレームを整合するためにサブ署名を設定します。

<AC> system-view

[AC] wips

[AC-wips] signature rule 1

[AC-wips-sig-1] ssid-length 10

6.1.126 trust mac-address

Syntax

trust mac-address *mac-address*

undo trust mac-address { *mac-address* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

mac-address: MAC アドレスを指定します。

all: すべての MAC アドレスを指定します。

説明

trust mac-address コマンドは許可された装置リストに AP もしくはクライアントの MAC アドレスを追加します。

undo trust mac-address コマンドは許可された装置リストから 1 つあるいはすべての MAC アドレスを削除します。

例

許可された装置リストに MAC アドレス **78AC-C0AF-944F** を追加します。

<AC> system-view

[AC] wips

[AC-wips] classification policy home

[AC-wips-cls-home] trust mac-address 78AC-C0AF-944F

6.1.127 trust oui

Syntax

trust oui *oui*

undo trust oui { *oui* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

oui: OUI の名前を指定します。大文字と小文字を区別しません。文字数は 6 文字です。

all: すべての OUI を指定します。

説明

trust oui コマンドは信頼された OUI リストに OUI を追加します。

undo trust oui コマンドは信頼された OUI リストから 1 つあるいはすべての OUI を削除します。

例

信頼された OUI リストに OUI **000fe4** と **000fe5** を追加します。

<AC> system-view

[AC] wips

[AC-wips] classification policy home

[AC-wips-cls-home] trust oui 000fe4

[AC-wips-cls-home] trust oui 000fe5

6.1.128 trust ssid

Syntax

trust ssid *ssid-name*

undo trust ssid { *ssid-name* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

ssid-name: SSID の名前を指定します。大文字と小文字を区別します。文字数は 1～32 文字です。

all: すべての SSID を指定します。

説明

trust ssid コマンドは信頼された SSID リストに SSID を追加します。

undo trust ssid コマンドは信頼された SSID リストから 1 つあるいはすべての SSID を削除します。

例

信頼された SSID リストに SSID **flood1** を追加します。

<AC> system-view

[AC] wips

[AC-wips] classification policy home

[AC-wips-cls-home] trust ssid flood1

6.1.129 unencrypted-authorized-ap

Syntax

unencrypted-authorized-ap [**quiet** *quiet-value*]

undo unencrypted-authorized-ap

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が暗号化されていない許可 AP を検出してアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デ

フォルトは 600 秒です。WIPS は遅延時間内に暗号化されていない許可 AP を検出してもアラームを引き起こしません。

説明

unencrypted-authorized-ap コマンドは暗号化されていない許可 AP 検出を有効にします。

undo unencrypted-authorized-ap コマンドは暗号化されていない許可 AP 検出を無効にします。

例

暗号化されていない許可 AP 検出を有効にします。遅延時間を 10 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] unencrypted-authorized-ap quiet 10

6.1.130 unencrypted-trust-client

Syntax

unencrypted-trust-client [**quiet** *quiet-value*]

undo unencrypted-trust-client

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が暗号化されていない許可クライアントを検出してアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に暗号化されていない許可クライアントを検出してもアラームを引き起こしません。

説明

unencrypted-trust-client コマンドは暗号化されていない許可クライアント検出を有効にします。

undo unencrypted-trust-client コマンドは暗号化されていない許可クライアント検出を無効にします。

例

暗号化されていない許可クライアント検出を有効にします。遅延時間を 10 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] unencrypted-trust-client quiet 10

6.1.131 up-duration

Syntax

up-duration *value1* [**to** *value2*]

undo up-duration

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

value1 [**to** *value2*]: AP の動作時間の値の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、どちらも 0～2592000 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

説明

up-duration コマンドは AP の動作時間と整合するように AP 分類ルールを設定します。

undo up-duration コマンドはデフォルトに戻します。

例

2000～40000 秒の動作時間の AP と整合するように AP 分類ルールを設定します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

[AC-wips-cls-rule-1] up-duration 2000 to 40000

6.1.132 virtual-security-domain

Syntax

virtual-security-domain *vsd-name*

undo virtual-security-domain *vsd-name*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

virtual-security-domain コマンドは VSD を作成し、その view に移行します。

undo virtual-security-domain コマンドは VSD を削除します。

例

VSD **office** を作成し、その view に移行します。

<AC> system-view

[AC] wips

[AC-wips] virtual-security-domain office

[AC-wips-vsd-office]

6.1.133 weak-iv

Syntax

weak-iv [**quiet** *quiet-value*]

undo weak-iv

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がウィーク IV のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にウィーク IV を検出してもアラームを引き起こしません。

説明

weak-iv コマンドはウィーク IV 検出を有効にします。

undo weak-iv コマンドはデフォルトに戻します。

例

ウィーク IV 検出を有効にします。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] weak-iv

6.1.134 windows-bridge

Syntax

windows-bridge [**quiet** *quiet-value*]

undo windows-bridge

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が Windows ブリッジを検出してアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に Windows ブリッジを検出してもアラームを引き起こしません。

説明

windows-bridge コマンドは Windows ブリッジ検出を有効にします。

undo windows-bridge コマンドは Windows ブリッジを無効にします。

例

Windows ブリッジ検出を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] windows-bridge quiet 360

6.1.135 wips

Syntax

wips

undo wips

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

説明

wips コマンドは WIPS view に移行します。

undo wips コマンドは WIPS view 内の設定をすべて削除します。

例

WIPS view に移行します。

<AC> system-view

[AC] wips

[AC-wips]

6.1.136 wips enable

Syntax

wips enable

undo wips enable

デフォルト

Radio view では、無線が AP group radio view で設定を使用します。

AP group radio view では、WIPS は無効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

説明

wips enable コマンドは WIPS を有効にします。

undo wips enable コマンドはデフォルトに戻します。

無線通信と WIPS センサは同じ Radio 上での併用をサポートしています。

無線通信と WIPS センサを併用している Radio の WIPS スキャンは、通信への影響を与えないために、端末との通信のないタイミングで行われます。

また、無線通信と WIPS センサが有効な Radio に対する通信、および端末の接続に対しては、通信を優先するため WIPS 検出はできません。

例

AP **ap1** の無線 1 に対して WIPS を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] wips enable

AP group **apgroup1** のモデル **QX-W1020** を持つ AP の無線 1 に対して WIPS を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] wips enable

6.1.137 wips virtual-security-domain

Syntax

wips virtual-security-domain *vsd-name*

undo wips virtual-security-domain

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、AP グループは VSD に追加されません。

View

AP view

定義済みユーザロール

network-admin

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

wips virtual-security-domain コマンドは AP を VSD に追加します。

undo wips virtual-security-domain コマンドは AP を VSD から削除します。

例

VSD **office** に AP を追加します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] wips virtual-security-domain office

AP group **apgroup1** を VSD **office** に追加します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] wips virtual-security-domain office

6.1.138 wireless-bridge

Syntax

wireless-bridge [**quiet** *quiet-value*]

undo wireless-bridge

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無線ブリッジを検出してアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に無線ブリッジを検出してもアラームを引き起こしません。

説明

wireless-bridge コマンドは無線ブリッジ検出を有効にします。

undo wireless-bridge コマンドは無線ブリッジを無効にします。

例

無線ブリッジ検出を有効にします。遅延時間を 100 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] wireless-bridge quiet 100

6.1.139 wlan nat-detect

Syntax

wlan nat-detect { **disable** | **enable** }

undo wlan nat-detect

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、NAT を設定したクライアントの検出は無効になっています。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: NAT が設定されているクライアントの検出を無効にします。

enable: NAT が設定されているクライアントの検出を有効にします。

説明

wlan nat-detect enable コマンドは NAT を設定したクライアント検出を有効にします。

wlan nat-detect disable コマンドは NAT を設定したクライアント検出を無効にします。

undo wlan nat-detect コマンドを使用して、デフォルトに戻します。

デバイスは、NAT で設定されたクライアントを検出するとアラームを生成します。 検出された NAT 設定クライアントに関する情報を表示するには、**display wlan nat-detect** コマンドを使用します。

例

AP **ap1** 用に NAT が設定されているクライアントの検出を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] wlan nat-detect enable

AP group **aaa** の AP 用に NAT が設定されているクライアントの検出を有効にします。

<AC> system-view

[AC] wlan ap-group aaa

[AC-wlan-ap-group-aaa] wlan nat-detect enable

目次

このセクションのページは **2-x-x** です。

7 章 WLAN QoS の設定 7-1
7.1 WLAN QoS の設定コマンド 7-1
7.1.1 atf 7-1
7.1.2 bandwidth-guarantee 7-2
7.1.3 bandwidth-guarantee service-template 7-4
7.1.4 cac policy 7-5
7.1.5 client-rate-limit (radio view/AP group radio view) 7-7
7.1.6 client-rate-limit (service template view) 7-8
7.1.7 client-rate-limit { disable | enable } 7-9
7.1.8 client-rate-limit enable (v7.1.13 以前のみ) 7-11
7.1.9 display wlan wmm 7-12
7.1.10 edca auto 7-16
7.1.11 edca client (ac-be | ac-bk) 7-17
7.1.12 edca client (ac-vi | ac-vo) 7-18
7.1.13 edca radio 7-20
7.1.14 mu-edca client 7-22
7.1.15 qos priority 7-24
7.1.16 qos trust 7-24
7.1.17 reset wlan wmm 7-25
7.1.18 svp map-ac 7-26
7.1.19 u-apsd enable 7-27
7.1.20 wlan client-rate-limit 7-28
7.1.21 wlan max-bandwidth 7-30
7.1.22 wmm 7-31

7章 WLAN QoS の設定

7.1 WLAN QoSの設定コマンド

7.1.1 atf

🕮 **メモ：**

atf コマンドはソフトウェアバージョン 7.2.47 を含む以降のソフトウェアからサポートしています。
atf コマンドは QX-W1100 シリーズおよび QX-W1200 シリーズでのみサポートしています。

Syntax

atf { **disable** | **enable** }

undo atf

デフォルト

radio view は、AP group view の設定を使用します。

AP group radio view では、Air Time Fairness は無効です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: Air Time Fairness を無効にします。

enable: Air Time Fairness を有効にします。

説明

atf enable コマンドは Air Time Fairness を有効にします。

atf disable コマンドは Air Time Fairness を無効にします。

undo atf コマンドはデフォルトに戻します。

このコマンドを使用すると、高速クライアントでワイヤレスリソースを使用する機会が増えます。これにより、ネットワーク全体の転送効率が向上しますが、低速クライアントの転送効率が低下する可能性があります。

この機能を設定する場合は、アクセスクライアントの数と高速クライアントの転送効率を考慮してください。

この機能でネットワークの転送効率が向上するのは、AP からクライアント方向の通信のみです。

radio view の設定は、AP group radio view の設定よりも優先されます。

例

AP **ap1** の Radio 1 で Air Time Fairness を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] atf enable

AP group **apgroup1** の AP の Radio1 で Air Time Fairness を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1130

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] atf enable

7.1.2 bandwidth-guarantee

Syntax

bandwidth-guarantee { **disable** | **enable** }

undo bandwidth-guarantee

デフォルト

radio view は以下の通りです。

- AP group view のサービステンプレート設定が使用されている場合、AP は AP group view 内の設定を使用します。
- サービステンプレートが手動で無線に紐づけられている場合、帯域幅保証は無効になります。

AP group radio view では、帯域幅保証は無効です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 帯域保証を無効にします。

enable: 帯域保証を有効にします。

説明

bandwidth-guarantee enable コマンドは帯域保証を有効にします。

bandwidth-guarantee disable コマンドは帯域保証を無効にします。

undo bandwidth-guarantee コマンドはデフォルトに戻します。

このコマンドを使用すると、ネットワークが輻輳しているときに、同じ無線に関連付けられたクライアントが保証帯域幅を取得できるようになります。保証帯域幅を設定するには、**bandwidth-guarantee service-template** コマンドを使用します。

radio view の設定は、AP group radio view の設定よりも優先されます。

例

AP **ap1** の帯域保証を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] service-template 1

[AC-wlan-ap-ap1-radio-1] bandwidth-guarantee enable

AP group **apgroup1** の帯域保証を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] bandwidth-guarantee enable

関連コマンド

bandwidth-guarantee service-template

7.1.3 bandwidth-guarantee service-template

Syntax

bandwidth-guarantee service-template *service-template-name* **percent** *percent*

undo bandwidth-guarantee { **all** | **service-template** *service-template-name* }

デフォルト

radio view は以下の通りです。

- AP group view のサービステンプレート設定が使用されている場合、AP は AP group view 内の設定を使用します。
- サービステンプレートが手動で無線に紐づけられている場合、サービステンプレートに保証された帯域幅の割合は設定されません。

AP group radio view では、サービステンプレートに保証帯域幅の割合が設定されていません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

service-template *service-template-name*: サービステンプレートを名前で指定します。大文字と小文字を区別しない 1～63 文字です。指定したサービステンプレートが無線に紐づけられていることを確認してください。

percent *percent*: 総帯域幅に対する保証帯域幅の割合を指定します。*percent* 引数の値の範囲は 1～100 です。合計帯域幅は、無線の最大帯域幅を示します。保証帯域幅は、サービステンプレートに対応する BSS の最小帯域幅を示します。

all: すべてのサービステンプレートを指定します。

説明

bandwidth-guarantee service-template コマンドは指定されたサービステンプレートの保証帯域幅の割合を設定します。

undo bandwidth-guarantee service-template コマンドは指定されたサービステンプレートの保証帯域幅設定をキャンセルします。

このコマンドを有効にするには、帯域保証機能が有効になっていることを確認してください。

同じ無線に紐づけられているすべてのサービステンプレートで、保証帯域幅の合計が100%を超えることはできません。

radio view の設定は、AP group radio view の設定よりも優先されます。

例

radio view でサービステンプレート 1 の保証帯域幅の割合を 30%に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] service-template 1

[AC-wlan-ap-ap1-radio-1] bandwidth-guarantee service-template 1 percent 30

[AC-wlan-ap-ap1-radio-1] bandwidth-guarantee enable

AP group radio view で、サービステンプレート 1 の保証帯域幅の割合を 30%に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] bandwidth-guarantee enable

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] service-template 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] bandwidth-guarantee service-template 1 percent 30

関連コマンド

- **bandwidth-guarantee enable**
- **wlan mac-bandwidth**

7.1.4 cac policy

Syntax

cac policy { **channelutilization** [*channelutilization-value*] | **client** [*client-number*] }

undo cac policy

デフォルト

radio view は、AP group view の設定を使用します。

AP group radio view では、クライアントベースのアドミッションポリシが使用され、許可されるクライアントの最大数は 20 です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

channelutilization: チャネル使用率に基づくアドミッションポリシを指定します。

channelutilization-value: 最大チャネル使用率を 0～100%の範囲で指定します。最大チャネル使用率は、一定の時間内に受信された AC-VO および AC-VI トラフィックの有効時間に対する中間時間を参照します。有効時間とは、データの送受信に使用可能な時間を指します。デフォルトでは、最大チャネル使用率は 65%です。

client: クライアントベースのアドミッションポリシを指定します。

client-number: 接続できるクライアントの最大数を 0～64 の範囲で指定します。クライアントは、AC-VO および AC-VI の両方のキューを使用している場合、1 つのクライアントとしてカウントされます。

説明

cac policy コマンドは Connect Admission Control（CAC）ポリシを設定します。

undo cac policy コマンドはデフォルトに戻します。

radio view の設定は、AP group radio view の設定よりも優先されます。

CAC ポリシは、AC-VO キューおよび AC-VI キューでのみ有効です。

例

CAC のチャネル使用率に基づくアドミッションポリシを設定し、最大チャネル使用率を 70%に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] cac policy channelutilization 70

CAC のチャネル使用に基づくアドミッションポリシを設定し、AP group **apgroup1** の最大チャネル使用率を 70%に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] cac policy channelutilization 70

7.1.5 client-rate-limit (radio view/AP group radio view)

Syntax

client-rate-limit { **inbound** | **outbound** } **mode** { **dynamic** | **static** } **cir** *cir*

undo client-rate-limit { **inbound** | **outbound** }

デフォルト

radio view は、AP group view の設定を使用します。

AP group radio view は、無線ベースのクライアントレート制限は設定されていません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

inbound: 受信トラフィックのレートを制限します。

outbound: 送信トラフィックのレートを制限します。

dynamic: 動的レート制限モードを指定します。このモードでは、各クライアントの最大レートは、合計最大レートをクライアント数で割った値になります。

static: 静的レート制限モードを指定します。各クライアントの最大レートは固定です。

cir *cir*: CIR を Kbps で指定します。*cir* 引数の値は 16～1700000 の範囲です。このオプションは、静的レート制限モードの場合は各クライアントの最大レートを設定し、動的レート制限モードの場合はすべてのクライアントの最大レートを設定します。

説明

client-rate-limit コマンドは無線ベースのクライアントレート制限を設定します。

undo client-rate-limit コマンドはデフォルトに戻します。

このコマンドを有効にするには、無線ベースのクライアントレート制限が有効になっていることを確認します。

このコマンドを複数回繰り返して、受信トラフィックと送信トラフィックの両方のレートを制限できます。

radio view の設定は、AP group radio view の設定よりも優先されます。

例

radio view で無線 1 のクライアントレート制限を設定します。各クライアントの受信トラフィックに対して CIR を 567 Kbps に設定し、すべてのクライアントの送信トラフィックに対して CIR を 89 Kbps に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-1] client-rate-limit enable

[AC-wlan-ap-ap1-1] client-rate-limit inbound mode static cir 567

[AC-wlan-ap-ap1-1] client-rate-limit outbound mode dynamic cir 89

AP group radio view で無線 1 のクライアントレート制限を設定します。各クライアントの受信トラフィックに対して CIR を 567 Kbps に設定し、すべてのクライアントの送信トラフィックに対して CIR を 89 Kbps に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] client-rate-limit enable

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] client-rate-limit inbound mode static cir 567

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] client-rate-limit outbound mode dynamic cir 89

関連コマンド

client-rate-limit { **disable** | **enable** }

7.1.6 client-rate-limit (service template view)

Syntax

client-rate-limit { **inbound** | **outbound** } **mode** { d**ynamic** | **static** } **cir** *cir*

undo client-rate-limit { **inbound** | **outbound** }

デフォルト

サービステンプレートベースのクライアントレート制限は設定されていません。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

inbound: 受信トラフィックのレートを制限します。

outbound: 送信トラフィックのレートを制限します。

dynamic: 動的レート制限モードを指定します。このモードでは、各クライアントの最大レートは、合計最大レートをクライアント数で割った値になります。

static: 静的レート制限モードを指定します。各クライアントの最大レートは固定です。

cir *cir*: CIR を Kbps で指定します。cir 引数の値は 16～1700000 の範囲です。このオプションは、静的レート制限モードの場合は各クライアントの最大レートを設定し、動的レート制限モードの場合はすべてのクライアントの最大レートを設定します。

説明

client-rate-limit コマンドはサービステンプレートベースのクライアントレート制限を設定します。

undo client-rate-limit コマンドはデフォルトに戻します。

ソフトウェアバージョン 7.1.13 を含む以前のソフトウェアで本コマンドを有効にするためには、client-rate-limit enable が有効になっている必要があります。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは client-rate-limit enable は不要です。このコマンドを複数回繰り返して、受信トラフィックと送信トラフィックの両方のレートを制限できます。

例

サービステンプレート 1 のレート制限を設定します。各クライアントの受信トラフィックに対して CIR を 567 Kbps に設定します。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] client-rate-limit enable

[AC-wlan-st-1] client-rate-limit inbound mode static cir 567

関連コマンド

client-rate-limit enable

7.1.7 client-rate-limit { disable | enable }

Syntax

client-rate-limit { **disable** | **enable** }

undo client-rate-limit

デフォルト

radio view は、AP group view の設定を使用します。

AP group radio view は、無線ベースのクライアントレート制限が無効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 無線ベースのクライアントレート制限を無効にします。

enable: 無線ベースのクライアントレート制限を有効にします。

説明

client-rate-limit enable コマンドは無線ベースのクライアントレート制限を有効にします。

client-rate-limit disable コマンドは無線ベースのクライアントレート制限を無効にします。

undo client-rate-limit コマンドはデフォルトに戻します。

このコマンドは、無線に関連する WLAN クライアントのトラフィックレートを制限します。このコマンドはソフトウェアバージョン 7.1.13 を含む以前のソフトウェアでのみ設定が必要です。レート制限方向とレート制限レートを設定するには、**client-rate-limit** コマンドを使用します。

クライアントレート制限のために、異なるレート制限方式とレート制限モードを設定することができ、すべての設定が有効になります。これらの設定間のレート制限のうち最小値が、各クライアントに適用されます。

radio view の設定は、AP group radio view の設定よりも優先されます。

例

AP **ap1** の無線 1 のクライアントレート制限を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] client-rate-limit enable

AP group **apgroup1** の無線 1 のクライアントレート制限を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] client-rate-limit enable

関連コマンド

client-rate-limit (radio view/AP group radio view)

7.1.8 client-rate-limit enable (v7.1.13 以前のみ)

Syntax

client-rate-limit enable

undo client-rate-limit enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

client-rate-limit enable コマンドはサービステンプレートベースのクライアントレート制限を有効にします。

undo client-rate-limit enable コマンドはデフォルトに戻します。

このコマンドは、サービステンプレートに関連付けられている WLAN クライアントのトラフィックレート制限の設定を有効にします。このコマンドは v7.1.13 を含む以前のバージョンでのみ設定が必要です。レート制限方向とレート制限レートを設定するには、**client-rate-limit** コマンドを使用します。

クライアントレート制限のために、異なるレート制限方式とレート制限モードを設定することができ、すべての設定が有効になります。これらの設定間のレート制限のうち最小値が、各クライアントに適用されます。

例

サービステンプレート 1 のクライアントレート制限を有効にします。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] client-rate-limit enable

関連コマンド

client-rate-limit (Service template view)

7.1.9 display wlan wmm

Syntax

display wlan wmm { **radio** { **all** | **ap** *ap-name* } | **client** { **all** | **ap** *ap-name* | **mac-address** *mac-address* } }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての無線またはすべてのクライアントを指定します。

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

mac-address *mac-address*: クライアントの MAC アドレスを H-H-H 形式で指定します。

説明

display wlan wmm radio コマンドは無線の WMM 統計情報を表示します。

display wlan wmm client コマンドはクライアントの WMM 統計情報を表示します。

例

AP **test** の無線の WMM 統計情報を表示します。

<AC> display wlan wmm radio ap test

```
AP ID : 4   AP name : test

Radio : 1
Client EDCA updates : 0
QoS mode  : WMM
```

```
WMM status : Enabled
Radio max AIFSN    : 15              Radio max ECWmin : 10
Radio max TXOPLimit : 32767           Radio max ECWmax : 10
CAC information
Clients accepted                 : 0
  Voice                          : 0
  Video                          : 0
Total request mediumtime(µs)       : 0
  Voice(µs)                      : 0
  Video(µs)                      : 0
Calls rejected due to insufficient resources  : 0
Calls rejected due to invalid parameters     : 0
Calls rejected due to invalid mediumtime     : 0
Calls rejected due to invalid delaybound     : 0

Radio : 2
Client EDCA updates : 0
QoS mode  : WMM
WMM status: Disabled
Radio max AIFSN    : 15              Radio max ECWmin : 10
Radio max TXOPLimit : 32767           Radio max ECWmin : 10
CAC information
Client accepted                  : 0
  Voice                          : 0
  Video                          : 0
Total request mediumtime(µs)       : 0
  Voice(µs)                      : 0
  Video(µs)                      : 0
Calls rejected due to insufficient resources  : 0
Calls rejected due to invalid parameters     : 0
Calls rejected due to invalid mediumtime     : 0
Calls rejected due to invalid delaybound     : 0
```

表 7-1 コマンド出力

フィールド	説明
Client EDCA	クライアントのEDCAパラメータが更新された回数です。
QoS mode	• WMM
WMM status	• Enable • Disable
Radio max AIFSN	無線がサポートする最大AIFSNです。

フィールド	説明
Radio max ECWmin	無線がサポートする最大ECWminです。
Radio max TXOPLimit	無線がサポートする最大TXOPLimitです。
Radio max ECWmax	無線がサポートする最大ECWmaxです。
Total request mediumtime	AC-VOおよびAC-VIキューの合計要求中間時間(マイクロ秒単位)です。

#すべてのクライアントの WMM 統計情報を表示します。

<AC> display wlan wmm client all

```
MAC address : 000f-e23c-0001          SSID : service
QoS mode : WMM
APSD information :
  Max SP length : 7
  L: Legacy    T: Trigger      D: Delivery
  AC           AC-BK    AC-BE   AC-VI    AC-VO
  Assoc State   T|D     L      T|D      T|D
Statistics information :
  Uplink packets     : 0          Downlink packets  : 0
  Uplink bytes       : 0          Downlink bytes    : 0
  Downgrade packets      : 0          Discarded packets      : 0
  Downgrade bytes        : 0          Discarded bytes        : 0
TS information:
  AC                 : AC-VO       User priority            : 7
  TID                : 1           Direction                : Bidirectional
  PSB                : 0           Surplus bandwidth allowance : 1.0000
  Medium time (μs)     : 39          MSDU size (bytes)          : 1500
  Mean data rate (Kbps) : 10.000      Minimum PHY rate (Mbps)    : 11.000
  TS creation time     : 0h:0m:5s
  TS updating time     : 0h:0m:5s
  Uplink TS packets    : 0          Downlink TS packets        : 0
  Uplink TS bytes      : 0          Downlink TS bytes          : 0
```

表 7-2 コマンド出力

フィールド	説明
QoS mode	**WMM**はQoSモードを表します。 QoSモードが利用できない場合、このフィールドには**N/A**が表示されます。
Max SP length	最大サービス期間(SP)の長さです。

フィールド	説明
AC	• AC-VO • AC-VI • AC-BE • AC-BK
Assoc state	ACキューのAPSD属性です。 • **T**－ACキューがtrigger-enabledです。 • **D**－ACキューがdelivery-enabledです。 • **T**	**D**－ACキューは、trigger-enabledとdelivery-enabledの両方です。 • **L**－ACはレガシー属性のものです。
User priority	有線ネットワークからのパケットのユーザ優先度です。
TID	トラフィック識別子です。範囲は0～15です。
Direction	トラフィック方向です。 • Uplink • Downlink • Bidirectional
PSB	省電力動作です。 • **1**－U-APSD省電力モードです。 • **0**－従来の省電力モードです。
Surplus bandwidth allowance	余剰帯域幅のパーセンテージです。
Medium time	許容される中間時間(マイクロ秒)です。
MSDU size	平均MSDUサイズ(バイト)です。
Mean data rate	平均データ転送速度(Kbps)です。
Minimum PHY rate	最小物理伝送速度(Mbps)です。

関連コマンド

reset wlan wmm

7.1.10 edca auto

Syntax

edca auto { disable | enable }

undo edca auto

デフォルト

radio view は、AP group view で設定を使用します。

AP group radio view では、有効です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

説明

edca auto enable コマンドは EDCA パラメータの自動調整を有効にします。

edca auto disable コマンドは EDCA パラメータの自動調整を無効にします。

undo edca client コマンドはデフォルトに戻します。

radio view の設定は、AP group radio view の設定よりも優先されます。

この機能を有効にすると、オンラインクライアントの数に基づいて AC が AC-BE および AC-BK キューの EDCA パラメータを自動的に調整できるようになります。

EDCA パラメータを手動で設定している場合、この機能は動作しません。

例

EDCA パラメータの自動調整を有効にします

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] edca auto enable

AP group **apgroup1** の Radio1 で EDCA パラメータの自動調整を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] edca auto enable

関連コマンド

edca client (ac-be | ac-bk)

7.1.11 edca client (ac-be | ac-bk)

Syntax

edca client { **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *

undo edca client { **ac-be** | **ac-bk** }

デフォルト

radio view は、AP group view で設定を使用します。

AP group radio view で使用される、クライアントの AC-BE キューと AC-BK キューのデフォルトの EDCA パラメータ値を表 7-3 に示します。

表 7-3 クライアントの AC-BE キューと AC-BK キューのデフォルト EDCA パラメータ値

AC	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-BK	7	4	10	0
AC-BE	3	4	10	0

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

ac-be: AC-BE（ベストエフォート型トラフィック）キューを指定します。

ac-bk: AC-BK（バックグラウンドトラフィック）キューを指定します。

aifsn *aifsn-value*: AIFSN（arbitration inter-frame spacing number）を 1～15 の範囲で指定します。

ecwmin *ecwmin-value*: ECWmin（the exponent form of CWmin）を指数形式で 0～15 の範囲で指定します。

ecwmax *ecwmax-value*: ECWmax（the exponent form of CWmax）を指数形式で 0～15 の範囲で指定します。ECWmax の値は ECWmin の値より小さくすることはできません。

noack: No ACK ポリシを使用するように AC キューを設定します。デフォルトでは、No ACK ポリシが使用されます。

txoplimit *txoplimit-value*: TXOP Limit（transmission opportunity limit）値を 0～65535（32 マイクロ秒単位）の範囲で指定します。値が 0 の場合、クライアントはチャネルを保持するたびに 1 つのパケットしか送信できません。

説明

edca client コマンドはクライアントの AC-BE キューまたは AC-BK キューの EDCA パラメータを設定します。

undo edca client コマンドはデフォルトに戻します。

radio view の設定は、AP group radio view の設定よりも優先されます。

すべてのクライアントが 802.11b クライアントである場合、AC-BE キューと AC-BK キューのそれぞれに対して TXOP Limit 値を 0 に設定することを推奨します。

802.11b と 802.11g の両方のクライアントが WLAN に存在する場合、AC-BK と AC-BE のそれぞれのキューにデフォルトの TXOPLimit 値を使用することを推奨します。

例

AC-BE キューの AIFSN を 5 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] edca client ac-be aifsn 5

AP group **apgroup1** の AC-BE キューに対して AIFSN を 5 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] edca client ac-be aifsn 5

7.1.12 edca client (ac-vi | ac-vo)

Syntax

edca client { **ac-vi** | **ac-vo** } { **aifsn** *aifsn-value* | **cac** { **disable** | **enable** } | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *

undo edca client { **ac-vi** | **ac-vo** }

デフォルト

radio view は、AP group view で設定を使用します。

AP group radio view で使用される、クライアントの AC-VI キューと AC-VO キューのデフォルトの EDCA パラメータ値を表 7-4 に示します。

表 7-4 クライアントの AC-BE キューと AC-BK キューのデフォルト EDCA パラメータ値

AC	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-VI	2	3	4	94
AC-VO	2	2	3	47

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

ac-vi: AC-VI（ビデオトラフィック）キューを指定します。

ac-vo: AC-VO（音声トラフィック）キューを指定します。

aifsn *aifsn-value*: AIFSN（arbitration inter-frame spacing number）を 1～15 の範囲で指定します。

cac: CAC を指定します。AC-VO および AC-VI キューは CAC をサポートします。CAC はデフォルトで無効になっています。

disable: CAC を無効にします。

enable: CAC を有効にします。

ecwmin *ecwmin-value*: ECWmin（the exponent form of CWmin）を指数形式で 0～15 の範囲で指定します。

ecwmax *ecwmax-value*: ECWmax（the exponent form of CWmax）を指数形式で 0～15 の範囲で指定します。ECWmax の値は ECWmin の値より小さくすることはできません。

txoplimit *txoplimit-value*: TXOP Limit（transmission opportunity limit）値を 0～65535（32 マイクロ秒単位）の範囲で指定します。値が 0 の場合、クライアントはチャネルを保持するたびに 1 つのパケットしか送信できません。

説明

edca client コマンドはクライアントの AC-VI または AC-VO キューの EDCA パラメータを設定します。

undo edca client コマンドはデフォルトに戻します。

radio view の設定は、AP group radio view の設定よりも優先されます。

すべてのクライアントが 802.11b クライアントである場合、AC-VI および AC-VO キューの TXOPLimit 値をそれぞれ 188 と 102 に設定することを推奨します。

802.11b と 802.11g のそれぞれのクライアントが WLAN に存在する場合、AC-VI と AC-VO のそれぞれのキューにデフォルトの TXOPLimit 値を使用することを推奨します。

例

AC-VO キューの AIFSN を 3 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] edca client ac-vo aifsn 3

AP group **apgroup1** の AC-VO キューの AIFSN を 3 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] edca client ac-vo aifsn 3

7.1.13 edca radio

Syntax

edca radio { **ac-be** | **ac-bk** | **ac-vi** | **ac-vo** } { **ack-policy** { **noack** | **normalack** } | **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **noack** | **txoplimit** *txoplimit-value* } *

undo edca radio { **ac-be** | **ac-bk** | **ac-vi** | **ac-vo** }

デフォルト

radio view は、AP group view の設定を使用します。

AP group radio view は、デフォルトの EDCA パラメータ値を表 7-5 に示します。

表 7-5 EDCA パラメータのデフォルト値

AC	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-BK	7	4	10	0
AC-BE	3	4	6	0
AC-VI	1	3	4	94
AC-VO	1	2	3	47

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

ac-be: AC-BE（ベストエフォート型トラフィック）キューを指定します。

ac-bk: AC-BK（バックグラウンドトラフィック）キューを指定します。

ac-vi: AC-VI（ビデオトラフィック）キューを指定します。

ac-vo: AC-VO（音声トラフィック）キューを指定します。

ack-policy: AC キューの ACK ポリシを指定します。

noack: No ACK ポリシ（デフォルト）を指定します。

normalack: Normal ACK ポリシを指定します。

aifsn *aifsn-value*: AIFSN（Arbitration inter-frame spacing number）を 1～15 の範囲で指定します。

ecwmin *ecwmin-value*: ECWmin（the exponent form of CWmin）の指数形式を指定します。*ecwmin-value* 引数の値の範囲は 0～10 です。

ecwmax *ecwmax-value*: ECWmax（the exponent form of CWmax）の指数形式を指定します。*ecwmax-value* 引数の値の範囲は 0～10 です。ECWmax の値は ECWmin の値より小さくすることはできません。

txopimit *txoplimit-value*: TXOP Limit（Transmission opportunity limit）の値を 32 マイクロ秒単位で指定します。*txoplimit-value* 引数の値の範囲は 0～32767 です。値が 0 の場合、クライアントはチャネルを保持するたびに 1 つのパケットのみを送信できます。

説明

edca radio コマンドは EDCA パラメータを設定します。

undo edca radio コマンドはデフォルトに戻します。

radio view の設定は、AP group radio view の設定よりも優先されます。

802.11b 無線の場合、AC-BK、AC-BE、AC-VI、AC-VO キューの TXOP 制限値をそれぞれ 0、0、188、102 に設定することを推奨します。

例

無線 2 の radio view で、AC-VO キューの AIFSN を 2 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] edca radio ac-vo aifsn 2

AP group **apgroup1** の無線 2 の radio view で、AC-VO キューの AIFSN を 2 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] edca radio ac-vo aifsn 2

7.1.14 mu-edca client

🕮 **メモ**:

mu-edca client コマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。
mu-edca client コマンドは QX-W1100 シリーズおよび QX-W1200 シリーズでのみサポートしています。

Syntax

mu-edca client { ac-be | ac-bk | ac-vi | ac-vo } { aifsn *aifsn-value* **| ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* **| muedcatimer** *muedcatimer-value* **} ***

undo mu-edca client { ac-be | ac-bk | ac-vi | ac-vo }

デフォルト

radio view は、AP group view で設定を使用します。

AP group radio view では、MU EDCA パラメータは指定されていません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

ac-be: AC-BE（ベストエフォート型トラフィック）キューを指定します。

ac-bk: AC-BK（バックグラウンドトラフィック）キューを指定します。

ac-vi: AC-VI（ビデオトラフィック）キューを指定します。

ac-vo: AC-VO（音声トラフィック）キューを指定します。

aifsn *aifsn-value*: AIFSN（arbitration inter-frame spacing number）を 2～15 の範囲で指定します。

ecwmin *ecwmin-value*: ECWmin（the exponent form of CWmin）を 0～15 の範囲で指定します。

ecwmax *ecwmax-value*: ECWmax（the exponent form of CWmax）を 0～15 の範囲で指定します。ECWmax の値は ECWmin の値より小さくすることはできません。

muedcatimer *muedcatimer-value*: MU EDCA パラメータのタイムアウトを 1 から 255 TU (1 TU=1024 us) の範囲で指定します。

説明

mu-edca client コマンドは MU EDCA パラメータを設定します。

undo mu-**edca client** コマンドはデフォルトに戻します。

radio view の設定は、AP group radio view の設定よりも優先されます。

この機能を使用すると、802.11ax 無線と非 802.11 ax 無線の両方が存在する場合に、クライアントは 802.11ax パケットに対して異なる EDCA パラメータセットを使用して、非 802.11 ax パケットの公平な伝送を保証できます。

MU EDCA パラメータを設定すると、関連付けられた AP が 802.11 ax クライアントをトリガーしてデータを送信するときに、クライアントは MU EDCA パラメータの使用を選択できます。EDCA パラメータと比較して、MU EDCA パラメータは、より大きな aifsn、ecwmin、および ecwmax 値が指定され、待機時間と平均バックオフ時間を増やして 802.11 ax パケットの優先度を下げます。

システムは MU EDCA パラメータを使用するためのタイマーを設定します。タイマーの期限が切れる前に AP がクライアントにデータを送信するようにトリガーすると、タイマーはリセットされます。タイマーの期限が切れると、MU EDCA パラメータの代わりに、EDCA パラメータが 802.11 ax パケットに再び使用されます。

例

AC-BE キューの AIFSN を 5 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mu-edca client ac-be aifsn 5

AP group **apgroup1** の AC-BE キューに対して AIFSN を 5 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1120

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1120] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1120-radio-1] mu-edca client ac-be aifsn 5

7.1.15 qos priority

Syntax

qos priotity *priority-value*

undo qos priotity

デフォルト

0

View

Service template view

定義済みユーザロール

network-admin

パラメータ

priority-value: ポートプライオリティを 0～7 の範囲で指定します。値が大きいほど優先度が高くなります。

説明

qos priority コマンドはポートプライオリティを設定します。

undo qos priority コマンドはデフォルトに戻します。

ポートトラステッドモードが有効な場合、AP はポートプライオリティをサービステンプレートのすべてのパケットに割り当てます。

パケットトラステッドモードが有効な場合、このコマンドは有効になりません。

例

サービステンプレート 1 のポートプライオリティを 2 に設定します。

<AC> system

[AC] wlan service-template 1

[AC-wlan-st-1] qos priority 2

関連コマンド

qos trust

7.1.16 qos trust

Syntax

qos trust { **dot11e** | **dscp** }

undo qos trust

デフォルト

ポートプライオリティを信頼する

View

Service template view

定義済みユーザロール

network-admin

パラメータ

dot11e: 優先度マッピングのためにパケット内で運ばれる 802.11e 優先度を使用します。
dscp: 優先度マッピングのためにパケット内で運ばれる DSCP 優先度を使用します。

説明

qos trust コマンドはパケットトラステッドモードを有効にします。

undo qos trust コマンドはデフォルトに戻します。

この機能は、アップリンクパケットでのみ有効です。

例

プライオリティマッピングのためにパケットで伝送される 802.11e プライオリティを使用するようにサービステンプレート 1 を設定します。

<AC> system

[AC] wlan service-template 1

[AC-wlan-st-1] qos trust dot11e

関連コマンド

qos priority

7.1.17 reset wlan wmm

Syntax

reset wlan wmm { **client** { **all** | **ap** *ap-name* | **mac-address** *mac-address* } | **radio** { **all** | **ap** *ap-name* } }

View

ユーザ view

定義済みユーザロール

network-admin

パラメータ

client: クライアントの WMM 統計情報を削除します。

all: すべての無線またはクライアントの WMM 統計情報を削除します。

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

mac-address *mac-address*: クライアントの MAC アドレスを H-H-H 形式で指定します。

radio: 無線の WMM 統計情報を削除します。

説明

reset wlan wmm コマンドは WMM 統計情報を削除します。

例

すべての無線の WMM 統計情報を削除します。

<AC> reset wlan wmm radio all

関連コマンド

display wlan wmm

7.1.18 svp map-ac

Syntax

svp map-ac { **ac-vi** | **ac-vo** }

svp map-ac disable

undo svp map-ac

デフォルト

radio view は、AP group view の設定を使用します。

AP group radio view は、SVP マッピングが無効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

ac-vi: AC-VI（ビデオトラフィック）キューを指定します。

ac-vo: AC-VO（音声トラフィック）キューを指定します。

説明

svp map-ac コマンドは指定された AC キューへの SVP マッピングを有効にします。

svp map-ac disable コマンドは SVP マッピングを無効にします。

undo svp map-ac コマンドはデフォルトに戻します。

SVP マッピングは、WMM 以外のクライアントでのみ有効です。

radio view の設定は、AP group radio view の設定よりも優先されます。

例

SVP パケットを AC-VO キューにマッピングします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] svp map-ac ac-vo

AP group **apgroup1** の SVP パケットを AC-VO キューにマッピングします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] svp map-ac ac-vo

7.1.19 u-apsd enable

🕮 **メモ**:

u-apsd enable コマンドはソフトウェアバージョン 7.2.42 を含む以降のソフトウェアからサポートしています。

Syntax

u-apsd enable

undo u-apsd enable

デフォルト

有効

View

Service template view

定義済みユーザロール

network-admin

説明

u-apsd enable コマンドは U-APSD を有効にします。

undo u-apsd enable コマンドは U-APSD を無効にします。

Unscheduled automatic power-save delivery (U-APSD) は、クライアントの電力を節約するために WMM によって定義された節電方法です。

U-APSD は、WMM を有効にすると自動的に有効になります。

クライアントが U-APSD をサポートしている場合、この機能を有効にして節電機能を向上させることを推奨します。

この機能を設定するにはサービステンプレートが無効になっていることを確認してください。

例

U-APSD を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] u-apsd enable

7.1.20 wlan client-rate-limit

Syntax

wlan client-rate-limit { **dot11a** | **dot11ac** | **dot11abe** | **dot11ax** | **dot11an** | **dot11b** | **dot11be** | **dot11eax** | **dot11g** | **dot11gac** | **dot11gax** | **dot11gbe** | **dot11gn** } { **inbound** | **outbound** } **cir** *cir* [**cbs** *cbs*]

undo wlan client-rate-limit [{ **dot11a** | **dot11ac** | **dot11abe** | **dot11ax** | **dot11an** | **dot11b** | **dot11be** | **dot11eax** | **dot11g** | **dot11gac** | **dot11gax** | **dot11gbe** | **dot11gn** } [**inbound** | **outbound**]]

デフォルト

クライアントタイプベースのクライアントレート制限は設定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

dot11a: 802.11a クライアントを指定します。

dot11abe: 802.11abe クライアントを指定します。

dot11ac: 802.11ac クライアントを指定します。

dot11ax: 802.11ax クライアントを指定します。

dot11an: 802.11an クライアントを指定します。

dot11b: 802.11b クライアントを指定します。

dot11be: 802.11be クライアントを指定します。

dot11eax: 802.11eax クライアントを指定します。

dot11g: 802.11g クライアントを指定します。

dot11gac: 802.11gac クライアントを指定します。

dot11gax: 802.11gax クライアントを指定します。

dot11gbe: 802.11gax クライアントを指定します。

dot11gn: 802.11gn クライアントを指定します。

inbound: 受信トラフィックのレートを制限します。

outbound: 送信トラフィックのレートを制限します。

cir *cir*: 各クライアントの CIR を Kbps 単位で指定します。*cir* 引き数の値は 1～2097152 の範囲です。

cbs *cbs*: 各クライアントの CBS をバイト単位で指定します。*cbs* 引数の値は 1～268435456 の範囲です。このオプションを指定しない場合、CBS の値は CIR の値から自動的に計算されます。

説明

wlan client-rate-limit コマンドはクライアントタイプベースのクライアントレート制限を設定します。

undo wlan client-rate-limit コマンドは設定を削除します。

クライアントレート制限のために、異なるレート制限方式とレート制限モードを設定することができ、すべての設定が有効になります。これらの設定間のうちレート制限の最小値が各クライアントに適用されます。

例

802.11an クライアントの受信トラフィックのレート制限を 20480 Kbps に設定します。

<AC> system-view

[AC] wlan client-rate-limit dot11an inbound cir 20480

7.1.21 wlan max-bandwidth

Syntax

wlan max-bandwidth { **dot11a** | **dot11abe** | **dot11ac** | **dot11ax** | **dot11an** | **dot11b** | **dot11be** | **dot11eax** | **dot11g** | **dot11gac** | **dot11gax** | **dot11gbe** | **dot11gn** } *bandwidth*

undo wlan max-bandwidth [**dot11a** | **dot11abe** | **dot11ac** | **dot11ax** | **dot11an** | **dot11b** | **dot11be** | **dot11eax** |**dot11g** | **dot11gac** | **dot11gax** | **dot11gbe** |**dot11gn**]

デフォルト

次の最大帯域幅設定が適用されます。

- dot11a と dot11g に対して 30000 Kbps
- dot11an、dot11gn、dot11gac、dot11gax に対して 250000 Kbps
- dot11gbe では 300000 Kbps
- dot11ac と dot11ax では 500000 Kbps
- dot11eax では 700000 Kbps
- dot11abe では 800000 Kbps
- dot11be では 1500000 Kbps
- dot11b では 7000 Kbps

View

System view

定義済みユーザロール

network-admin

パラメータ

dot11a: 802.11a 無線モードを指定します。

dot11abe: 802.11abe 無線モードを指定します。

dot11ac: 802.11ac 無線モードを指定します。

dot11ax: 802.11ax 無線モードを指定します。

dot11an: 802.11an 無線モードを指定します。

dot11b: 802.11b 無線モードを指定します。

dot11be: 802.11be 無線モードを指定します。

dot11eax: 802.11eax 無線モードを指定します。

dot11g: 802.11g 無線モードを指定します。

dot11gac: 802.11gac 無線モードを指定します。

dot11gax: 802.11gax 無線モードを指定します。

dot11gbe: 802.11gax 無線モードを指定します。

dot11gn: 802.11gn 無線モードを指定します。

bandwidth: 最大帯域幅を Kbps 単位で指定します。値の範囲は、無線の種類によって次のように変化します。

- dot11a と dot11g は 16～30000 です。
- dot11an、dot11gn、dot11gac、dot11gax は 16～250000 です。
- dot11gbe では 16～300000 です。
- dot11ac と dot11ax は 16～500000 です。
- dot11eax では 16～700000 です。
- dot11abe では 16～800000 です。
- dot11be では 16～1500000 です。
- dot11b は 16～7000 です。

🕮 **メモ：**

dot11abe、**dot11be**、**dot11eax**、**dot11gbe** パラメータはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

説明

wlan max-bandwidth コマンドは無線タイプごとの最大帯域幅を設定します。

undo wlan max-bandwidth コマンドは指定した無線タイプのデフォルト設定またはすべての無線タイプのデフォルト設定に戻します。

最大帯域幅は、保証された帯域幅を計算するために使用されます。

例

802.11ac の最大帯域幅を 2000 Kbps に設定します。

<AC> system-view

[AC] wlan max-bandwidth dot11ac 2000

7.1.22 wmm

Syntax

wmm { **disable** | **enable** }

undo wmm

デフォルト

radio view は、AP group view で設定を使用します。

AP group radio view は、WMM が有効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: WMM を無効にします。

enable: WMM を有効にします。

説明

wmm enable コマンドは WMM を有効にします。

wmm disable コマンドは WMM を無効します。

undo wmm コマンドはデフォルトに戻します。

radio view の設定は、AP group radio view の設定よりも優先されます。

すべての 802.11n クライアントは WLAN QoS をサポートしている必要があります。802.11n クライアントが関連する AP と通信するために、無線が 802.11an または 802.11gn モードで動作しているときに WMM を有効にしてください。

例

WMM を無効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] wmm disable

AP group **apgroup1** の WMM を無効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] wmm disable

目次

このセクションのページは **2-x-x** です。

8 章 WLAN ローミングの設定 8-1
8.1 WLAN ローミングの設定コマンド 8-1
8.1.1 authentication-mode 8-1
8.1.2 display wlan mobility 8-2
8.1.3 display wlan mobility group 8-3
8.1.4 display wlan mobility roam-track mac-address 8-5
8.1.5 group enable 8-6
8.1.6 member 8-7
8.1.7 snmp-agent trap enable wlan mobility 8-8
8.1.8 source 8-9
8.1.9 tunnel-type 8-10
8.1.10 wlan mobility group 8-11
8.1.11 wlan mobility-group-isolation enable 8-12
8.2 WLAN 802.11r コマンド 8-13
8.2.1 ft enable 8-13
8.2.2 ft method 8-14
8.2.3 ft mobility-domain-id 8-15
8.2.4 ft reassociation-timeout 8-16
8.3 WLAN 802.11v コマンド 8-17
8.3.1 bss transition-management disassociation 8-17
8.3.2 bss transition-management enable 8-18
8.3.3 sacp anti-sticky 8-20
8.3.4 sacp anti-sticky forced-logoff 8-22
8.3.5 sacp anti-sticky interval 8-23
8.3.6 sacp anti-sticky rssi 8-24

8章 WLAN ローミングの設定

8.1 WLANローミングの設定コマンド

8.1.1 authentication-mode

メモ：

この章のコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

authentication-mode *authentication-mode* **[cipher | simple]** *authentication-key*

undo authentication-mode

デフォルト

IACTP 制御メッセージの認証モードは設定されていません。AC は IACTP 制御メッセージの完全性を検証しません。

View

Mobility group view

定義済みユーザロール

network-admin

パラメータ

authentication-mode: 認証モードを指定します。128 ビット MD 5 認証モードのみサポートします。

cipher: 暗号テキストの認証キーを指定します。

simple: プレーンテキストの認証キーを指定します。

authentication-key: 認証キーの文字列を設定します。大文字と小文字を区別します。**simple** を指定した場合、プレーンテキストで 1～16 の文字列でなくてはなりません。**cipher** を設定した場合、33～53 文字の暗号テキストでなければなりません。セキュリティのため、プレーンテキストのキーを含むすべてのキーは暗号化されて保存されます。

説明

authentication-mode コマンドは IACTP 制御メッセージの認証モードを設定します。

undo authentication-mode コマンドはデフォルトに戻します。

例

#モビリティグループ aaa の 認証モードを MD5 に設定し、認証キー12345 をプレーンテキストで設定します。

<AC> system-view

[AC] wlan mobility group aaa

[AC] authentication-mode md5 simple 12345

8.1.2 display wlan mobility

メモ：

この章のコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan mobility { roam-in | roam-out } [member ip *ipv4-address* **]**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

roam-in: 別の AC からローミングしたクライアントに関する情報を表示します。

roam-out: 別の AC にローミングしたクライアントに関する情報を表示します。

member ip *ipv4-address*: メンバ AP の IPv4 アドレスを指定します。

説明

display wlan mobility コマンドは AC 間でローミングしたクライアントに関する情報を表示します。

例

AC にローミングしたすべてのクライアントに関する情報を表示します。

<AC> display wlan mobility roam-in

```
Total entries: 1
MAC address    BSSID          VLAN ID  HA IP address
```

```
5250-0012-0411  cbab-abab-abab  1       192.168.0.101
```

指定されたメンバ AC にローミングしたクライアントに関する情報を表示します。
<AC> display wlan mobility roam-in member ip 192.168.0.101

```
Total entries: 1
MAC address     BSSID          VLAN ID
5250-0012-0411  cbab-abab-abab  1
```

#別の AC にローミングしたすべてのクライアントに関する情報を表示します。

<AC> display wlan mobility roam-out

```
Total entries: 1
MAC address     BSSID          VLAN ID  Online time      FA IP address
5250-0012-0411  cbab-abab-abab  1       00hr 01min 39sec  192.168.0.102
```

#指定されたメンバ AC から別の AC にローミングしたクライアントに関する情報を表示します。

[AC] display wlan mobility roam-out member ip 192.168.0.102

```
Total entries: 1
MAC address     BSSID          VLAN ID  Online time
5250-0012-0411  cbab-abab-abab  1       00hr 03min 02sec
```

表 8-1 コマンド出力

フィールド	説明
MAC address	クライアントのMACアドレス
BSSID	クライアントが関連付けられているAPのBSSID
VLAN ID	クライアントのVLAN ID
Online time	クライアントのオンライン時間
HA IP address	クライアントのローミング元APのIPアドレス
FA IP address	クライアントのローミング先APのIPアドレス

8.1.3 display wlan mobility group

メモ：

この章のコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan mobility group

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan mobility group コマンドはモビリティグループ情報を表示します。

例

#モビリティグループ情報を表示します。

<AC> display wlan mobility group

```
Mobility group name: office
 Tunnel type: IPv4
 Source IPv4: 172.16.220.101
 Source IPv6: Not configured
 Authentication method: Not configured
 Mobility group status: Enabled
 Member entries: 2
 IP address                          State         Online time
 172.16.220.102                       Down          00hr 00min 00sec
 172.16.220.105                       Up            00hr 36min 27sec
```

表 8-2 コマンド出力

フィールド	説明
Tunnel type	モビリティグループのIACTPトンネルタイプです。 • IPv4 • IPv6
Source IPv4	IACTPトンネルの確立に使用する送信元IPv4アドレスです。
Source IPv6	IACTPトンネルの確立に使用する送信元IPv6アドレスです。
Authentication method	モビリティグループに使用される認証方式です。
Mobility group status	モビリティグループのステータスです。 • enable • disable
IP address	メンバAPのIPアドレスです。
State	IACTPトンネルのステータスです。 • UP • DOWN
Online time	メンバAPのオンライン時間です。

8.1.4 display wlan mobility roam-track mac-address

メモ：

この章のコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan mobility roam-track mac-address *mac-address*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address *mac-address*: クライアントの MAC アドレスを指定します。

説明

display wlan mobility roam-track mac-address コマンドはホーム AC 上のクライアントのローミング情報を表示します。最新のローミングトラック情報が最初に表示されます。

例

#ホーム AC 上の指定されたクライアントのローミング情報を表示します。

<AC> display wlan mobility roam-track mac-address 5250-0012-0411

```
Total entries: 2
BSSID         Created at          Online time      AP IP address  RID  AP name
3ce5-a68d-2280  2017-03-14 11:12:28  00hr 48min 46sec  192.168.0.2    2    ap1
3ce5-a608-1150  2017-03-14 11:12:05  00hr 40min 46sec  127.0.0.1      2    ap2
```

表 8-3 コマンド出力

フィールド	説明
BSSID	クライアントが関連付けられているAPのBSSIDです。
Created at	クライアントのローミングトラックエントリが作成された日時。
Online time	クライアントのオンライン時間。

フィールド	説明
AC IP address	クライアントが関連付けられているACのIPアドレスです。
RID	クライアントが関連付けられている無線のIDです。
AP name	クライアントが関連付けられているAPの名前です。

8.1.5 group enable

メモ：

この章のコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

group enable

undo group enable

デフォルト

無効

View

Mobility group view

定義済みユーザロール

network-admin

説明

group enable コマンドはモビリティグループを有効にします。

undo group enable コマンドはモビリティグループを無効にします。

例

#モビリティグループ floor 1 を有効にします。

<AC> system-view

[AC] wlan mobility group floor1

[AC-wlan-mg-floor1] tunnel-type ipv4

[AC-wlan-mg-floor1] source ip 192.168.0.1

[AC-wlan-mg-floor1] member ip 192.168.0.2

[AC-wlan-mg-floor1] group enable

関連コマンド

member

source

tunnel-type

wlan mobility group

8.1.6 member

メモ：

この章のコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

member ip *ip-address*

undo member [**ip** *ip-address*]

デフォルト

メンバ AC の設定なし

View

Mobility group view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: メンバ AC の IPv4 アドレスを指定します。

説明

member コマンドはモビリティグループメンバを追加します。

undo member コマンドはモビリティグループメンバを削除します。

モビリティグループが無効の場合のみ、メンバの追加・削除が可能です。

モビリティグループのメンバは、IACTP トンネルの確立に使用される IP アドレスによって識別されます。

AC は 1 つのモビリティグループだけに属することが出来ます。

モビリティグループには、最大 31 のモビリティグループメンバを追加できます。

undo member コマンドの使用時に、IP アドレスを省略した場合、モビリティグループ内のすべてのメンバを削除します。

例

#モビリティグループ floor 1 にメンバ 192.168.1.55 を追加します。

<AC> system-view

[AC] wlan mobility group floor1

[AC-wlan-mg-floor1] member ip 192.168.1.55

8.1.7 snmp-agent trap enable wlan mobility

Syntax

snmp-agent trap enable wlan mobility

undo snmp-agent trap enable wlan mobility

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan mobility コマンドは WLAN ローミングの SNMP 通知を有効にします。

undo snmp-agent trap enable wlan mobility コマンドは WLAN ローミングの SNMP 通知を無効にします。

重要な WLAN ローミングイベントを NMS に送信するには、WLAN ローミングの SNMP 通知を有効にします。 WLAN ローミングイベント通知を正しく送信するには、オペレーションマニュアルのセクション 11 *システム管理 “SNMP”* の説明に従って SNMP も設定する必要があります。

例

WLAN ローミングの SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan mobility

8.1.8 source

メモ：

この章のコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

source ip *ip-address*

undo source

デフォルト

送信元 IPv4 アドレスの設定なし

View

Mobility group view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: 送信元 IPv4 アドレスを指定します。

説明

source コマンドは IACTP トンネルを確立するための送信元 IPv4 アドレスを設定します。

undo source コマンドは IACTP トンネルを確立するための送信元 IPv4 アドレスを削除します。

モビリティグループが無効の場合のみ、送信元 IPv4 アドレスの設定・削除が可能です。

1 つの送信元 IPv4 アドレスだけ設定することができます。

例

#IACTP トンネルを確立するための送信元 IPv 4 アドレス 192.168.1.55 を設定します。

<AC> system-view

[AC] wlan mobility group floor1

[AC-wlan-mg-floor1] source ip 192.168.1.55

関連コマンド

group enable

member

8.1.9 tunnel-type

メモ：

この章のコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

tunnel-type ipv4

undo tunnel-type

デフォルト

IPv4

View

Mobility group view

定義済みユーザロール

network-admin

説明

tunnel-type コマンドは IACTP トンネルの IP アドレスタイプを設定します。

undo tunnel-type コマンドはデフォルトに戻します。

例

#モビリティグループ floor1 の IACTP トンネルの IP アドレスタイプとして IPv4 を設定します。

<AC> system-view

[AC] wlan mobility group floor1

[AC-wlan-mg-floor1] tunnel-type ipv4

8.1.10 wlan mobility group

メモ：

この章のコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

wlan mobility group *group-name*

undo wlan mobility group *group-name*

デフォルト

設定なし

View

Mobility group view

定義済みユーザロール

network-admin

パラメータ

group-name: モビリティグループ名を指定します。モビリティグループ名は、1～15 文字の文字列です。大文字と小文字を区別します。

説明

wlan mobility group コマンドはモビリティグループを作成します。

undo wlan mobility group コマンドはモビリティグループを削除します。

メンバ AC に設定するモビリティグループは、同じ名前である必要があります。

1 つの AC に作成できるモビリティグループは 1 つだけです。

例

#モビリティグループ **office** を作成し、その view に移行します。

<AC>system-view

[AC] wlan mobility group office

[AC-wlan-mg-office]

8.1.11 wlan mobility-group-isolation enable

メモ：

この章のコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

wlan mobility-group-isolation enable

undo wlan mobility-group-isolation enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

wlan mobility-group-isolation enable コマンドは、モビリティグループのトンネル分離を有効にします。

undo wlan mobility-group-isolation enable コマンドは、モビリティグループのトンネル分離を無効にします。

このコマンドは、モビリティグループ内の AP 間にループが存在する場合に必要です。このコマンドにより、AP はモビリティグループ内のトンネル間でパケットを転送できなくなり、ブロードキャストストームが回避されます。

例

#モビリティグループのトンネル分離をイネーブルにします。

<AC>system-view

[AC] wlan mobility-group-isolation enable

8.2 WLAN 802.11rコマンド

🕮 **メモ：**

この章のコマンドはソフトウェアバージョン 7.2.18 を含む以降のソフトウェアからサポートしています。

8.2.1 ft enable

🕮 **メモ：**

- W1200 シリーズの AP は、ソフトウェアバージョン 7.2.93a を含む以降のソフトウェアから WPA3 パーソナル、WPA3 エンタープライズ 192bit セキュリティなしモードでの 802.11r の利用をサポートしています。ソフトウェアバージョン 7.2.89 を含む以前のソフトウェアでは、WPA3 パーソナル、WPA3 エンタープライズ 192bit セキュリティなしモードでは 802.11r は使用できません。
- W1000 シリーズと W1100 シリーズの AP は、WPA3 パーソナル、WPA3 エンタープライズ 192bit セキュリティなしモードでは 802.11r は使用できません。
- WPA3 エンタープライズ 192bit セキュリティモード、エンハンスドオープンシステム認証では 802.11r は使用できません。

Syntax

ft enable

undo ft enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

ft enable コマンドは FT（Fast BSS Transition）を有効にします。

undo ft enable コマンドは FT を無効にします。

FT により、クライアントが BSS から同一 ESS の別の BSS にローミングする際の遅延が短縮されます。802.11r FT を使用すると、クライアントはローミング先の AP とメッセージを交換する必要があります。FT は 2 つのメッセージ交換方法を提供します。

FT を有効にする場合、サービステンプレートが無効であることを確認してください。

FT を有効にするサービステンプレートは、security-ie rsn、client association-location ac を使用し、WPA3 と enhanced-open が無効である必要があります。

例

FT を有効にします。

<AC> system-view

[AC] wlan service-template st

[AC-wlan-st-st] ft enable

8.2.2 ft method

Syntax

ft method { **over-the-air** | **over-the-ds** }

undo ft method

デフォルト

over-the-air

View

Service template view

定義済みユーザロール

network-admin

パラメータ

over-the-air: Over-the-air FT を指定します。この方法では、クライアントは事前ローミング認証のためにローミング先の AP と直接通信できます。

over-the-DS: Over-the-DS FT を指定します。この方法では、クライアントは事前ローミング認証のために現在接続している AP を経由してローミング先の AP と通信します。

説明

ft method コマンドは FT 方法を設定します。

undo ft method コマンドはデフォルトに戻します。

FT 方法を設定する場合、サービステンプレートが無効であることを確認してください。

このコマンドは FT が有効の場合にのみ適用されます。

例

FT 方法を Over-the-DS に設定します。

<AC> system-view

[AC] wlan service-template st

[AC-wlan-st-st] ft method over-the-ds

関連コマンド

ft enable

8.2.3 ft mobility-domain-id

メモ：

このコマンドはソフトウェアバージョン 7.2.56 を含む以降のソフトウェアからサポートしています。

Syntax

ft mobility-domain-id *mobility-domain-id*

undo ft mobility-domain-id

デフォルト

設定無し

View

Service template view

定義済みユーザロール

network-admin

パラメータ

mobility-domain-id : モビリティドメイン ID を 1 から 65535 の範囲で指定します。

説明

ft mobility-domain-id コマンドはモビリティドメイン ID を設定します。

undo ft mobility-domain-id コマンドはデフォルトに戻します。

クライアントが異なる AP 間を移動するときに、クライアントのアクセス時間を短縮するには、この機能を設定します。

この機能を設定すると、クライアントは、2 つの AP が同じモビリティドメイン ID を持つ場合に限り、802.11r FT(fast BSS transition) を介して異なる AP 間をローミングできます。

クライアントが、FT が有効なっていてもモビリティグループに含まれていない AP 間を移動する場合、クライアントは AP 間の FT ローミングを使用する場合があります。ただ

し、AP は同じモビリティグループに属していないため、ローミングは失敗します。次に、クライアントはアソシエーションを使用して新しい AP に切り替えます。

AP に異なるモビリティドメイン ID を設定することで、クライアントは AP 間の FT ローミングを試行せずに新しい AP に直接関連付けができるようになります。その結果、AP 間の FT ローミング処理が省略されるため、サービス切り替え時間が短縮されます。サービステンプレートを有効にする前に、この機能を設定します。この機能は、FT が有効の場合にだけ有効です。

例

AC にモビリティドメイン ID666 を設定します。

<AC> system-view

[AC] wlan service-template st

[AC-wlan-st-st] ft mobility-domain-id 666

関連コマンド

ft enable

8.2.4 ft reassociation-timeout

Syntax

ft reassociation-timeout *timeout*

undo ft reassociation-timeout

デフォルト

20 秒

View

Service template view

定義済みユーザロール

network-admin

パラメータ

timeout: 再関連付けタイムアウトタイマを 1～100 秒の範囲で指定します。

説明

ft reassociation-timeout コマンドは再関連付けタイムアウトタイマを設定します。

undo ft reassociation-timeout コマンドはデフォルトに戻します。

再関連付けタイムアウトタイマを設定する場合、サービステンプレートが無効であることを確認してください。

このコマンドは FT が有効の場合のみ適用されます。

タイムアウトタイマが終了する前にクライアントが再関連付け要求を送信しない場合、ローミングプロセスは終了されます。

例

再関連付けタイムアウトタイマを 30 秒に設定します。

<AC> system-view

[AC] wlan service-template st

[AC-wlan-st-st] ft reassociation-timeout 30

関連コマンド

ft enable

8.3 WLAN 802.11vコマンド

🕮 **メモ：**

この章のコマンドはソフトウェアバージョン 7.2.47 を含む以降のソフトウェアからサポートしています。

8.3.1 bss transition-management disassociation

Syntax

bss transition-management disassociation { **forced** | **recommended** } [**timer** *time*]

undo bss transition-management disassociation

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

パラメータ

forced: アソシエーション解除タイマの期限が切れてもクライアントが AP とのアソシエーションを解除していない場合、AP はそのクライアントを強制的にログオフします。

recommended: アソシエーション解除タイマの期限が切れてもクライアントが AP とのアソシエーションを解除していない場合、AP はクライアントを強制的にログオフしません。

time: アソシエーション解除タイマを 0～180 秒の範囲で指定します。デフォルトのタイマは 90 秒です。このタイマを 0 に設定すると、bss transition-management disassociation forced が有効の場合、AP は BTM 要求をクライアントに送信した直後に、そのクライアントを強制的にログオフします。bss transition-management disassociation recommended が有効の場合、AP はクライアントに BTM 要求を送信した後、そのクライアントからログオフしません。

説明

bss transition-management disassociation コマンドは BTM アソシエーション解除を設定します。

undo bss transition-management disassociation コマンドはデフォルトに戻します。

BTM のアソシエーション解除を有効にするには、まず BTM を有効にします。BTM アソシエーション解除を設定する場合、サービステンプレートが無効であることを確認してください。

BTM アソシエーション解除が設定されている場合、AP はクライアントから BTM query ーを受信すると BTM request をクライアントに送信し、BSS 移行のためにクライアントを案内します。

bss transition-management disassociation forced を設定すると、アソシエーション解除タイマの期限が切れてもクライアントが AP とのアソシエーションを解除していない場合に、クライアントが強制的にログオフされます。この機能は慎重に使用してください。

例

BTM のアソシエーション解除(forced)を有効にし、タイマを 60 秒に設定します

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] bss transition-management disassociation forced timer 60

関連コマンド

bss transition-management enable

sacp anti-sticky

8.3.2 bss transition-management enable

Syntax

bss transition-management enable

undo bss transition-management enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

bss transition-management enable コマンドは BTM を有効にします。

undo bss transition-management enable コマンドはデフォルトに戻します。

BTM を使用すると、接続中の AP の信号強度が低い場合や、より優れた AP が検出された場合に、クライアントは最適な AP にローミングできます。

client anti-sticky が無効の場合、AP はクライアントの信号強度がしきい値よりも低いかどうかを調べず、unsolicited BTM をトリガしません。

この作業を行う前に、サービステンプレートが無効になっていることを確認してください。

例

BTM を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] bss transition-management enable

関連コマンド

bss transition-management forced-disassociation

sacp anti-sticky

8.3.3 sacp anti-sticky

🕮 **メモ：**

- このコマンドの書式はソフトウェアバージョンにより異なります。
- ソフトウェアバージョン 7.2.82b を含む以前のソフトウェアで **rssi**、**interval**、**forced-logoff** のパラメータを設定した状態で 7.2.85a を含む以降のソフトウェアにバージョンアップした場合、パラメータに対応した”**sacp anti-sticky rssi**”、“**sacp anti-sticky interval**”、”**sacp anti-sticky forced-logoff**”のコマンドが自動設定されます。

Syntax

ソフトウェアバージョン 7.2.82b を含む以前のソフトウェア：

sacp anti-sticky { **disable** | **enable** [**rssi** *rssi-value*] [**interval** *interval*] [**forced-logoff**] }

undo sacp anti-sticky

ソフトウェアバージョン 7.2.85a を含む以降のソフトウェア：

sacp anti-sticky { **disable** | **enable** }

undo sacp anti-sticky

デフォルト

Radio view では、無線は AP group radio view の設定を使用します

AP group radio view ではクライアント anti-sticky は有効です

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

rssi *rssi-value*: RSSI しきい値を 5～100(dbm)の範囲で設定します。デフォルトのしきい値は 20dbm です。

interval *interval*: 検出間隔を 3～10(秒)の範囲で設定します。デフォルトの検出間隔は 3 秒です。

forced-logoff: 信号強度が RSSI しきい値よりも低い非 802.11v クライアントをログオフします。

説明

sacp anti-sticky enable コマンドはクライアント anti-sticky を有効にします。

sacp anti-sticky disable コマンドはクライアント anti-sticky を無効にします。

undo sacp anti-sticky コマンドはデフォルトに戻します。

この機能により、AP は指定された間隔でクライアントの信号強度を調べることができます。802.11v クライアントの場合、クライアントの信号強度が RSSI しきい値より低いと、関連付けられた AP が BSS 移行をトリガして、クライアントをより適切な BSS に導きます。802.11v 以外のクライアントの場合、アクションは実行されません。

例

AP1 の radio1 でクライアント anti-sticky を有効にし、RSSI しきい値を 30 に設定し、検出間隔を 5 秒に設定し、非 802.11v クライアントの強制ログオフを有効にします

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1] sacp anti-sticky enable rssi 30 interval 5 forced-logoff

AP グループ 1 のモデル QX-W1120 の radio2 でクライアント anti-sticky を有効にし、RSSI しきい値を 30 に設定し、検出間隔を 5 秒に設定し、非 802.11v クライアントの強制ログオフを有効にします

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1120

[AC-wlan-ap-group-1-model-QX-W1120] radio 2

[AC-wlan-ap-group-1-model-QX-W1120-radio-2] sacp anti-sticky enable rssi 30 interval 5 forced-logoff

関連コマンド

bss transition-management disassociation

bss transition-management enable

sacp anti-sticky forced-logoff

sacp anti-sticky interval

sacp anti-sticky rssi

8.3.4 sacp anti-sticky forced-logoff

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.85a を含む以降のソフトウェアからサポートされています。

Syntax

sacp anti-sticky forced-logoff { **disable** | **enable** }

undo sacp anti-sticky forced-logoff

デフォルト

Radio view では、無線は AP group radio view の設定を使用します

AP group radio view では非 802.11v クライアントの強制ログオフは無効です

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

sacp anti-sticky forced-logoff enable コマンドはクライアント anti-sticky の RSSI しきい値を下回る非 802.11v クライアントの強制ログオフを有効にします。

sacp anti-sticky forced-logoff disable コマンドはクライアント anti-sticky の RSSI しきい値を下回る非 802.11v クライアントの強制ログオフを無効にします。

undo sacp anti-sticky forced-logoff コマンドはデフォルトに戻します。

例

AP1 の radio1 でクライアント anti-sticky の非 802.11v クライアントの強制ログオフを有効にします

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1] sacp anti-sticky forced-logoff enable

AP グループ 1 のモデル QX-W1120 の radio2 でクライアント anti-sticky の非 802.11v クライアントの強制ログオフを有効にします

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1120

[AC-wlan-ap-group-1-model-QX-W1120] radio 2

[AC-wlan-ap-group-1-model-QX-W1120-radio-2] sacp anti-sticky forced-logoff enable

関連コマンド

sacp anti-sticky

8.3.5 sacp anti-sticky interval

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.85a を含む以降のソフトウェアからサポートされています。

Syntax

sacp anti-sticky interval *interval*

undo sacp anti-sticky interval

デフォルト

Radio view では、無線は AP group radio view の設定を使用します

AP group radio view ではデフォルトの検出間隔は 3 秒です

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

interval: 検出間隔を 3～10(秒)の範囲で設定します。

説明

sacp anti-sticky interval コマンドはクライアント anti-sticky の検出間隔を設定します。

undo sacp anti-sticky interval コマンドはデフォルトに戻します。

例

AP1 の radio1 でクライアント anti-sticky の検出間隔を 5 秒に設定します

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1] sacp anti-sticky interval 5

AP グループ 1 のモデル QX-W1120 の radio2 でクライアント anti-sticky の検出間隔を 5 秒に設定します

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1120

[AC-wlan-ap-group-1-model-QX-W1120] radio 2

[AC-wlan-ap-group-1-model-QX-W1120-radio-2] sacp anti-sticky interval 5

関連コマンド

sacp anti-sticky

8.3.6 sacp anti-sticky rssi

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.85a を含む以降のソフトウェアからサポートされています。

Syntax

sacp anti-sticky rssi *rssi-value*

undo sacp anti-sticky rssi

デフォルト

Radio view では、無線は AP group radio view の設定を使用します

AP group radio view では RSSI しきい値のデフォルトは 20(dBm)です

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

rssi-value: RSSI しきい値を 5～100(dbm)の範囲で設定します。

説明

sacp anti-sticky rssi コマンドはクライアント anti-sticky の RSSI しきい値を設定します。

undo sacp anti-sticky rssi コマンドはデフォルトに戻します。

例

AP1 の radio1 でクライアント anti-sticky の RSSI しきい値を 30 に設定します

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1] sacp anti-sticky rssi 30

AP グループ 1 のモデル QX-W1120 の radio2 でクライアント anti-sticky の RSSI しきい値を 30 に設定します

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1120

[AC-wlan-ap-group-1-model-QX-W1120] radio 2

[AC-wlan-ap-group-1-model-QX-W1120-radio-2] sacp anti-sticky rssi 30

関連コマンド

sacp anti-sticky

目次

このセクションのページは**2-x-x** です。

9 章 WLAN ロードバランスの設定.....9-1
9.1 WLAN ロードバランスの設定コマンド 9-1
9.1.1 ap radio 9-1
9.1.2 description 9-2
9.1.3 display wlan load-balance group 9-3
9.1.4 display wlan load-balance status service-template 9-4
9.1.5 snmp-agent trap enable wlan load-balance 9-6
9.1.6 wlan load-balance access-denial 9-6
9.1.7 wlan load-balance enable 9-7
9.1.8 wlan load-balance group 9-8
9.1.9 wlan load-balance mode bandwidth 9-9
9.1.10 wlan load-balance mode session 9-10
9.1.11 wlan load-balance mode traffic 9-10
9.1.12 wlan load-balance rssi-threshold 9-11

9章 WLAN ロードバランスの設定

9.1 WLANロードバランスの設定コマンド

9.1.1 ap radio

Syntax

ap name *ap-name* **radio** *radio-id*

undo ap { **name** *ap-name* [**radio** *radio-id*] | **all** }

デフォルト

なし

View

Load balancing group view

定義済みユーザロール

network-admin

パラメータ

ap-name: AP 名を指定します。AP がすでに存在していなければなりません。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

radio-id: 名前で無線を指定します。この引数の範囲は AP のモデルにより異なります。

all: すべての無線を指定します。

説明

ap radio コマンドはロードバランスグループに無線を追加します。

undo ap コマンドはロードバランスグループから 1 つもしくはすべての無線を取り除きます。

1 つのロードバランスグループにのみ無線を追加できます。

undo ap コマンド内で無線を指定しない場合、このコマンドは指定された AP のすべての無線をロードバランスグループから取り除きます。

例

AP 1 の無線 2 をロードバランスグループ 10 に追加します。

<AC> system-view

[AC] wlan load-balance group 10

[AC-wlan-lb-group-10] ap name ap1 radio 2

9.1.2 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

Load balancing group view

定義済みユーザロール

network-admin

パラメータ

text: ロードバランスグループに対する記述を指定します。1~63 の文字列です。大文字、小文字を区別します。

説明

description コマンドはロードバランスグループに対して記述を設定します。

undo description コマンドはロードバランスグループに対する記述を削除します。

例

ロードバランスグループ 10 に対する記述を marketing に追加します。

<AC> system-view

[AC] wlan load-balance group 10

[AC-wlan-lb-group10] description marketing

9.1.3 display wlan load-balance group

Syntax

display wlan load-balance group { *group-id* | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-id: ロードバランスグループ ID を指定します。範囲は 1～65535 です。

all: すべてのロードバランスグループを指定します。

説明

display wlan load-balance group コマンドはロードバランスグループ情報を表示します。

例

ロードバランスグループ 1 の情報を表示します。

<AC> display wlan load-balance group 1

```
                    WLAN load balance group information
-------------------------------------------------------------------------------
Group ID            : 1
Description         :
Group members       : ap3-radio2,
                      ap2-radio1,
                      ap1-radio1,
-------------------------------------------------------------------------------
```

すべてのロードバランスグループの情報を表示します。

<AC> display wlan load-balance group all

```
               WLAN load balance group information
-------------------------------------------------------------------------------
Group ID             : 1
Description          :
Group members         : ap3-radio2,
                      ap2-radio1,
                      ap1-radio1,
-------------------------------------------------------------------------------
```

```
Group ID              : 2
Description           : marketing
Group members         : ap3-radio1,
------------------------------------------------------------------------------
```

表 9-1 コマンド出力

フィールド	説明
グループメンバ	ロードバランスグループ内の無線のリスト

9.1.4 display wlan load-balance status service-template

Syntax

display wlan load-balance status service-template *template-name* { **client** *mac-address* | **group** *group-id* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

template-name: サービステンプレート名を指定します。1～63 文字の文字列です。大文字と小文字を区別しません。

group-id: ロードバランシンググループ内の無線に関する情報を表示します。group-id 引数には、ロードバランシンググループの ID を指定します。範囲は 1～65535 です。

mac-address: クライアントを検出した無線に関する情報を表示します。mac-address 引数には、クライアントの MAC アドレスを H-H-H 形式で指定します。

説明

display wlan load-balance status service-template コマンドはサービステンプレートにバインドされている無線のロードバランシング情報を表示します。

例

サービステンプレート **st1** にバインドされ、ロードバランシンググループ 1 にある無線のロードバランシング情報を表示します。

<AC> display wlan load-balance status service-template st1 group 1

```
Current load balancing mode (threshold/gap): session (2/1)
```

```
Total radios: 4

APID/RID  Group ID  Session  Bandwidth(Mbps)  Traffic(%)  Balance(Y/N)
------------------------------------------------------------------------------
1/1       1         2        100              5           Y
1/2       1         10       50               10          N
2/1       1         2        10               1           Y
2/2       1         2        0                0           Y
```

サービステンプレート **st1** にバインドされ、MAC アドレスが **702d-2249-33bf** のクライアントを検出する無線のロードバランシング情報を表示します。

<AC> display wlan load-balance status service-template st1 client 702d-2249-33bf

```
Current load balancing mode (threshold/gap): session (2/1)
Load balancing group exist: Yes
Total radios: 4

APID/RID  Group ID  Session  Bandwidth(Mbps)  Traffic(%)  Balance(Y/N)
------------------------------------------------------------------------------
3/1       0         2        100              5           Y
1/2       1         10       50               10          N
4/1       1         2        10               1           Y
4/2       0         2        0                0           Y
```

表 9-2 コマンド出力

フィールド	説明
Load-balance group exist	負荷分散グループの有無: **Yes**または**No**.
Group ID	ロードバランシンググループID。0は、無線がロードバランシンググループにないことを示します。
Session	無線に関連付けられたクライアントの数
Bandwidth(Mbps)	無線の帯域幅（Mbps）
Traffic(%)	無線でサポートされている最大帯域幅に対する、無線でのトラフィックの割合
Balance(Y/N)	ロードバランシングの状態: • **Y**—無線がロードバランシングされています。 • **N**—無線がロードバランシングされていません。

9.1.5 snmp-agent trap enable wlan load-balance

Syntax

snmp-agent trap enable wlan load-balance

undo snmp-agent trap enable wlan load-balance

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan load-balance コマンドは WLAN ロードバランスに対する SNMP 通知を有効にします。

undo snmp-agent trap enable wlan load-balance コマンドはデフォルトに戻します。

重要な WLAN ロードバランスイベントを NMS に報告するために、SNMP 通知を有効にします。WLAN ロードバランスイベント通知を正確に送信するために、オペレーションマニュアルのセクション 11 *システム管理 "SNMP"* に記載されるように SNMP も設定しなければなりません。

例

WLAN ロードバランスに対して SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan load-balance

9.1.6 wlan load-balance access-denial

Syntax

wlan load-balance access-denial *access-denial*

undo wlan load-balance access-denial

デフォルト

10

View

System view

定義済みユーザロール

network-admin

パラメータ

access-denial: 紐付け要求の拒否の最大数を指定します。範囲は 2~10 です。

説明

wlan load-balance access-denial コマンドは紐付け要求に対する拒否の最大数を設定します。

undo wlan load-balance access-denial コマンドはデフォルトに戻します。

AP が拒絶する回数が最大数に達した場合、AP はクライアントからの紐付け要求を許可します。

例

紐付け要求の拒否の最大数を 4 に設定します。

<AC> system-view

[AC] wlan load-balance access-denial 4

9.1.7 wlan load-balance enable

Syntax

wlan load-balance enable

undo wlan load-balance enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

wlan load-balance enable コマンドは WLAN ロードバランスを有効にします。

undo wlan load-balance enable コマンドは WLAN ロードバランスを有効にします。

例

WLAN ロードバランスを有効にします。

<AC> system-view

[AC] wlan load-balance enable

9.1.8 wlan load-balance group

Syntax

wlan load-balance group *group-id*

undo wlan load-balance group { *group-id* | **all** }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id: ロードバランスグループ ID を指定します。範囲は 1～65535 です。

all: すべてのロードバランスグループを指定します。

説明

wlan load-balance group コマンドはロードバランスグループを作成し、その view に移行します。

undo wlan load-balance group コマンドは 1 つもしくはすべてのロードバランスグループを取り除きます。

特定の AP 間でロードバランスを実行するために、AP の無線をロードバランスグループに追加することができます。AC はロードバランスグループに属さない無線ではロードバランスを実行しません。

例

ロードバランスグループ 10 を作成し、その view に移行します。

<AC> system-view

[AC] wlan load-balance group 10

[AC-wlan-lb-group-10]

関連コマンド

ap radio

9.1.9 wlan load-balance mode bandwidth

Syntax

wlan load-balance mode bandwidth *value* [**gap** *gap-value*]

undo wlan load-balance mode

デフォルト

セッションモードロードバランス

View

System view

定義済みユーザロール

network-admin

パラメータ

value: 帯域幅しきい値を指定します。範囲は 1~500Mbps です。

gap-value: 帯域幅ギャップしきい値を指定します。範囲は 1~200Mbps です。

帯域幅ギャップしきい値のデフォルトは 20Mbps です。

説明

wlan load-balance mode bandwidth コマンドは帯域幅モードロードバランスを設定します。

undo wlan load-balance mode コマンドはデフォルトに戻します。

以下の条件が満たされたとき、AC は帯域幅モードロードバランスを実行します。

- AP の帯域幅が帯域幅しきい値に達する場合。
- 最小の帯域幅を有する AP 間の帯域幅ギャップが、帯域幅ギャップしきい値に達する場合。

例

帯域幅モードにロードバランスモードを設定し、帯域幅しきい値と帯域幅ギャップしきい値をそれぞれ 100Mbps と 20Mbps に設定します。

<AC> system-view

[AC] wlan load-balance mode bandwidth 100 gap 20

9.1.10 wlan load-balance mode session

Syntax

wlan load-balance mode session *value* [**gap** *gap-value*]

undo wlan load-balance mode

デフォルト

セッションモードロードバランスを使用します。セッションしきい値は 20 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

value: セッションしきい値を指定します。範囲は 1～120 の範囲です。

gap-value: セッションギャップしきい値を指定します。範囲は 1~12 です。セッションギャップしきい値のデフォルトは 4 です。

説明

wlan load-balance mode session コマンドはセッションモードロードバランスを設定します。

undo wlan load-balance mode コマンドはデフォルトに戻します。

以下の条件が満たされたとき、AC はセッションモードロードバランスを実行します。

- AP に紐付いたクライアント数がセッションしきい値に達する場合。
- 最小のクライアントを有する AP 間のセッションギャップが、セッションギャップしきい値に達する場合。

例

セッションモードにロードバランスモードを設定し、セッションしきい値とセッションギャップしきい値をそれぞれ 7 と 5 に設定します。

<AC> system-view

[AC] wlan load-balance mode session 7 gap 5

9.1.11 wlan load-balance mode traffic

Syntax

wlan load-balance mode traffic *value* [**gap** *gap-value*]

undo wlan load-balance mode

デフォルト

セッションモードのロードバランシングが使用されます。

View

System view

定義済みユーザロール

network-admin

パラメータ

value: トラフィックのしきい値を、トラフィックと AP の最大帯域幅の比率で指定します。範囲は 1～80%です。

gap-value: トラフィックギャップと AP の最大帯域幅の比率でトラフィックギャップのしきい値を指定します。この引数の値の範囲は 10～40%です。デフォルトのトラフィックギャップのしきい値は 20%です。

説明

wlan load-balance mode traffic コマンドはトラフィックモードロードバランスを設定します。

undo wlan load-balance mode コマンドはデフォルトに戻します。

次の条件が満たされると、AC はトラフィックモードのロードバランシングを実行します。

1) AP のトラフィックがトラフィックのしきい値に達する。
2) トラフィックが最も少ない AP と AP の間のトラフィックギャップがトラフィックギャップのしきい値に達する。

例

ロードバランシングモードをトラフィックモードに設定し、トラフィックしきい値とトラフィックギャップしきい値をそれぞれ 25%と 20%に設定します。

<AC> system-view

[AC] wlan load-balance mode traffic 25 gap 20

9.1.12 wlan load-balance rssi-threshold

Syntax

wlan load-balance rssi-threshold *rssi-threshold*

undo wlan load-balance rssi-threshold

デフォルト

25

View

System view

定義済みユーザロール

network-admin

パラメータ

rssi-threshold: RSSI しきい値を指定します。範囲は 5~100 です。

説明

wlan load-balance rssi-threshold コマンドは RSSI（Received Signal Strength Indicator）しきい値を設定します。

undo wlan load-balance rssi-threshold コマンドはデフォルトに戻します。

クライアントは複数の AP に検出される可能性があります。クライアントの RSSI がロードバランス RSSI しきい値より低い場合、AP はそのクライアントを検出しません。クライアントを検出できる AP が 1 つだけの場合、オーバーロードであっても AP はクライアントに対するアクセス確率を向上させます。

例

RSSI しきい値を 40 に設定します。

<AC> system-view

[AC] wlan load-balance rssi-threshold 40

目次

このセクションのページは **2-x-x** です。

10 章 WLAN 無線リソースの計測の設定 10-1
10.1 WLAN 無線リソースの計測の設定コマンド 10-1
10.1.1 display wlan measure-report 10-1
10.1.2 measure 10-4
10.1.3 measure-duration 10-6
10.1.4 measure-interval 10-7
10.1.5 resource-measure 10-8
10.1.6 rm-capability mode 10-9

10章 WLAN 無線リソースの計測の設定

10.1 WLAN無線リソースの計測の設定コマンド

10.1.1 display wlan measure-report

Syntax

display wlan measure-report ap *ap-name* **radio** *radio-id* [**client mac-address** *mac-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

radio *radio-id*: 番号を使用して無線を指定します。設定範囲はデバイスモデルにより異なります。

client mac-address *mac-address*: クライアントを MAC アドレスで指定します。 このオプションを指定しない場合、すべてのクライアントの計測結果を表示します。

説明

display wlan measure-report コマンドはクライアントの測定結果を表示します。

例

AP ap1 の無線 2 に接続したクライアントの計測結果を表示します。

<AC> display wlan measure-report ap ap1 radio 2

```
Total number of clients: 1

Client MAC address                          : 0aef-e760-3587
```

```
Link measurement:
  Link margin                          : 2 dBm
  RCPI                                 : -85 dBm
  RSNI                                 : 53 dBm
Noise histogram:
  Antenna ID                           : 3
  ANPI                                 : -56 dBm
  IPI0 to IPI10 density                : 5 12 16 13 8 5 5 15 17 1 3
Spectrum measurement:
  Transmit power                       : 20 dBm
  BSS                                  : Detected
  OFDM preamble                        : Detected
  Radar                                : Detected
  Unidentified signal                  : Undetected
  CCA busy fraction                    : 60
  RPI0 to RPI7 density                 : 3 7 11 19 15 23 15 7
Frame report entry:
  BSSID                                : a072-2351-e253
  PHY type                             : fhss
  Average RCPI                         : -10 dBm
  Last RSNI                            : 2 dBm
  Last RCPI                            : -20 dBm
  Frames                               : 1
Dot11BSSAverageAccessDelay group:
  Average access delay                 : 32 ms
  BestEffort average access delay      : 1 ms
  Background average access delay      : 1 ms
  Video average access delay           : 1 ms
  Voice average access delay           : 1 ms
  Clients                              : 32
  Channel utilization rate             : 11
Transmit stream:
  Traffic ID                           : 0
  Sent MSDUs                           : 60
  Discarded MSDUs                      : 5
  Failed MSDUs                         : 3
  MSDUs resent multiple times          : 3
  Lost QoS CF-Polls                    : 2
  Average queue delay                  : 2 ms
  Average transmit delay               : 1 ms
  Bin0 range                           : 0 to 10 ms
  Bin0 to Bin5                         : 5 10 10 5 10 10
```

表 10-1 コマンド出力

Field	Description
Link margin	受信したRSSIと最低の利用可能なRSSIとの間のギャップ。
RCPI	受信チャネル電力インジケータ。
RSNI	受信信号対雑音インジケータ。
ANPI	測定中の平均雑音電力インジケータ。
IPI0 to IPI10 density	測定期間全体に対する異なるIPI範囲の時間の割合。 IPInはIPI範囲を表します。 nの値は1～10の範囲です。 • **0**: IPI <= –92 dBm. • **1**: –92 dBm < IPI <= –89 dBm. • **2**: –89 dBm < IPI <= –86 dBm. • **3**: –86 dBm < IPI <= –83 dBm. • **4**: –83 dBm < IPI <= –80 dBm. • **5**: –80 dBm < IPI <= –75 dBm • **6**: –75 dBm < IPI <= –70 dBm. • **7**: –70 dBm < IPI <= –65 dBm. • **8**: –65 dBm < IPI <= –60 dBm. • **9**: –60 dBm < IPI <= –55 dBm. • **10**: –55 dBm < IPI.
Transmit power	クライアントの送信電力。
BSS	クライアントが他のBSSからの無線パケットを検出したかどうか。
OFDM preamble	クライアントがOFDMプリアンブルを検出したかどうか。
Radar	クライアントがレーダー信号を検出したかどうか。
Unidentified signal	クライアントが未知の信号を検出したかどうか。
CCA busy fraction	全測定期間に対するチャネルのビジー時間の割合。
RPI0 to RPI7 density	測定期間全体に対するRPIの範囲が異なる時間の割合。 RPInはRPI範囲を表します。nの値は1～7の範囲です。 • **0**: RPI <= –87 dBm. • **1**: –87 dBm < RPI <= –82 dBm. • **2**: –82 dBm < RPI <= –77 dBm. • **3**: –77 dBm < RPI <= –72 dBm. • **4**: –72 dBm < RPI <= –67 dBm.

Field	Description
	● **5**: –67 dBm < RPI <= –62 dBm. ● **6**: –62 dBm < RPI <= –57 dBm. ● **7**: –57 dBm < RPI.
PHY type	物理メディアの種類 ● fhss. ● dsss. ● irbaseband. ● ofdm. ● hrdsss. ● erp.
Frames	測定中の同じMACアドレスとBSSIDからのフレーム数。
Bin0 range	Bin0の値の範囲。
Bin0 to Bin5	平均遅延範囲ごとに正常に送信されたMSDUの数。 Binxは平均遅延範囲を表します。xの値は0～5の範囲です。 ● **Bin0**: Delay< 10 ms. ● **Bin1**: 10 ms <= Delay < 20 ms. ● **Bin2**: 20 ms <= Delay < 40 ms. ● **Bin3**: 40 ms <= Delay < 80 ms. ● **Bin4**: 80 ms <= Delay < 160 ms. ● **Bin5**: 160 ms <= Delay.

10.1.2 measure

🕮 **メモ：**

spectrum、**tpc** パラメータはソフトウェアバージョン 7.2.55 を含む以降のソフトウェアからサポートしています。

Syntax

measure { **all** | **link** | **neighbor** | **radio** | **spectrum** | **tpc** } { **disable** | **enable** }

undo measure

デフォルト

radio view：AP group radio view の設定を使用します。

AP group radio view：無効

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

all: すべての測定機能を指定します。

link: リンク測定を指定します。リンク測定は、要求されたリンクの RCPI、RSNI、リンク冗長性を測定します。

neighbor: 隣接測定を指定します。近隣測定は、隣接 AP のチャネルおよび BSSID を測定します。

radio: 無線測定を指定します。無線測定は、チャネル負荷、雑音ヒストグラム、ビーコン、フレーム、station 統計、位置、送信ストリームを測定します。

spectrum: スペクトル測定を指定します。スペクトル測定は、基本測定、CCA 測定（Clear Channel Assessment）、RPI 測定（Receive Power Indication）を実施します。

tpc: TPC 測定を指定します。TPC 測定は、リンク冗長性とクライアントへの送信電力を測定します。

disable: 指定された測定機能またはすべての測定機能を無効にします。

enable: 指定された測定機能またはすべての測定機能を有効にします。

説明

measure enable コマンドは指定された測定機能またはすべての測定機能を有効にします。

measure disable コマンドは指定された測定機能またはすべての測定機能を無効にします。

undo measure コマンドはデフォルトに戻します。

link、**neighbor**、**radio** を有効にする場合は、**resource-measure** コマンドを有効にする必要があります。

spectrum、**tpc** を有効にする場合は、**spectrum-management** コマンドを有効にする必要があります。**spectrum-management** コマンドの詳細は、コマンドマニュアルのセクション 2 WLAN の”*WLAN RRM*”を参照してください。

spectrum、**tpc** は 5GHz のラジオでのみ使用できます。

例

AP ap1 の spectrum 測定を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] measure spectrum enable

AP group apgroup1 の spectrum 測定を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] measure spectrum enable

関連コマンド

- **measure-duration**
- **measure-interval**
- **resource-measure**
- **spectrum-management**

10.1.3 measure-duration

Syntax

measure-duration *time*

undo measure-duration

デフォルト

radio view：AP group radio view の設定を使用します。

AP group radio view：500 TU

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

time: 測定期間を指定します。設定範囲は 1～10000TU です。1TU=1024 マイクロ秒です。

説明

measure-duration コマンドは測定期間を設定します。

undo measure-duration コマンドはデフォルトに戻します。

AP で測定が有効になると、AP からクライアントへの測定要求により測定期間を通知します。

例

AP ap1 の測定期間を 512TU に指定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] measure-duration 512

AP group apgroup1 の測定期間を 512TU に指定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] measure-duration 512

関連コマンド

- **measure**
- **measure-interval**

10.1.4 measure-interval

Syntax

measure-interval *value*

undo measure-interval

デフォルト

radio view：AP group radio view の設定を使用します。

AP group radio view：30 秒

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

value: 測定間隔を指定します。設定範囲は 1～60 秒です。

説明

measure-interval コマンドは AP が測定要求をクライアントに送信するための測定間隔を設定します。

undo measure-interval コマンドはデフォルトに戻します。

例

AP ap1 の測定間隔を 35 秒に指定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] measure-interval 35

AP group apgroup1 の測定間隔を 35 秒に指定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] measure-interval 35

関連コマンド

- **measure**
- **measure-duration**

10.1.5 resource-measure

Syntax

resource-measure { **disable** | **enable** }

undo resource-measure

デフォルト

radio view：AP group radio view の設定を使用します。

AP group radio view：無効

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 無線リソース測定を無効にします。

enable: 無線リソース測定を有効にします。

説明

resource-measure enable コマンドは無線リソース測定を有効にします。

resource-measure disable コマンドは無線リソース測定を無効にします。

undo resource-measure コマンドはデフォルトに戻します。

AP で無線測定を有効にすると、AP はビーコン、プローブ応答、アソシエーション応答、再アソシエーション応答の Radio Measurement フィールドを 1 に設定し、計測要求を送信できることをクライアントに通知します。また、このフレームで、AP がサポートする計測タイプをクライアントに通知します。

AP は定期的に Measurement Pilot フレームを送信して、クライアントが AP を高速に検出できるようにします。Measurement Pilot フレームは、ビーコンよりも頻繁に送信され、より少ない情報しか運びません。

例

AP ap1 の無線資源計測を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] resource-measure enable

AP group apgroup1 の無線資源計測を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] resource-measure enable

10.1.6 rm-capability mode

Syntax

rm-capability mode { **all** | **none** | **partial** }

undo rm-capability mode

デフォルト

radio view：AP group radio view の設定を使用します。

AP group radio view：設定なし

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

all: all モードを指定します。クライアントは、すべての無線資源計測機能が AP の無線資源計測機能と一致する場合にのみ、AP に接続することができます。

none: none モードを指定します。AP はクライアントの無線資源計測機能をチェックしません。

partial: 部分モードを指定します。クライアントは、少なくとも 1 つの無線資源計測機能が AP の無線資源計測機能と一致する場合、AP に接続することができます。

説明

rm-capability mode コマンドはクライアント無線資源計測機能の一致モードを設定します。

undo rm-capability mode コマンドはデフォルトに戻します。

この設定は、無線資源計測が有効な場合にのみ有効です。

例

AP ap1 のクライアント無線資源計測機能を部分モードに指定します

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] resource-measure enable

[AC-wlan-ap-ap1-radio-2] rm-capability mode partial

AP group apgroup1.のクライアント無線資源計測機能を部分モードに指定します

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] rm-capability mode partial

関連コマンド

resource-measure

目次

このセクションのページは **2-x-x** です。

11 章 チャネルスキャンの設定 11-1
11.1 チャネルスキャンの設定コマンド 11-1
11.1.1 scan channel blacklist 11-1
11.1.2 scan channel whitelist 11-2
11.1.3 scan idle-time 11-3
11.1.4 scan max-service-time 11-4
11.1.5 scan scan-time 11-6

11章 チャネルスキャンの設定

11.1 チャネルスキャンの設定コマンド

11.1.1 scan channel blacklist

Syntax

scan channel blacklist *channel-list*

undo scan channel blacklist { *channel-list* | **all** }

デフォルト

Radio view では、無線は AP group radio view の設定を使用します

AP group radio view では、チャネルスキャンブラックリストは存在しません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

channel-list: チャネル番号を指定します。設定範囲は 1～165 です。

all: チャネルスキャンブラックリストのすべてのチャネルを指定します。

説明

scan channel blacklist コマンドはチャネルスキャンブラックリストを設定します。

undo scan channel blacklist コマンドは指定したチャネルをチャネルスキャンブラックリストから削除します。

AP のチャネルスキャンブラックリストを設定すると、AP はブラックリストのチャネルをスキャンしません。同じ AP のチャネルスキャンブラックリストとホワイトリストの両方を設定することはできません。チャネルスキャンブラックリストを設定する前に、チャネルスキャンホワイトリストのすべてのチャネルを削除してください。

Radio view の設定は、AP group radio view の設定よりも優先されます。

例

AP1 のチャネルスキャンブラックリストにチャネル 1 と 6 を追加します。

<AC> system-view

[AC] wlan ap 1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] scan channel blacklist 1 6

AP グループ 10 のモデル **QX-W1020** の AP のチャネルスキャンブラックリストにチャネル 1 と 6 を追加します。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] ap-model QX-W1020

[AC-wlan-ap-group-10-ap-model-QX-W1020] radio 2

[AC-wlan-ap-group-10-ap-model-QX-W1020-radio-2] scan channel blacklist 1 6

11.1.2 scan channel whitelist

Syntax

scan channel whitelist *channel-list*

undo scan channel whitelist { *channel-list* | **all** }

デフォルト

Radio view では、無線は AP group radio view の設定を使用します

AP group radio view では、チャネルスキャンホワイトリストは存在しません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

channel-list: チャネル番号を指定します。設定範囲は 1～165 です。

all: チャネルスキャンホワイトリストのすべてのチャネルを指定します。

説明

scan channel whitelist コマンドは、チャネルスキャンホワイトリストを設定します。

undo scan channel whitelist コマンドは指定したチャネルをチャネルスキャンホワイトリストから削除します。

AP のチャネルスキャンホワイトリストを設定すると、AP はホワイトリスト内のチャネルだけをスキャンします。同じ AP のチャネルスキャンブラックリストとホワイトリスト

の両方を設定することはできません。チャネルスキャンホワイトリストを設定する前に、チャネルスキャンブラックリストのすべてのチャネルを削除してください。

Radio view の設定は、AP group radio view の設定よりも優先されます。

例

AP1 のチャネルスキャンホワイトリストにチャネル 1 と 6 を追加します。

<AC> system-view

[AC] wlan ap 1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] scan channel whitelist 1 6

AP グループ 10 のモデル **QX-W1020** の AP のチャネルスキャンホワイトリストにチャネル 1 と 6 を追加します。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] ap-model QX-W1020

[AC-wlan-ap-group-10-ap-model-QX-W1020] radio 2

[AC-wlan-ap-group-10-ap-model-QX-W1020-radio-2] scan channel whitelist 1 6

11.1.3 scan idle-time

Syntax

scan idle-time *idle-time*

undo scan idle-time

デフォルト

Radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、サービスアイドルタイムアウトは 100 ミリ秒です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

idle-time: サービスアイドルタイムアウトを指定します。設定範囲は 60～5000 ミリ秒です。最大サービス期間より長く設定することはできません。

説明

scan idle-time コマンドはサービスアイドルタイムアウトを設定します。

undo scan idle-time コマンドはデフォルトに戻します。

AP は、サービス期間中、指定したサービスアイドルタイムアウトが切れても、現在のサービス期間がスキャン期間を超えるまで、新しいスキャン期間を開始しません。

サービスアイドルタイムアウトは、ビーコン間隔の倍数でなければなりません。ビーコン間隔より小さいサービスアイドルタイムアウトを設定すると、ビーコン間隔値をサービスアイドルタイムアウトとして使用します。

Radio view の設定は、AP group radio view の設定よりも優先されます。

例

AP 1 のサービスアイドルタイムアウトを 500 ミリ秒に指定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] scan idle-time 500

AP グループ 10 のモデル **QX-W1020** の AP のサービスアイドルタイムアウトタイマーを 500 ミリ秒に設定します。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] ap-model QX-W1020

[AC-wlan-ap-group-10-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-10-ap-model-QX-W1020-radio-1] scan idle-time 500

関連コマンド

beacon interval

11.1.4 scan max-service-time

Syntax

scan max-service-time { *max-service-time* | **no-limit** }

undo scan max-service-time

デフォルト

Radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、最大サービス期間はソフトウェアバージョンにより異なります。

ソフトウェアバージョン 7.2.18 を含む以前のソフトウェアでは 5000 ミリ秒です。

ソフトウェアバージョン 7.2.21 を含む以降のソフトウェアでは no-limit です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

max-service-time: 最大サービス期間を指定します。設定範囲は 100～5000 ミリ秒です。AP の最大サービス期間に達すると、AP は転送するトラフィックがあるかどうかにかかわらず、スキャン期間を開始します。

no-limit: 無線がサービス期間を制限しないように設定します。無線サービスの品質を確保するには、このキーワードを指定します。サービスアイドルタイムアウトが切れるまで、AP はスキャン期間を開始しません。

Radio view の設定は、AP group radio view の設定よりも優先されます。

説明

scan max-service-time コマンドは最大サービス期間を設定します。

undo scan max-service-time コマンドはデフォルトに戻します。

例

AP 1 の最大サービス期間を 3000 ミリ秒に指定します。

<AC> system-view

[AC] wlan ap ap1 model WA4320i-ACN

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] scan max-service-time 3000

AP グループ 10 のモデル **QX-W1020** の AP の最大サービス期間を 3000 ミリ秒に設定します。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] ap-model QX-W1020

[AC-wlan-ap-group-10-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-10-ap-model-QX-W1020-radio-1] scan max-service-time 3000

11.1.5 scan scan-time

Syntax

scan scan-time *scan-time*

undo scan scan-time

デフォルト

Radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、スキャン時間は 100 ミリ秒です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

scan-time: スキャン時間を指定します。設定範囲は 100～5000 ミリ秒です。スキャン期間は最大サービス期間より長くすることはできません。

説明

scan scan-time コマンドはスキャン時間を設定します。

undo scan scan-time コマンドはデフォルトに戻します。

Radio view の設定は、AP group radio view の設定よりも優先されます。

例

AP 1 のスキャン期間を 500 ミリ秒に指定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] scan scan-time 500

AP グループ 10 のモデル QX-W1020 の AP のスキャン時間を 500 ミリ秒に設定します。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] ap-model QX-W1020

[AC-wlan-ap-group-10-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-10-ap-model-QX-W1020-radio-1] scan scan-time 500

目次

このセクションのページは **2-x-x** です。

12 章 バンドナビゲーションの設定.....12-1
12.1 バンドナビゲーションの設定コマンド.....12-1
12.1.1 band-navigation.....12-1
12.1.2 wlan band-navigation aging-time.....12-2
12.1.3 wlan band-navigation balance access-denial.....12-3
12.1.4 wlan band-navigation balance session.....12-4
12.1.5 wlan band-navigation enable.....12-5
12.1.6 wlan band-navigation rssi-threshold.....12-5

12章 バンドナビゲーションの設定

12.1 バンドナビゲーションの設定コマンド

12.1.1 band-navigation

Syntax

band-navigation { **disable** | **enable** }

undo band-navigation

デフォルト

AP view：AP group view の設定を使用します。

AP group view：有効

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: AP または AP グループのバンドナビゲーションを無効にします。

enable: AP または AP グループのバンドナビゲーションを有効にします。

説明

band-navigation enable コマンドは AP または AP グループのバンドナビゲーションを有効にします。

band-navigation disable コマンドは AP または AP グループのバンドナビゲーションを無効にします。

undo band-navigation コマンドはデフォルトに戻します。

バンドナビゲーションは、グローバル、AP いずれの場合も、本コマンドを有効後、動作します。

例

AP ap1 のバンドナビゲーションを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] band-navigation enable

AP group 1 のバンドナビゲーションを有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] band-navigation enable

[AC-wlan-ap-ap1-radio-1] scan idle-time 500

関連コマンド

wlan band-navigation enable

12.1.2 wlan band-navigation aging-time

Syntax

wlan band-navigation aging-time *aging-time*

undo wlan band-navigation aging-time

デフォルト

180 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

aging-time: クライアント情報のエージングタイマを指定します。設定範囲は 10～600 秒です。

説明

wlan band-navigation aging-time コマンドはクライアント情報のエージングタイマを設定します。

undo wlan band-navigation aging-time コマンドはデフォルトに戻します。

AP がクライアントからアソシエーション要求を受信すると、AP はクライアントの情報を記録し、クライアント情報エージングタイマを開始します。エージングタイマが満了する前に AP がプローブ要求またはアソシエーション要求をクライアントから受信しない場合、AP はクライアントの情報を削除します。

適切なクライアント情報のエージングタイマを設定して、クライアントの関連付けとシステムリソースの効率性を確保します。

例

クライアント情報のエージングタイマを 50 秒に指定します。

<AC> system-view

[AC] wlan band-navigation aging-time 50

12.1.3 wlan band-navigation balance access-denial

Syntax

wlan band-navigation balance access-denial *access-denial*

undo wlan band-navigation balance access-denial

デフォルト

AP は 5GHz または 2.4GHz アソシエーション要求を拒否しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

access-denial: 5GHz または 2.4GHz アソシエーション要求の最大拒否回数を指定します。設定範囲は 1～10 回です。

説明

wlan band-navigation balance access-denial コマンドは 5GHz または 2.4GHz アソシエーション要求の最大拒否回数を設定します。

undo wlan band-navigation balance access-denial コマンドはデフォルトに戻します。

クライアントの 5GHz または 2.4GHz アソシエーション要求の拒否回数が指定した最大拒否回数になると、AP はクライアントのアソシエーション要求を受け入れます。

このコマンドは、5GHz と 2.4GHz の両方の接続で有効です。

band-navigation は、最初は 5GHz での接続を優先するので、2.4GHz アソシエーション要求を拒否する回数となります。

その後、GAP 数などの設定により、2.4GHz での接続を優先する状態になると、5GHz アソシエーション要求を拒否する回数となります。

例

5GHz または 2.4GHz アソシエーション要求の最大拒否回数を 5 回に指定します。

<AC> system-view

[AC] wlan band-navigation balance access-denial 5

12.1.4 wlan band-navigation balance session

Syntax

wlan band-navigation balance session *session* [**gap** *gap*]

undo wlan band-navigation balance session

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

session: 5GHz の無線クライアント数のしきい値を指定します。設定範囲は 2～120 です。

gap: 5GHz と最も少ない無線のクライアント数の差のしきい値を指定します。設定範囲は 1～8 で、デフォルト値は 4 です。

説明

wlan band-navigation balance session コマンドはバンドナビゲーションのロードバランスを設定します。

undo wlan band-navigation balance session コマンドはデフォルトに戻します。

AC は、バンドナビゲーションを有効にしてもロードバランスを有効にしない場合、デュアルバンドクライアントを 5GHz 無線に誘導します。

AP は、次の条件が満たされた場合にクライアントの 5GHz アソシエーション要求を拒否します。

- 5GHz 無線のクライアント数が、指定したしきい値に達した場合。
- 5GHz 無線のクライアント数と最も少ない無線クライアント数との差が、指定したしきい値に達した場合。

例

バンドナビゲーションの負荷分散を有効にし、クライアント数のしきい値である、session、gap をそれぞれ 10 と 5 に設定します。

<AC> system-view

[AC] wlan band-navigation balance session 10 gap 5

12.1.5 wlan band-navigation enable

Syntax

wlan band-navigation enable

undo wlan band-navigation enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

wlan band-navigation enable コマンドはバンドナビゲーションをグローバルで有効にします。

undo wlan band-navigation enable コマンドはデフォルトに戻します。

バンドナビゲーションが動作するには、ワイヤレスサービステンプレートの高速アソシエーションが無効になっている必要があります。

バンドナビゲーションは、グローバル、AP 両方でこのコマンドが有効の場合のみ動作します。

例

グローバルバンドナビゲーションを有効にします。

<AC> system-view

[AC] wlan band-navigation enable

関連コマンド

- **band-navigation**
- **quick-association enable**

12.1.6 wlan band-navigation rssi-threshold

Syntax

wlan band-navigation rssi-threshold *rssi-threshold*

undo wlan band-navigation rssi-threshold

デフォルト

15

View

System view

定義済みユーザロール

network-admin

パラメータ

rssi-threshold: バンドナビゲーションの RSSI しきい値を指定します。設定範囲は 5～100 です。

説明

wlan band-navigation rssi-threshold コマンドはバンドナビゲーションの RSS（Received Signal Strength Indicator）しきい値を設定します。

undo wlan band-navigation rssi-threshold コマンドはデフォルトに戻します。

複数の無線でクライアントを検出する可能性があります。5GHz 無線は、クライアントの RSSI がバンドナビゲーション RSSI しきい値よりも低い場合、クライアントのアソシエーション要求を拒否します。

例

バンドナビゲーションの RSSI しきい値を 40 に指定します。

<AC> system-view

[AC] wlan band-navigation rssi-threshold 40

目次

このセクションのページは **2-x-x** です。

13 章 WLAN の高可用性の設定 13-1
13.1 デュアルリンクバックアップコマンド 13-1
13.1.1 backup-ac 13-1
13.1.2 priority 13-2
13.1.3 wlan tunnel-preempt 13-3
13.2 AP ライセンス同期コマンド 13-4
13.2.1 ap-license-synchronization enable 13-4
13.2.2 display wlan ap-license-group 13-5
13.2.3 local ip 13-6
13.2.4 member ip 13-7
13.2.5 wlan ap-license-group 13-8
13.3 WLAN アップリンク検出コマンド 13-8
13.3.1 wlan uplink track 13-8

13章 WLAN の高可用性の設定

13.1 デュアルリンクバックアップコマンド

13.1.1 backup-ac

Syntax

backup-ac ip *ipv4-address*

undo backup-ac ip

デフォルト

AP view では、AP は AP group view の設定を使用します。

AP group view では、バックアップ AC は指定されていません。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

ip *ipv4-address*: IPv4 アドレスでバックアップ AC を指定します。

説明

backup ac コマンドはバックアップ AC を指定します。

undo backup ac コマンドはデフォルトに戻します。

AP view または AP group view のどちらかで、1 つの IPv4 アドレスを指定することができます。

AP view の設定は、AP group view の設定に優先します。AP view で undo コマンドを実行した場合、AP group view で指定されたバックアップ AC が使用されます。

undo コマンドを実行すると、バックアップ CAPWAP トンネルも終了します。

例

AP ap1 でバックアップ AC を指定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] backup-ac ip 192.168.1.1

AP グループ group1 でバックアップ AC を指定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] backup-ac ip 192.168.1.1

13.1.2 priority

Syntax

priority *priority*

undo priority

デフォルト

AP view は、AP group view の設定を使用します。

AP group view は、AC の AP 接続優先度は 4 です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

priority: AC の AP 接続優先度を 0～7 の範囲で指定します。値が大きいほど接続優先度が高くなります。

説明

priority コマンドは AC の AP 接続優先度を設定します。

undo priority コマンドはデフォルトに戻します。

AP は、より高い接続優先度を有する AC と CAPWAP トンネルを優先して確立します。

AP 接続優先度は、AC ディスカバリ中にのみ有効です。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap3** の AP 接続優先度を 7 に設定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1020

[AC-wlan-ap-ap3] priority 7

AP group **group1** の、AP 接続優先度を 7 に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] priority 7

13.1.3 wlan tunnel-preempt

Syntax

wlan tunnel-preempt { **disable** | **enable** }

undo wlan tunnel-preempt

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、AP は Global configuration view で設定を使用します。

Global configuration view では、マスタ CAPWAP トンネルプリエンプションは無効です。

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

disable: マスタ CAPWAP トンネルプリエンプションを無効にします。

enable: マスタ CAPWAP トンネルプリエンプションを有効にします。

説明

wlan tunnel-preempt enable コマンドはマスタ CAPWAP トンネルプリエンプションを有効にします。

wlan tunnel-preempt disable コマンドはマスタ CAPWAP トンネルプリエンプションを無効にします。

undo wlan tunnel-preempt コマンドはデフォルトに戻します。

wlan tunnel-preempt コマンドは、デュアルリンクバックアップを利用している環境において、優先度の高い AP との CAPWAP トンネルが切断されバックアップ AP との CAPWAP トンネルがマスタに切り替わった後、再度優先度の高い AP との CAPWAP トンネルが復旧した場合の動作を設定します。

この機能が有効な場合、高優先の AP との CAPWAP トンネルが復旧した際、10 分後にマスタに接続が切り戻ります。

この機能が無効な場合、高優先の AP との CAPWAP トンネルが復旧しても、マスタに接続は切り戻りません。

例

AP **ap1** のマスタ CAPWAP トンネルプリエンプションを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-ap-ap1] wlan tunnel-preempt enable

AP グループ **group1** の AP の CAPWAP トンネルプリエンプションを有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] wlan tunnel-preempt enable

グローバルにマスタ CAPWAP トンネルプリエンプションを有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] wlan tunnel-preempt enable

13.2 APライセンス同期コマンド

🕮 **メモ**：

この章のコマンドはソフトウェアバージョン 7.2.18 を含む以降のソフトウェアからサポートしています。

13.2.1 ap-license-synchronization enable

Syntax

ap-license-synchronization enable

undo ap-license-synchronization enable

デフォルト

無効

View

AP license synchronization group view

定義済みユーザロール

network-admin

説明

ap-license-synchronization enable コマンドは AP ライセンス同期機能を有効にします。

undo ap-license-synchronization enable コマンドは AP ライセンス同期機能を無効にします。

本機能により、AP ライセンスをマスタ AC からバックアップ AC に同期させることができます。同期するためには、AP ライセンス同期グループを作成する必要があります。

本機能を有効にする前に、AP ライセンス同期グループ内で IP アドレスを指定する必要があります。

例

AP ライセンス同期を有効にします。

<AC> system-view

[AC] wlan ap-license-group

[AC-wlan-als-group] ap-license-synchronization enable

13.2.2 display wlan ap-license-group

Syntax

display wlan ap-license-group

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan ap-license-group コマンドは AP ライセンス同期グループの情報を表示します。

例

AP ライセンス同期グループの情報を表示します。

<AC> display wlan ap-license-group

```
Group total licenses: 32
Group used licenses: 12
```

```
AP license synchronization: Enabled
Local IP: 2.2.2.2
Local role: Master
Member information:
IP address      Total    Used   Member role   State   Online duration
2.2.2.3          8        2      Master        Up     00hr 00min 04sec
```

表 13-1 コマンド出力

フィールド	補足
Group total licenses	APライセンス同期グループ内のAPライセンスの合計
Group used licenses	APライセンス同期グループ内で使用されているAPライセンス数
AP license synchronization	APライセンス同期機能の有効・無効表示
Local IP	ローカルACのIPアドレス
Local role	ローカルACの役割 ● マスタ ● 設定なし
IP address	APライセンス同期グループ内のメンバACのIPアドレス
Total	メンバACに登録されているAPライセンスの合計
Used	メンバACで使用されているAPライセンス数
Member role	メンバACの役割 ● マスタ
State	APライセンス同期グループ内のメンバACの状態 ● Up ● Down
Online duration	メンバACのオンライン時間

13.2.3 local ip

Syntax

local ip *ipv4-address*

undo local ip

デフォルト

設定なし

View

AP license synchronization group view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: AP ライセンス同期グループ内の AC の IPv4 アドレスを指定します。

説明

local ip コマンドは AP ライセンス同期グループ内の AC に対して IP アドレスを指定します。

undo local ip コマンドはデフォルトに戻します。

本コマンドを実行する前に、AP ライセンス同期機能が無効であることを確認してください。

例

AP ライセンス同期グループ内の AC の IP アドレスを指定します。

<AC> system-view

[AC] wlan ap-license-group

[AC-wlan-als-group] local ip 192.168.1.1

13.2.4 member ip

Syntax

member ip *ipv4-address*

undo member ip *ipv4-address*

デフォルト

設定なし

View

AP license synchronization group view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: メンバ AC の IPv4 アドレスを指定します。

説明

member ip コマンドは AP ライセンス同期グループにメンバ AC を追加します。

undo local ip コマンドは AP ライセンス同期グループからメンバ AC を削除します。

本コマンドを実行する前に、AP ライセンス同期機能が無効であることを確認してください。

例

AP ライセンス同期グループにメンバ AC を追加します。

<AC> system-view

[AC] wlan ap-license-group

[AC-wlan-als-group] member ip 192.168.1.2

13.2.5 wlan ap-license-group

Syntax

wlan ap-license-group

View

System view

定義済みユーザロール

network-admin

説明

wlan ap-license-group コマンドは AP license synchronization group view に移行します。

AC で作成できる AP ライセンス同期グループは 1 つのみです。

例

AP license synchronization group view に移行します。

<AC> system-view

[AC] wlan ap-license-group

[AC-wlan-als-group]

13.3 WLANアップリンク検出コマンド

13.3.1 wlan uplink track

Syntax

wlan uplink track *track-entry-number*

undo wlan uplink track

デフォルト

WLAN アップリンク検出はトラックエントリと関連付けられていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: トラックエントリ ID を指定します。範囲は 1～1024 です。

説明

wlan uplink track コマンドはWLANアップリンク検出をトラックエントリと関連付けます。

undo wlan uplink track コマンドはデフォルトに戻します。

本コマンドにより、トラックエントリに関連付けられたアップリンク状態に基づいて無線状態を AC が調節できるようになります。トラックエントリがネガティブ状態の場合、AC は接続しているすべての AP の無線を無効にします。トラックエントリがポジティブ状態の場合、AC は接続しているすべての AP の無線を有効にします。

本コマンドを複数回実行した場合、最新の設定が有効になります。

例

トラックエントリ 1 を WLAN アップリンク検出に関連付けます。

<AC> system-view

[AC] wlan uplink track 1

目次

このセクションのページは **2-x-x** です。

14 章 WLAN RRM 14-1
14.1 WLAN RRM コマンド 14-1
14.1.1 adjacency-factor 14-1
14.1.2 ap name 14-2
14.1.3 calibrate-bandwidth self-decisive 14-3
14.1.4 calibrate-channel 2.4g channel-set-optimization enable 14-5
14.1.5 calibrate-channel 2.4g channel-set-optimization neighbor-threshold 14-7
14.1.6 calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent 14-8
14.1.7 calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent-per-set 14-9
14.1.8 calibrate-channel channel-set-optimization 14-10
14.1.9 calibrate-channel channel-set-optimization neighbor-threshold 14-13
14.1.10 calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent 14-14
14.1.11 calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent-per-set 14-16
14.1.12 calibrate-channel mode 14-17
14.1.13 calibrate-channel monitoring time-range 14-19
14.1.14 calibrate-channel pronto 14-20
14.1.15 calibrate-channel self-decisive 14-21
14.1.16 calibrate-channel track radar-detect enable 14-23
14.1.17 calibrate-power 2.4g coverage rssi-threshold 14-24
14.1.18 calibrate-power 2.4g coverage weak-signal-client ratio 14-25
14.1.19 calibrate-power 2.4g coverage weak-signal-client threshold 14-27
14.1.20 calibrate-power 2.4g coverage weak-signal-packet ratio 14-28
14.1.21 calibrate-power 2.4g coverage weak-signal-packet threshold 14-29
14.1.22 calibrate-power 2.4g max 14-30
14.1.23 calibrate-power 5g coverage rssi-threshold 14-31
14.1.24 calibrate-power 5g coverage weak-signal-client ratio 14-32
14.1.25 calibrate-power 5g coverage weak-signal-client threshold 14-34
14.1.26 calibrate-power 5g coverage weak-signal-packet ratio 14-35
14.1.27 calibrate-power 5g coverage weak-signal-packet threshold 14-36
14.1.28 calibrate-power 5g max 14-37
14.1.29 calibrate-power 6g coverage rssi-threshold 14-38
14.1.30 calibrate-power 6g coverage weak-signal-client ratio 14-39

14.1.31 calibrate-power 6g coverage weak-signal-client threshold 14-41
14.1.32 calibrate-power 6g coverage weak-signal-packet ratio 14-42
14.1.33 calibrate-power 6g coverage weak-signal-packet threshold 14-43
14.1.34 calibrate-power 6g max 14-44
14.1.35 calibrate-power coverage enable 14-45
14.1.36 calibrate-power min 14-48
14.1.37 calibrate-power mode 14-49
14.1.38 calibrate-power self-decisive 14-50
14.1.39 calibrate-power threshold 14-52
14.1.40 channel holddown-time 14-53
14.1.41 channel-capability mode 14-54
14.1.42 channel-switch mode 14-55
14.1.43 crc-error-threshold 14-56
14.1.44 description 14-57
14.1.45 display wlan rrm baseline 14-58
14.1.46 display wlan rrm baseline apply-result 14-61
14.1.47 display wlan rrm-calibration-group 14-62
14.1.48 display wlan rrm-history ap 14-63
14.1.49 display wlan rrm-status ap 14-65
14.1.50 interference-threshold 14-68
14.1.51 power holddown-time 14-69
14.1.52 power-capability mode 14-70
14.1.53 power-constraint mode 14-72
14.1.54 rrm 14-73
14.1.55 scan-only 14-74
14.1.56 snmp-agent trap enable wlan rrm 14-75
14.1.57 spectrum-management 14-76
14.1.58 tolerance-level 14-77
14.1.59 wlan calibrate-channel pronto ap all 14-78
14.1.60 wlan calibrate-power pronto ap all 14-80
14.1.61 wlan rrm baseline apply 14-80
14.1.62 wlan rrm baseline remove 14-81
14.1.63 wlan rrm baseline save 14-82
14.1.64 wlan rrm calibration-bandwidth interval 14-83
14.1.65 wlan rrm calibration-channel interval 14-84
14.1.66 wlan rrm-calibration-group 14-85
14.1.67 wlan rrm calibration-power interval 14-86

14章 WLAN RRM

14.1 WLAN RRMコマンド

14.1.1 adjacency-factor

Syntax

adjacency-factor *neighbor*

undo adjacency-factor

デフォルト

RRM view：AP group view の設定を使用します。

AP group RRM view：3(ソフトウェアバージョン 7.2.21 を含む以前)

1(ソフトウェアバージョン 7.2.27 を含む以降)

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

neighbor: 1～16 の範囲内の隣接係数を指定します。

説明

adjacency-factor コマンドは隣接係数を設定します。

undo adjacency-factor コマンドはデフォルトに戻します。

隣接係数は、TPC をトリガする管理可能な検出された無線の量と、電力調整しきい値との比較に使用される RSSI の順位を定義します。AC はそれに関連付けられた無線だけを管理できます。

たとえば、隣接係数が 3 の場合、無線が 3 つの他の管理可能な無線を検出すると、AC は無線の TPC を実行します。他の管理可能な無線によって検出された無線の RSSI を降順でランク付けした後、AC は電力調整しきい値と比較する 3 番目に大きい RSSI を選択します。

例

AP **ap1** の無線 1 に対して、隣接係数を 7 に設定します。

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] adjacency-factor 7

AP グループ **group1** の **QX-W1020** モデルを持つ AP の無線 1 に対して、隣接係数を 7 に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] adjacency-factor 7

14.1.2 ap name

Syntax

ap name *ap-name* **radio** *radio-id*

undo ap { **name** *ap-name* [**radio** *radio-id*] | **all** }

デフォルト

設定なし

View

RRM holddown group view

定義済みユーザロール

network-admin

パラメータ

name *ap-name*: AP 名を指定します。指定された AP がすでに存在していなければなりません。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

radio-id: ID で無線を指定します。この引数の値は 1 もしくは 2 です。1 つの RRM holddown group に属することができる無線は 1 つだけです。新たな RRM holddown group に無線を追加すると、既存の RRM holddown group からはその無線が削除されます。

all: すべての無線を指定します。

説明

ap name コマンドは RRM holddown group に無線を追加します。

undo ap name コマンドは RRM holddown group から 1 つまたはすべての無線を取り除きます。

例

ap 1 の radio 2 を RRM holddown group 10 に追加します。

<AC> system-view

[AC] wlan rrm-calibration-group 10

[AC-wlan-rrm-calibration-group-10] ap name ap1 radio 2

14.1.3 calibrate-bandwidth self-decisive

🕮 **メモ**:

- このコマンドはソフトウェアバージョン 7.2.55 を含む以降のソフトウェアからサポートしています。
- Global configuration view では、**disable** のパラメータを使用できません。

Syntax

RRM view / AP group RRM view

calibrate-bandwidth self-decisive { **disable** | **enable** }

undo calibrate-bandwidth self-decisive

Global Configuration view

ソフトウェアバージョン 7.2.75 を含む以降のソフトウェア

calibrate-bandwidth self-decisive enable { **5g** | **6g** | **all** }

undo calibrate-bandwidth self-decisive enable { **5g** | **6g** | **all** }

ソフトウェアバージョン 7.2.73 を含む以前のソフトウェア

calibrate-bandwidth self-decisive enable

undo calibrate-bandwidth self-decisive

デフォルト

RRM view：AP group view の設定を使用します。

AP group RRM view：global configuration view の設定を使用します。

Global configuration view：無効

View

RRM view

AP group RRM view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

disable: 帯域幅自動調整機能を無効にします。

enable: 帯域幅自動調整機能を有効にします。

5g: 5GHz 無線を指定します。

6g: 6GHz 無線を指定します。

all: 5GHz 無線と 6GHz 無線両方を指定します。

🕮 **メモ：**

5g、**6g**、および **all** のパラメータはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

説明

calibrate-bandwidth self-decisive enable コマンドは帯域幅自動調整を有効にします。

calibrate-bandwidth self-decisive disable コマンドは帯域幅自動調整を無効にします。

undo calibrate-bandwidth self-decisive コマンドはデフォルトに戻します。

帯域幅自動調整が有効の場合、AC は帯域幅自動調整間隔に達するとチャネル品質検出を開始し、帯域幅調整を実行するかどうかを決定します。ネイバ無線の数が多い場合は、干渉を減らすために無線の帯域幅を減らし、数が少ない場合は、伝送レートを増やすために帯域幅を増やします。

このコマンドは、5 GHz 無線および 6GHz 無線でのみ有効です。

🕮 **メモ：**

6GHz 無線での使用はソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。なお、6GHz 無線のサポートは AP の機種により異なります。

例

ap1 と名付けた AP の無線 1 に対して帯域幅自動調整を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-bandwidth self-decisive enable

group1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して帯域幅自動調整を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-bandwidth self-decisive enable

#グローバルで帯域幅自動調整を有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-bandwidth self-decisive enable

14.1.4 calibrate-channel 2.4g channel-set-optimization enable

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-channel 2.4g channel-set-optimization enable

undo calibrate-channel 2.4g channel-set-optimization enable

デフォルト

有効

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent：管理対象外の周辺の比率のしきい値を 1～100 の範囲で設定します。

説明

calibrate-channel 2.4g channel-set-optimization enable コマンドは 2.4 GHz 無線のチャネル最適化を有効にします。

undo calibrate-channel 2.4g channel-set-optimization enable コマンドは 2.4 GHz 無線のチャネル最適化を無効にします。

異なるベンダの AP が混在した環境では、これらの AP を統一した方法で管理できず、異なるチャネルグループを使用する可能性があるため、2.4 GHz 無線に対して重大な干渉が発生する可能性があります。これは、ユーザーエクスペリエンスに大きな影響を与えます。

この機能により、AC は、サードパーティ製 AP の周辺の無線で最も使用されるチャネルグループを自動 DFS で採用できます。この操作により、異なるベンダの AP 間のチャネル間干渉を最大限に減らすことができます。

装置は、(1、6、11)、(1、7、13)、(2、7、12)、(3、8、13)、(4、9、14)のチャネルグループの検出をサポートしています。

周辺の無線には、次のタイプがあります。

- **Managed neighbor**– 同じ AC で管理されている AP 無線を検出した場合
- **Unmanaged neighbor**– 別の AC で管理されている AP 無線を検出した場合

この機能を有効にすると、次の条件がすべて満たされた場合、装置は自動 DFS 中に 2.4 GHz 無線のチャネル最適化を実行します。

- 周辺の合計数が設定されたしきい値に達するか、それを超えた場合
- 管理対象外の周辺の比率（管理対象外の周辺/周辺の合計）が設定されたしきい値に達した場合か、それを超えた場合
- 単一のチャネルグループ（管理対象外の周辺/周辺の合計）の管理対象外の周辺の比率が設定されたしきい値に達した場合か、それを超えた場合

RRM view の設定は、AP group RRM view および Global configuration view の設定より優先されます。

AP group RRM view の設定は、Global configuration view の設定より優先されます。

例

2.4 GHz 無線のチャネル最適化を無効にします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] undo calibrate-channel 2.4g channel-set-optimization enable

関連コマンド

- **calibrate-channel 2.4g channel-set-optimization neighbor-threshold**
- **calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent**
- **calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent-per-set**
- **calibrate-channel channel-set-optimization**
- **calibrate-channel channel-set-optimization neighbor-threshold**
- **calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent**
- **calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent-per-set**

14.1.5 calibrate-channel 2.4g channel-set-optimization neighbor-threshold

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-channel 2.4 g channel-set-optimization neighbor-threshold *count*

undo calibrate-channel 2.4 g channel-set-optimization neighbor-threshold

デフォルト

10

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

count: 近隣数のしきい値を 1～1000 の範囲で設定します。

説明

calibrate-channel 2.4 g channel-set-optimization neighbor-threshold コマンドは近隣数のしきい値を設定します。

undo calibrate-channel 2.4 g channel-set-optimization neighbor-threshold コマンドはデフォルトに戻します。

RRM view の設定は、AP group RRM view および Global configuration view の設定より優先されます。

AP group RRM view の設定は、Global configuration view の設定より優先されます。

例

近隣数しきい値を 11 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-channel 2.4g channel-set-optimization neighbor-threshold 11

関連コマンド

- **calibrate-channel 2.4 g channel-set-optimization enable**
- **calibrate-channel channel-set-optimization**

14.1.6 calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent *percent*

undo calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent

デフォルト

50%

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 管理対象外の周辺の比率のしきい値を 1～100 の範囲で設定します。

説明

calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent コマンドは管理対象外の近隣比率のしきい値を設定します。

undo calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent コマンドはデフォルトに戻します。

RRM view の設定は、AP group RRM view および Global configuration view の設定より優先されます。

AP group RRM view の設定は、Global configuration view の設定より優先されます。

例

管理対象外の近隣比率のしきい値を 20%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent 20

関連コマンド

- **calibrate-channel 2.4 g channel-set-optimization enable**
- **calibrate-channel channel-set-optimization**

14.1.7 calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent-per-set

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent-per-set *percent*

undo channel-set-optimization neighbor-unmanaged-threshold percent-per-set

デフォルト

10%

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 単一のチャネルグループの管理対象外の近隣比率しきい値を 1～100 の範囲で設定します。

説明

calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent-per-set コマンドは 1 つのチャネルグループの管理対象外の近隣比率しきい値を設定します。

undo calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent-per-set コマンドはデフォルトに戻します。

RRM view の設定は、AP group RRM view および Global configuration view の設定より優先されます。

AP group RRM view の設定は、Global configuration view の設定より優先されます。

例

単一のチャネルグループの管理対象外の近隣比率しきい値を 20%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent-per-set 20

14.1.8 calibrate-channel channel-set-optimization

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-channel channel-set-optimization { **disable** | **enable** }

undo calibrate-channel channel-set-optimization

デフォルト

RRM view では、AP group RRM view の設定が使用されます。

AP group RRM view では、Global configuration view の設定が使用されます。

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

説明

calibrate-channel channel-set-optimization enable コマンドは 2.4 GHz 無線のチャネル最適化を有効にします。

calibrate-channel channel-set-optimization disable コマンドは 2.4 GHz 無線のチャネル最適化を無効にします。

undo calibrate-channel channel-set-optimization コマンドはデフォルトに戻します。

異なるベンダの AP が混在した環境では、これらの AP を統一した方法で管理できず、異なるチャネルグループを使用する可能性があるため、2.4 GHz 無線に対して重大な干渉が発生する可能性があります。これは、ユーザーエクスペリエンスに大きな影響を与えます。

この機能を使用すると、AC は、auto DFS でサードパーティ製 AP の近隣無線で最も使用されるチャネルグループを採用できます。この操作により、異なるベンダの AP 間のチャネル間干渉を最大限に減らすことができます。

装置は、(1、6、11)、(1、7、13)、(2、7、12)、(3、8、13)、(4、9、14)のチャネルグループの検出をサポートしています。

周辺の無線には、次のタイプがあります。

- **Managed neighbor**– 同じ AC で管理されている AP 無線を検出した場合
- **Unmanaged neighbor**– 別の AC で管理されている AP 無線を検出した場合

この機能を有効にすると、次の条件がすべて満たされた場合、装置は自動 DFS 中に 2.4 GHz 無線のチャネル最適化を実行します。

- 周辺の合計数が設定されたしきい値に達するか、それを超えた場合
- 管理対象外の周辺の比率（管理対象外の周辺/周辺の合計）が設定されたしきい値に達した場合か、それを超えた場合
- 単一のチャネルグループ（管理対象外の周辺/周辺の合計）の管理対象外の周辺の比率が設定されたしきい値に達した場合か、それを超えた場合

このコマンドは、2.4 GHz 無線でのみ有効です。

RRM view の設定は、AP group RRM view および Global configuration view の設定より優先されます。

AP group RRM view の設定は、Global configuration view の設定より優先されます。

例

AP ap1 の 2.4 GHz 無線のチャネル最適化を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] rrm

[AC-wlan-ap-ap1-radio-2-rrm] calibrate-channel-set-optimization enable

AP グループ group 1 の QX-W1110 で 2.4 GHz 無線のチャネル最適化を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1110

[AC-wlan-ap-group-group1-ap-model-QX-W1110] radio 2

[AC-wlan-ap-group-group1-ap-model-QX-W1110-radio-2] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1110-radio-2-rrm] calibrate-channel channel-set-optimization enable

関連コマンド

- **calibrate-power 2.4g channel-set-optimization enable**
- **calibrate-channel 2.4g channel-set-optimization neighbor-threshold**
- **calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent**
- **calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent-per-set**
- **calibrate-channel channel-set-optimization neighbor-threshold**
- **calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent**
- **calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent-per-set**

14.1.9 calibrate-channel channel-set-optimization neighbor-threshold

🕮 メモ：

このコマンドはソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-channel channel-set-optimization neighbor-threshold *count*

undo calibrate-channel channel -set-optimization neighbor-threshold

デフォルト

RRM view では、AP group RRM view の設定が使用されます。

AP group RRM view では、Global configuration view の設定が使用されます。

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

count：近隣数のしきい値を 1～1000 の範囲で設定します。

説明

calibrate-channel channel-set-optimization neighbor-threshold コマンドは周辺数のしきい値を設定します。

undo calibrate-channel channel-set-optimization neighbor-threshold コマンドはデフォルトに戻します。

このコマンドは、2.4 GHz 無線でのみ有効です。

RRM view の設定は、AP group RRM view および Global configuration view の設定より優先されます。

AP group RRM view の設定は、Global configuration view の設定より優先されます。

例

AP ap1 の周辺の数のしきい値を 11 に設定します。

<AC> system-view

[AC] wlan ap ap 1 model QX-W1110

[AC-wlan-ap-ap 1] radio 2

[AC-wlan-ap-ap 1-radio-2] rrm

[AC -wlan-ap-ap 1-radio-2-rrm] calibrate-channel-set-optimization neighbor-threshold 11

#AP グループ group 1 の QX-W1110 で、周辺の数のしきい値を 11 に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1110

[AC-wlan-ap-group-group1-ap-model-QX-W1110] radio 2

[AC-wlan-ap-group-group1-ap-model-QX-W1110-radio-2] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1110-radio-2-rrm] calibrate-channel channel-set-optimization neighbor-threshold 11

関連コマンド

- **calibrate-power 2.4g channel-set-optimization enable**
- **calibrate-channel channel-set-optimization**

14.1.10 calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent *percent*

undo calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent

デフォルト

RRM view では、AP group RRM view の設定が使用されます。

AP group RRM view では、Global configuration view の設定が使用されます。

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

percent：管理対象外の周辺の比率のしきい値を 1～100 の範囲で設定します。

説明

calibrate-channel channel-set-optimization neighbor-unmanaged-threshold コマンドは管理対象外の周辺の比率のしきい値を設定します。

undo calibrate-channel channel-set-optimization neighbor-unmanaged-threshold コマンドはデフォルトに戻します。

このコマンドは、2.4 GHz 無線でのみ有効です。

RRM view の設定は、AP group RRM view および Global configuration view の設定より優先されます。

AP group RRM view の設定は、Global configuration view の設定より優先されます。

例

AP ap 1 の管理対象外の周辺の比率しきい値を 20%に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] rrm

[AC-wlan-ap-ap1-radio-2-rrm] calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent 20

AP グループ group1 の QX-W1110 で、管理対象外の周辺の比率のしきい値を 20%に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1110

[AC-wlan-ap-group-group1-ap-model-QX-W1110] radio 2

[AC-wlan-ap-group-group1-ap-model-QX-W1110-radio-2] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1110-radio-2-rrm] calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent 20

14.1.11 calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent-per-set

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-channel- set-optimization neighbor-unmanaged-threshold percent-per-set *percent*

undo calibrate-channel-set-optimization neighbor-unmanaged-threshold percent-per-set

デフォルト

RRM view では、AP group RRM view の設定が使用されます。

AP group RRM view の RRM view では、Global configuration view の設定が使用されます。

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

percent：管理対象外の周辺の比率のしきい値を 1～100 の範囲で設定します。

説明

calibrate-channel- set-optimization neighbor-unmanaged-threshold percent-per-set コマンドは単一のチャネルグループの管理対象外の近隣比率しきい値を設定します。

undo calibrate-channel- set-optimization neighbor-unmanaged-threshold percent-per-set コマンドはデフォルトに戻します。

このコマンドは、2.4 GHz 無線でのみ有効です。

RRM view の設定は、AP group RRM view および Global configuration view の設定より優先されます。

AP group RRM view の設定は、Global configuration view の設定より優先されます。

例

AP ap1 の単一のチャネルグループの管理対象外の近隣比率しきい値を 20%に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] rrm

[AC-wlan-ap-ap1-radio-2-rrm] calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent-per-set 20

#AP グループ group 1 の QX-W1110 で、単一のチャネルグループの管理対象外の近隣比率しきい値を 20%に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1110

[AC-wlan-ap-group-group1-ap-model-QX-W1110] radio 2

[AC-wlan-ap-group-group1-ap-model-QX-W1110-radio-2] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1110-radio-2-rrm] calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent 20

関連コマンド

- **calibrate-channel 2.4g channel-set-optimization enable**
- **calibrate-channel channel-set-optimization**

14.1.12 calibrate-channel mode

Syntax

calibrate-channel mode { **periodic** | **scheduled** }

undo calibrate-channel mode

デフォルト

RRM view では、AP group RRM view の構成が使用されます。

AP group RRM view では、auto-DFS モードは定期的です。

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

periodic: 定期的な auto-DFS を指定します。

scheduled: スケジュールされた auto-DFS を指定します。

説明

calibrate-channel mode コマンドは auto-DFS モードを設定します。

undo calibrate-channel mode コマンドはデフォルトに戻します。

定期的な auto-DFS モードでは、AC はチャネルキャリブレーション間隔で無線用の DFS を自動的に実行します。

スケジュールされた auto-DFS モードでは、AC は指定された時間間隔で DFS を実行します。干渉が深刻な場合は、進行中の無線サービスに影響を与えないようにこのモードを使用します。

例

auto-DFS モードを AP **ap1** の無線 1 に**スケジュール**するように設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel self-decisive enable

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel mode scheduled

auto-DFS モードを AP グループ **group1** のモデル **QX-W1020** を持つ AP の無線 1 に**スケジュール**するように設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-channel self-decisive enable

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-channel mode scheduled

関連コマンド

- **calibrate-channel monitoring time-range**

- **calibrate-channel pronto**
- **wlan rrm calibration-channel interval**

14.1.13 calibrate-channel monitoring time-range

Syntax

calibrate-channel monitoring time-range *time-range-name*

undo calibrate-channel monitoring time-range

デフォルト

RRM view では、AP group RRM view の構成が使用されます。

AP group RRM view では、チャネル監視の時間範囲が指定されていません。

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

time-range-name: 時間範囲の名前を指定します。大文字と小文字を区別しない 1～32 文字です。文字列は文字で始める必要がありますが、all には設定できません。

説明

calibrate-channel monitoring time-range コマンドはチャネル監視の時間範囲を指定します。

undo calibrate-channel monitoring time-range コマンドはチャネル監視の時間範囲を削除します。

スケジュールされた auto-DFS では、AC は指定された時間範囲の統計情報を収集し、チャネルレポートとネイバーレポートを生成します。

例

AP **ap1** の無線 1 に対するチャネル監視の時間範囲を指定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel monitoring time-range time1

AP グループ **group1** のモデル **QX-W1020** の無線 1 に対するチャネル監視の時間範囲を指定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-channel monitoring time-range time1

関連コマンド

time-range

14.1.14 calibrate-channel pronto

Syntax

calibrate-channel pronto

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

説明

calibrate-channel pronto コマンドはスケジュールされた auto-DFS を実行します。

例

ジョブを作成し、AP **ap1** の無線 1 に対するジョブにコマンドを割り当てます。

<AC> system-view

[AC] scheduler job calibration1

[AC-job-calibration1] command 1 system-view

[AC-job-calibration1] command 2 wlan ap ap1

[AC-job-calibration1] command 3 radio 1

[AC-job-calibration1] command 4 rrm

[AC-job-calibration1] command 5 calibrate-channel pronto

ジョブを作成し、AP グループ **g1** のモデル **QX-W1020** を持つ AP の無線 1 に対するジョブにコマンドを割り当てます。

<AC> system-view

[AC] scheduler job calibration2

[AC-job-calibration2] command 1 system-view

[AC-job-calibration2] command 2 wlan ap-group g1

[AC-job-calibration2] command 3 ap-model QX-W1020

[AC-job-calibration2] command 4 radio 1

[AC-job-calibration2] command 5 rrm

[AC-job-calibration2] command 6 calibrate-channel pronto

14.1.15 calibrate-channel self-decisive

Syntax

ソフトウェアバージョン 7.2.75 を含む以降のソフトウェア

RRM view/AP group RRM view

calibrate-channel self-decisive { **disable** | **enable** }

undo calibrate-channel self-decisive

Global configuration view

calibrate-channel self-decisive enable { **2.4g** | **5g** | **6g** | **all** }

undo calibrate-channel self-decisive enable { **2.4g** | **5g** | **6g** | **all** }

ソフトウェアバージョン 7.2.58 を含む以降のソフトウェア

RRM view/AP group RRM view

calibrate-channel self-decisive { **disable** | **enable** }

undo calibrate-channel self-decisive

Global configuration view

calibrate-channel self-decisive enable { **2.4g** | **5g** | **all** }

undo calibrate-channel self-decisive enable { **2.4g** | **5g** | **all** }

ソフトウェアバージョン 7.2.27 を含む以降のソフトウェア

RRM view/AP group RRM view

calibrate-channel self-decisive { **disable** | **enable** }

undo calibrate-channel self-decisive

Global configuration view

calibrate-channel self-decisive enable { **2.4g** | **5g** | **all** }

undo calibrate-channel self-decisive { **2.4g** | **5g** | **all** }

ソフトウェアバージョン 7.2.21 を含む以前のソフトウェア

calibrate-channel self-decisive { **disable** | **enable** }

undo calibrate-channel self-decisive

デフォルト

ソフトウェアバージョン 7.2.27 を含む以降のソフトウェア

RRM view：AP group view の設定を使用します。

AP group RRM view：Global configuration view の設定を使用します。

Global configuration view：無効

ソフトウェアバージョン 7.2.21 を含む以前のソフトウェア

RRM view：AP group view の設定を使用します。

AP group RRM view：無効

View

RRM view

AP group RRM view

Global configuration view(ソフトウェアバージョン 7.2.27 以降のバージョンでサポート)

定義済みユーザロール

network-admin

パラメータ

disable: auto-DFS を無効にします。

enable: auto-DFS を有効にします。

2.4g: 2.4GHz 無線を指定します。

5g: 5GHz 無線を指定します。

6g: 6GHz 無線を指定します。

all: ソフトウェアバージョン 7.2.21 を含む以前のソフトウェアでは、このパラメータを指定できません。ソフトウェアバージョン 7.2.27 を含む以降のソフトウェアでは、2.4GHz 無線と 5GHz 無線を指定します。ソフトウェアバージョン 7.2.75 を含む以降のソフトウェアでは、2.4GHz 無線と 5GHz 無線と 6GHz 無線を指定します。

説明

calibrate-channel self-decisive enable コマンドは auto-DFS を有効にします。

calibrate-channel self-decisive disable コマンドは auto-DFS を無効にします。

undo calibrate-channel self-decisive コマンドはデフォルトに戻します。

例

ap1 と名付けた AP の無線 1 に対して auto-DFS を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel self-decisive enable

group1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して auto-DFS を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-channel self-decisive enable

関連コマンド

calibrate-channel mode

14.1.16 calibrate-channel track radar-detect enable

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.85a を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-channel track radar-detect enable

undo calibrate-channel track radar-detect enable

デフォルト

無効

View

Global configuration view

定義済みユーザロール

network-admin

説明

calibrate-channel track radar-detect enable コマンドはレーダ検出トリガの RRM を有効にします。

undo calibrate-channel track radar-detect enable コマンドはデフォルトに戻します。

AP が現在のチャネルでレーダ信号を検出すると、チャネルを変更するか、レーダ干渉を防ぐために通信を抑制します。しかし、チャネルにより干渉などにより無線ネットワークの品質が悪化させる可能性があります。

この機能を有効にすると、AP がレーダ信号を検出しチャネルを変更した後、RRM に通知し、新しいチャネルを評価します。必要に応じて、RRM は自動的にチャネルを調整し、無線ネットワークの品質を向上させます。

例

レーダ検出トリガの RRM を有効化します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-channel track radar-detect enable

14.1.17 calibrate-power 2.4g coverage rssi-threshold

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 2.4g coverage rssi-threshold *rssi*

undo calibrate-power 2.4g coverage rssi-threshold

デフォルト

20

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

rssi: RSSI しきい値を 1～100 の範囲で指定します。パケットの RSSI が RSSI しきい値より低い場合、パケットは弱信号パケットと判別されます。

説明

calibrate-power 2.4g coverage rssi-threshold コマンドはコマンドは、2.4 GHz 無線での弱信号パケットとして判別する RSSI しきい値を設定します。

undo calibrate-power 2.4g coverage rssi-threshold コマンドはデフォルトに戻します。

例

2.4GHz 無線の弱信号パケットと判別する RSSI しきい値に 80 を設定します。

<Sysname> system-view

[Sysname] wlan global-configuration

[Sysname-wlan-global-configuration] calibrate-power 2.4g coverage rssi-threshold 80

関連コマンド

- **calibrate-power 2.4g coverage weak-signal-client ratio**
- **calibrate-power 2.4g coverage weak-signal-client threshold**
- **calibrate-power 2.4g coverage weak-signal-packet ratio**
- **calibrate-power 2.4g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

14.1.18 calibrate-power 2.4g coverage weak-signal-client ratio

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 2.4g coverage weak-signal-client ratio *percent*

undo calibrate-power 2.4g coverage weak-signal-client ratio

デフォルト

25

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 弱信号クライアント割合のしきい値を 1～100 の範囲で指定します。単位はパーセントです。

説明

calibrate-power 2.4g coverage weak-signal-client ratio コマンドは 2.4 GHz 無線の弱信号クライアント割合のしきい値を設定します。

undo calibrate-power 2.4g coverage weak-signal-client ratio コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱信号クライアントの数が、calibrate-power 2.4 g coverage weak-signal-client threshold コマンドで設定したしきい値に達するか、それを超えた場合。
- 無線に関連付けられた弱信号クライアントの割合が、このコマンドで設定した割合しきい値に達するか、それを超えた場合。

例

2.4GHz 無線の弱信号クライアント割合のしきい値を 30%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 2.4g coverage weak-signal-client ratio 30

関連コマンド

- **calibrate-power 2.4g coverage rssi-threshold**
- **calibrate-power 2.4g coverage weak-signal-client threshold**
- **calibrate-power 2.4g coverage weak-signal-packet ratio**
- **calibrate-power 2.4g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

14.1.19 calibrate-power 2.4g coverage weak-signal-client threshold

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 2.4g coverage weak-signal-client threshold *counts*

undo calibrate-power 2.4g coverage weak-signal-client threshold

デフォルト

3

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

counts: 弱信号クライアント数のしきい値を 1～75 の範囲で指定します。

説明

calibrate-power 2.4g coverage weak-signal-client threshold コマンドは 2.4 GHz 無線の弱信号クライアント数のしきい値を設定します。

undo calibrate-power 2.4g coverage weak-signal-client threshold コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱信号クライアントの数が、このコマンドで設定したしきい値に達するか、それを超えた場合。
- 無線に関連付けられた弱信号クライアントの割合が、**calibrate-power 2.4g coverage weak-signal-client ratio** コマンドで設定した割合しきい値に達するか、それを超えた場合。

例

2.4GHz 無線の弱信号クライアント数のしきい値を 20 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 2.4g coverage weak-signal-client threshold 20

関連コマンド

- **calibrate-power 2.4g coverage rssi-threshold**
- **calibrate-power 2.4g coverage weak-signal-client ratio**
- **calibrate-power 2.4g coverage weak-signal-packet ratio**
- **calibrate-power 2.4g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

14.1.20 calibrate-power 2.4g coverage weak-signal-packet ratio

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 2.4g coverage weak-signal-packet ratio *percent*

undo calibrate-power 2.4g coverage weak-signal-packet ratio

デフォルト

20

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 弱信号パケット割合のしきい値を 1～100 の範囲で指定します。単位はパーセントです。

説明

calibrate-power 2.4g coverage weak-signal-packet ratio コマンドは 2.4 GHz 無線の弱信号パケット割合のしきい値を設定します。

undo calibrate-power 2.4g coverage weak-signal-packet ratio コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- クライアントの弱信号パケット数が、calibrate-power 2.4 g coverage weak-signal-packet threshold コマンドで設定したしきい値に達するか、それを超えた場合。
- クライアントの弱信号パケットの割合が、このコマンドで設定した割合しきい値に達するか、それを超えた場合。

例

2.4GHz 無線の弱信号パケット割合のしきい値を 30%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 2.4g coverage weak-signal-packet ratio 30

関連コマンド

- **calibrate-power 2.4g coverage rssi-threshold**
- **calibrate-power 2.4g coverage weak-signal-client ratio**
- **calibrate-power 2.4g coverage weak-signal-client threshold**
- **calibrate-power 2.4g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

14.1.21 calibrate-power 2.4g coverage weak-signal-packet threshold

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 2.4g coverage weak-signal-packet threshold *counts*

undo calibrate-power 2.4g coverage weak-signal-packet threshold

デフォルト

5

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

counts: クライアントの弱信号パケット数のしきい値を 1～255 の範囲で指定します。

説明

calibrate-power 2.4g coverage weak-signal-packet threshold コマンドは 2.4 GHz 無線の弱信号パケット数のしきい値を設定します。

undo calibrate-power 2.4g coverage weak-signal-packet threshold コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- クライアントの弱信号パケットの数が、このコマンドで設定したしきい値に達するか、それを超えた場合。
- クライアントの弱信号パケットの割合が、**calibrate-power 2.4g coverage weak-signal-packet ratio** コマンドで設定した割合しきい値に達するか、それを超えた場合。

例

2.4GHz 無線の弱信号パケット数のしきい値を 20 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 2.4g coverage weak-signal-packet threshold 20

関連コマンド

- **calibrate-power 2.4g coverage rssi-threshold**
- **calibrate-power 2.4g coverage weak-signal-client ratio**
- **calibrate-power 2.4g coverage weak-signal-client threshold**
- **calibrate-power 2.4g coverage weak-signal-packet ratio**
- **calibrate-power coverage enable**

14.1.22 calibrate-power 2.4g max

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 2.4g max *tx-power*

undo calibrate-power 2.4g max

デフォルト

2.4GHz 無線でサポートされる最大送信電力

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

tx-power: 最大送信電力を 1～27(dBm)の範囲で指定します。

説明

calibrate-power 2.4g max コマンドは TPC 実行後の無線に対して最大伝送電力を設定します。

undo calibrate-power 2.4g max コマンドはデフォルトに戻します。

このコマンドは、auto-TPC で設定できる無線の最大送信電力を設定します。

最大送信電力は、最小送信電力より小さい値を設定することはできません。

例

2.4GHz 無線の最大送信電力を 15 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 2.4g max 15

14.1.23 calibrate-power 5g coverage rssi-threshold

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 5g coverage rssi-threshold *rssi*

undo calibrate-power 5g coverage rssi-threshold

デフォルト

25

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

rssi: RSSI しきい値を 1～100 の範囲で指定します。パケットの RSSI が RSSI しきい値より低い場合、パケットは弱信号パケットと判別されます。

説明

calibrate-power 5g coverage rssi-threshold コマンドはコマンドは、5GHz 無線での弱信号パケットとして判別する RSSI しきい値を設定します。

undo calibrate-power 5g coverage rssi-threshold コマンドはデフォルトに戻します。

例

5GHz 無線の弱信号パケットと判別する RSSI しきい値に 80 を設定します。

<Sysname> system-view

[Sysname] wlan global-configuration

[Sysname-wlan-global-configuration] calibrate-power 5g coverage rssi-threshold 80

関連コマンド

- **calibrate-power 5g coverage weak-signal-client ratio**
- **calibrate-power 5g coverage weak-signal-client threshold**
- **calibrate-power 5g coverage weak-signal-packet ratio**
- **calibrate-power 5g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

14.1.24 calibrate-power 5g coverage weak-signal-client ratio

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 5g coverage weak-signal-client ratio *percent*

undo calibrate-power 5g coverage weak-signal-client ratio

デフォルト

25

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 弱信号クライアント割合のしきい値を 1～100 の範囲で指定します。単位はパーセントです。

説明

calibrate-power 5g coverage weak-signal-client ratio コマンドは 5GHz 無線の弱信号クライアント割合のしきい値を設定します。

undo calibrate-power 5g coverage weak-signal-client ratio コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱信号クライアントの数が、**calibrate-power 5g coverage weak-signal-client threshold** コマンドで設定したしきい値に達するか、それを超えた場合。
- 無線に関連付けられた弱信号クライアントの割合が、このコマンドで設定した割合しきい値に達するか、それを超えた場合。

例

5GHz 無線の弱信号クライアント割合のしきい値を 30%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 5g coverage weak-signal-client ratio 30

関連コマンド

- **calibrate-power 5g coverage rssi-threshold**
- **calibrate-power 5g coverage weak-signal-client threshold**
- **calibrate-power 5g coverage weak-signal-packet ratio**
- **calibrate-power 5g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

14.1.25 calibrate-power 5g coverage weak-signal-client threshold

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 5g coverage weak-signal-client threshold *counts*

undo calibrate-power 5g coverage weak-signal-client threshold

デフォルト

3

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

counts: 弱信号クライアント数のしきい値を 1～75 の範囲で指定します。

説明

calibrate-power 5g coverage weak-signal-client threshold コマンドは 5GHz 無線の弱信号クライアント数のしきい値を設定します。

undo calibrate-power 5g coverage weak-signal-client threshold コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱信号クライアントの数が、このコマンドで設定したしきい値に達するか、それを超えた場合。
- 無線に関連付けられた弱信号クライアントの割合が、**calibrate-power 5g coverage weak-signal-client ratio** コマンドで設定した割合しきい値に達するか、それを超えた場合。

例

5GHz 無線の弱信号クライアント数のしきい値を 20 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 5g coverage weak-signal-client threshold 20

関連コマンド

- **calibrate-power 5g coverage rssi-threshold**
- **calibrate-power 5g coverage weak-signal-client ratio**
- **calibrate-power 5g coverage weak-signal-packet ratio**
- **calibrate-power 5g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

14.1.26 calibrate-power 5g coverage weak-signal-packet ratio

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 5g coverage weak-signal-packet ratio *percent*

undo calibrate-power 5g coverage weak-signal-packet ratio

デフォルト

20

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 弱信号パケット割合のしきい値を 1～100 の範囲で指定します。単位はパーセントです。

説明

calibrate-power 5g coverage weak-signal-packet ratio コマンドは 5GHz 無線の弱信号パケット割合のしきい値を設定します。

undo calibrate-power 5g coverage weak-signal-packet ratio コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- クライアントの弱信号パケット数が、**calibrate-power 5g coverage weak-signal-packet threshold** コマンドで設定したしきい値に達するか、それを超えた場合。
- クライアントの弱信号パケットの割合が、このコマンドで設定した割合しきい値に達するか、それを超えた場合。

例

5GHz 無線の弱信号パケット割合のしきい値を 30%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 5g coverage weak-signal-packet ratio 30

関連コマンド

- **calibrate-power 5g coverage rssi-threshold**
- **calibrate-power 5g coverage weak-signal-client ratio**
- **calibrate-power 5g coverage weak-signal-client threshold**
- **calibrate-power 5g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

14.1.27 calibrate-power 5g coverage weak-signal-packet threshold

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 5g coverage weak-signal-packet threshold *counts*

undo calibrate-power 5g coverage weak-signal-packet threshold

デフォルト

5

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

counts: クライアントの弱信号パケット数のしきい値を 1～255 の範囲で指定します。

説明

calibrate-power 5g coverage weak-signal-packet threshold コマンドは 5GHz 無線の弱信号パケット数のしきい値を設定します。

undo calibrate-power 5g coverage weak-signal-packet threshold コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- クライアントの弱信号パケットの数が、このコマンドで設定したしきい値に達するか、それを超えた場合。
- クライアントの弱信号パケットの割合が、**calibrate-power 5g coverage weak-signal-packet ratio** コマンドで設定した割合しきい値に達するか、それを超えた場合。

例

5GHz 無線の弱信号パケット数のしきい値を 20 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 5g coverage weak-signal-packet threshold 20

関連コマンド

- **calibrate-power 5g coverage rssi-threshold**
- **calibrate-power 5g coverage weak-signal-client ratio**
- **calibrate-power 5g coverage weak-signal-client threshold**
- **calibrate-power 5g coverage weak-signal-packet ratio**
- **calibrate-power coverage enable**

14.1.28 calibrate-power 5g max

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 5g max *tx-power*

undo calibrate-power 5g max

デフォルト

5GHz 無線でサポートされる最大送信電力

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

tx-power: 最大送信電力を 1～27(dBm)の範囲で指定します。

説明

calibrate-power 5g max コマンドは TPC 実行後の無線に対して最大伝送電力を設定します。

undo calibrate-power 5g max コマンドはデフォルトに戻します。

このコマンドは、auto-TPC で設定できる無線の最大送信電力を設定します。

最大送信電力は、最小送信電力より小さい値を設定することはできません。

例

5GHz 無線の最大送信電力を 15 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 5g max 15

14.1.29 calibrate-power 6g coverage rssi-threshold

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 6g coverage rssi-threshold *rssi*

undo calibrate-power 6g coverage rssi-threshold

デフォルト

25

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

rssi: RSSI しきい値を 1～100 の範囲で指定します。パケットの RSSI が RSSI しきい値より低い場合、パケットは弱信号パケットと判別されます。

説明

calibrate-power 6g coverage rssi-threshold コマンドは 6GHz 無線での弱信号パケットとして判別する RSSI しきい値を設定します。

undo calibrate-power 6g coverage rssi-threshold コマンドはデフォルトに戻します。

例

6GHz 無線の弱信号パケットと判別する RSSI しきい値に 80 を設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 6g coverage rssi-threshold 80

関連コマンド

- **calibrate-power 6g coverage weak-signal-client ratio**
- **calibrate-power 6g coverage weak-signal-client threshold**
- **calibrate-power 6g coverage weak-signal-packet ratio**
- **calibrate-power 6g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

14.1.30 calibrate-power 6g coverage weak-signal-client ratio

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 6g coverage weak-signal-client ratio *percent*

undo calibrate-power 6g coverage weak-signal-client ratio

デフォルト

25

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 弱信号クライアント割合のしきい値を 1～100 の範囲で指定します。単位はパーセントです。

説明

calibrate-power 6g coverage weak-signal-client ratio コマンドは 6GHz 無線の弱信号クライアント割合のしきい値を設定します。

undo calibrate-power 6g coverage weak-signal-client ratio コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱信号クライアントの数が、**calibrate-power 6g coverage weak-signal-client threshold** コマンドで設定したしきい値に達するか、それを超えた場合。
- 無線に関連付けられた弱信号クライアントの割合が、このコマンドで設定した割合しきい値に達するか、それを超えた場合。

例

6GHz 無線の弱信号クライアント割合のしきい値を 30%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 6g coverage weak-signal-client ratio 30

関連コマンド

- **calibrate-power 6g coverage rssi-threshold**
- **calibrate-power 6g coverage weak-signal-client threshold**
- **calibrate-power 6g coverage weak-signal-packet ratio**
- **calibrate-power 6g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

14.1.31 calibrate-power 6g coverage weak-signal-client threshold

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 6g coverage weak-signal-client threshold *counts*

undo calibrate-power 6g coverage weak-signal-client threshold

デフォルト

3

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

counts: 弱信号クライアント数のしきい値を 1～75 の範囲で指定します。

説明

calibrate-power 6g coverage weak-signal-client threshold コマンドは 6GHz 無線の弱信号クライアント数のしきい値を設定します。

undo calibrate-power 6g coverage weak-signal-client threshold コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱信号クライアントの数が、このコマンドで設定したしきい値に達するか、それを超えた場合。
- 無線に関連付けられた弱信号クライアントの割合が、**calibrate-power 6g coverage weak-signal-client ratio** コマンドで設定した割合しきい値に達するか、それを超えた場合。

例

5GHz 無線の弱信号クライアント数のしきい値を 20 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 6g coverage weak-signal-client threshold 20

関連コマンド

- **calibrate-power 6g coverage rssi-threshold**
- **calibrate-power 6g coverage weak-signal-client ratio**
- **calibrate-power 6g coverage weak-signal-packet ratio**
- **calibrate-power 6g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

14.1.32 calibrate-power 6g coverage weak-signal-packet ratio

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 6g coverage weak-signal-packet ratio *percent*

undo calibrate-power 6g coverage weak-signal-packet ratio

デフォルト

20

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 弱信号パケット割合のしきい値を 1～100 の範囲で指定します。単位はパーセントです。

説明

calibrate-power 6g coverage weak-signal-packet ratio コマンドは 6GHz 無線の弱信号パケット割合のしきい値を設定します。

undo calibrate-power 6g coverage weak-signal-packet ratio コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- クライアントの弱信号パケット数が、**calibrate-power 6g coverage weak-signal-packet threshold** コマンドで設定したしきい値に達するか、それを超えた場合。
- クライアントの弱信号パケットの割合が、このコマンドで設定した割合しきい値に達するか、それを超えた場合。

例

6GHz 無線の弱信号パケット割合のしきい値を 30%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 6g coverage weak-signal-packet ratio 30

関連コマンド

- **calibrate-power 6g coverage rssi-threshold**
- **calibrate-power 6g coverage weak-signal-client ratio**
- **calibrate-power 6g coverage weak-signal-client threshold**
- **calibrate-power 6g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

14.1.33 calibrate-power 6g coverage weak-signal-packet threshold

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 6g coverage weak-signal-packet threshold *counts*

undo calibrate-power 6g coverage weak-signal-packet threshold

デフォルト

5

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

counts: クライアントの弱信号パケット数のしきい値を 1～255 の範囲で指定します。

説明

calibrate-power 6g coverage weak-signal-packet threshold コマンドは 6GHz 無線の弱信号パケット数のしきい値を設定します。

undo calibrate-power 6g coverage weak-signal-packet threshold コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- クライアントの弱信号パケットの数が、このコマンドで設定したしきい値に達するか、それを超えた場合。
- クライアントの弱信号パケットの割合が、**calibrate-power 6g coverage weak-signal-packet ratio** コマンドで設定した割合しきい値に達するか、それを超えた場合。

例

6GHz 無線の弱信号パケット数のしきい値を 20 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 6g coverage weak-signal-packet threshold 20

関連コマンド

- **calibrate-power 6g coverage rssi-threshold**
- **calibrate-power 6g coverage weak-signal-client ratio**
- **calibrate-power 6g coverage weak-signal-client threshold**
- **calibrate-power 6g coverage weak-signal-packet ratio**
- **calibrate-power coverage enable**

14.1.34 calibrate-power 6g max

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 6g max *tx-power*

undo calibrate-power 6g max

デフォルト

6GHz 無線でサポートされる最大送信電力

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

tx-power: 最大送信電力を 1～27(dBm)の範囲で指定します。

説明

calibrate-power 6g max コマンドは TPC 実行後の無線に対して最大伝送電力を設定します。

undo calibrate-power 6g max コマンドはデフォルトに戻します。

このコマンドを設定すると、無線の伝送電力は設定値を超えなくなります。

最大送信電力は、最小送信電力より小さい値を設定することはできません。

例

6GHz 無線の最大送信電力を 15 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 6g max 15

14.1.35 calibrate-power coverage enable

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。
Global configuration View の 6g パラメータはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

Radio view または AP グループの Radio view:

calibrate-power coverage { disable | enable }

undo calibrate-power coverage

Global configuration View:

calibrate-power coverage enable { 2.4g | 5g | 6g | all }

undo calibrate-power coverage enable { 2.4g | 5g | 6g | all }

デフォルト

Radio view：AP group view の設定を使用します。

AP group Radio view：global configuration view の設定を使用します。

Global configuration view：無効

View

Radio view

AP group Radio view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

2.4g: 2.4GHz 無線を指定します。

5g: 5GHz 無線を指定します。

6g: 6GHz 無線を指定します。

all: ソフトウェアバージョン 7.2.75 を含む以降のソフトウェアでは 2.4GHz 無線、5GHz 無線、6GHz 無線のすべてを指定します。

ソフトウェアバージョン 7.2.73 を含む以前のソフトウェアでは 2.4GHz 無線と 5GHz 無線両方を指定します。

説明

calibrate-power coverage enable コマンドは死角検出を有効にします。

calibrate-power coverage disable コマンドは死角検出を無効にします。

undo calibrate-power coverage コマンドはデフォルトに戻します。

この機能により、AC は無線信号カバレッジに死角 (または弱い信号領域) が存在するかどうかを判断できます。死角が検出された場合、AC は auto-TPC を実行するときに対応する AP の送信電力を増加させます。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱信号クライアントの数が、しきい値に達するか、または超えている場合。
- 無線に関連付けられた弱信号クライアントの割合がしきい値に達するか、それを超えている場合。

AC は、次の条件が満たされた場合に、クライアントが弱信号クライアントであると判断します。

- クライアントの弱信号パケット数がしきい値に達するか、またはしきい値を超えた場合。
- クライアントの弱信号パケットの割合がしきい値に達するか、それを超えた場合。

パケットの RSSI が RSSI しきい値より低い場合、そのパケットは弱信号パケットと見なされます。

例

ap1 と名付けた AP の Radio3 で死角検出を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 3

[AC-wlan-ap-ap1-radio-3] calibrate-power coverage enable

group1 と名付けた AP group のモデル **QX-W1020** の無線 3 で、死角検出を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 3

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-3] calibrate-power coverage enable

#グローバルで 2.4GHz 無線の死角検出を有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power coverage enable 2.4g

関連コマンド

- calibrate-power 2.4g coverage rssi-threshold
- calibrate-power 2.4g coverage weak-signal-client ratio
- calibrate-power 2.4g coverage weak-signal-client threshold
- calibrate-power 2.4g coverage weak-signal-packet ratio
- calibrate-power 2.4g coverage weak-signal-packet threshold
- calibrate-power 5g coverage rssi-threshold
- calibrate-power 5g coverage weak-signal-client ratio
- calibrate-power 5g coverage weak-signal-client threshold
- calibrate-power 5g coverage weak-signal-packet ratio
- calibrate-power 5g coverage weak-signal-packet threshold
- calibrate-power 6g coverage rssi-threshold
- calibrate-power 6g coverage weak-signal-client ratio
- calibrate-power 6g coverage weak-signal-client threshold
- calibrate-power 6g coverage weak-signal-packet ratio
- calibrate-power 6g coverage weak-signal-packet threshold

14.1.36 calibrate-power min

Syntax

calibrate-power min *tx-power*

undo calibrate-power min

デフォルト

RRM view: AP group view の設定を使用します。

AP group RRM view: 11dBm (ソフトウェアバージョン 7.2.18 を含む以前)

1dBm (ソフトウェアバージョン 7.2.21)

6dBm (ソフトウェアバージョン 7.2.27 を含む以降)

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

tx-power: 無線に対する最小伝送電力を指定します。

ソフトウェアバージョン 7.2.18 を含む以前のソフトウェアでの設定範囲は 11~20dBm です。

ソフトウェアバージョン 7.2.19 を含む以降のソフトウェアでの設定範囲は 1~20dBm です。

説明

calibrate-power min コマンドは TPC 実行後の無線に対して最小伝送電力を設定します。

undo calibrate-power min コマンドはデフォルトに戻します。

このコマンドは、TPC が実行された後も無線の伝送電力がネットワーク要求を満足できることを保証します。

例

ap1 と名付けた AP の無線 1 に対して最小伝送電力を 10dBm で設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-power min 10

group1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して最小伝送電力を 10dBm で設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-power min 10

14.1.37 calibrate-power mode

Syntax

calibrate-power mode { **coverage** | **custom** | **density** }

undo calibrate-power mode

デフォルト

RRM view では、AP group RRM view の構成が使用されます。

AP group RRM view では、TPC モードはカスタムです。

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

coverage: カバレッジモードを指定します。

custom: カスタムモードを指定します。

density: デンシティモードを指定します。

説明

calibrate-power mode コマンドは TPC モードを設定します。

undo calibrate-power mode コマンドはデフォルトに戻します。

AP 間の干渉を避けるには、デンシティモードを使用します。信号カバレッジのパフォーマンスを向上させるには、カバレッジモードを使用します。これらの 2 つのモードがネ

ットワーク要件を満たせない場合は、カスタムモードを使用して電力調整設定をカスタマイズします。

デンシティモードまたはカバレッジモードでは、電力調整の設定はシステムによって定義され、変更することはできません。

例

AP **ap1** の無線 1 に対して TPC モードをカバレッジに設定します。

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-power mode coverage

AP グループ **group1** のモデル **QX-W1020** の無線 1 に対して TPC モードをデンシティに設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-power mode density

14.1.38 calibrate-power self-decisive

Syntax

calibrate-power self-decisive { **disable** | **enable** }

undo calibrate-power self-decisive

デフォルト

RRM view：AP group view の設定を使用します。

AP group RRM view：無効

View

RRM view

AP group RRM view

Global configuration view(ソフトウェアバージョン 7.2.24 以降のバージョンでサポート)

定義済みユーザロール

network-admin

パラメータ

disable: AC がパワーキャリブレーション間隔で TPC を実行するための定期的な auto-TPC を無効にします。

enable: AC がパワーキャリブレーション間隔で TPC を実行するための定期的な auto-TPC を有効にします。

説明

calibrate-power self-decisive enable コマンドは AC がパワーキャリブレーション間隔で TPC を実行するための定期的な auto-TPC を有効にします。

calibrate-power self-decisive disable コマンドは AC がパワーキャリブレーション間隔で TPC を実行するための定期的な auto-TPC を無効にします。

undo calibrate-power self-decisive コマンドはデフォルトに戻します。

例

ap1 と名付けた AP の無線 1 に対して auto-TPC を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-power self-decisive enable

group1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して auto-TPC を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-power self-decisive enable

関連コマンド

wlan rrm calibration-power interval

14.1.39 calibrate-power threshold

Syntax

calibrate-power threshold *value*

undo calibrate-power threshold

デフォルト

RRM view：AP group view の設定を使用します。

AP group RRM view：65(ソフトウェアバージョン 7.2.21 を含む以前)

75(ソフトウェアバージョン 7.2.27 を含む以降)

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

value: 電力しきい値を範囲で指定します。

ソフトウェアバージョン 7.2.18 を含む以前のソフトウェアでの設定範囲は 50～90 です。

この範囲は、無線の電力が-90dBm~-50dBm の範囲にあることを示します。

ソフトウェアバージョン 7.2.21 を含む以降のソフトウェアでの設定範囲は 1~196 です。

この範囲は、無線の電力が-196dBm~-1dBm の範囲にあることを示します。

説明

calibrate-power threshold コマンドは電力しきい値を設定します。

undo calibrate-power threshold コマンドはデフォルトに戻します。

無線同士の干渉を防ぐため、高密度な WLAN では-80dBm に設定することを推奨します。

例

ap1 と名付けた AP の無線 1 に対して電力しきい値を 70 で設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-power threshold 70

group1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して電力しきい値を 70 で設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-power threshold 70

14.1.40 channel holddown-time

Syntax

channel holddown-time *minutes*

undo channel holddown-time

デフォルト

720 分

View

RRM holddown group view

定義済みユーザロール

network-admin

パラメータ

minutes: channel holddown time を 10~1440 分の範囲で指定します。

説明

channel holddown-time コマンドは channel holddown time を設定します。

undo channel holddown-time コマンドはデフォルトに戻します。

RRM holddown group 内の無線のチャネルが変更されるたび、システムは無線に対する channel holddown タイマを開始します。RRM holddown group 内のすべての無線に対するチャネルは、指定された channel holddown time 中は保持されます。

例

RRM holddown group 10 に対して channel holddown time を 600 分に設定します。

<AC> system-view

[AC] wlan rrm-calibration-group 10

[AC-wlan-rrm-calibration-group-10] channel holddown-time 600

14.1.41 channel-capability mode

Syntax

channel-capability mode { **all** | **none** | **partial** }

undo channel-capability mode

デフォルト

radio view：AP group view の設定を使用します。

AP group radio view：チェックなし

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

all: all モードを指定します。クライアントは、クライアントのサポートされたチャネルがすべて、無線のサポートされたチャネルと一致するときのみ紐付けを許可されます。

none: none モードを指定します。クライアントチャネル能力はチェックされません。

partial: partial モードを指定します。クライアントは、クライアントのサポートされたチャネルのうち 1 つでも、無線のサポートされたチャネルのうちの 1 つと一致すれば紐付けを許可されます。

説明

channel-capability mode コマンドはクライアントチャネル能力マッチモードを設定します。

undo channel-capability mode コマンドはデフォルトに戻します。

このコマンドは、5GHz 無線でのみ使用できます。

このコマンドは、無線が 5GHz モードで動作し、スペクトル管理が有効なときのみ無線に対して効力をもちます。

例

ap1 と名付けた AP の無線 1 に対して **all** モードを設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] spectrum-management enable

[AC-wlan-ap-ap1-radio-1] channel-capability mode all

apgroup1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して **all** モードを設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] spectrum-management enable

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] channel-capability mode all

関連コマンド

spectrum-management

14.1.42 channel-switch mode

Syntax

channel-switch mode { **continuous** | **suspend** }

undo channel-switch mode

デフォルト

radio view：AP group view の設定を使用します。

AP group radio view：チャネルスイッチの間、オンライン中のすべてのクライアントはフレームの送信を停止します。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

continuous：チャネルスイッチの間、オンライン中のクライアントがフレームの送信を継続するように設定します。

suspend：チャネルスイッチが完了するまで、オンライン中のクライアントがフレームの送信を停止するように設定します。

説明

channel-switch mode コマンドはチャネルスイッチモードを設定します。

undo channel-switch mode コマンドはデフォルトに戻します。

例

ap1 と名付けた AP の無線 1 に対して **continuous** モードを設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] spectrum-management enable

[AC-wlan-ap-ap1-radio-1] channel-switch mode continuous

apgroup1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して **continuous** モードを設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] spectrum-management enable

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] channel-switch mode continuous

関連コマンド

spectrum-management

14.1.43 crc-error-threshold

Syntax

crc-error-threshold *percent*

undo crc-error-threshold

デフォルト

RRM view：AP group view の設定を使用します。

AP group RRM view：20%(ソフトウェアバージョン 7.2.21 を含む以前)

0%(ソフトウェアバージョン 7.2.27 を含む以降)

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

percent: CRC エラーしきい値を 0~100%の範囲で指定します。

説明

crc-error-threshold コマンドは CRC エラーしきい値を設定します。

undo crc-error-threshold コマンドはデフォルトに戻します。

すべての 802.11 パケットの CRC エラーパケットの割合が無線の CRC エラーしきい値に達したことを AC が検出すると、無線は DFS を実行します。

例

ap1 と名付けた AP の無線 1 に対して CRC エラーしきい値を 50%で設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] crc-error-threshold 50

apgroup1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して CRC エラーしきい値を 50%で設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] crc-error-threshold 50

14.1.44 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

RRM holddown group view

定義済みユーザロール

network-admin

パラメータ

text: RRM holddown group 記述を 1~64 字のケースセンシティブな文字列で指定します。

説明

description コマンドは RRM holddown group に記述を設定します。

undo description コマンドはデフォルトに戻します。

例

RRM holddown group 10 に対する記述を office に設定します。

<AC> system-view

[AC] wlan rrm-calibration-group 10

[AC-wlan-rrm-calibration-group-10] description office

14.1.45 display wlan rrm baseline

Syntax

display wlan rrm baseline { **all** | **name** *baseline-name* } [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての無線ベースラインを指定します。

name *baseline-name*: 無線ベースラインを名前で指定します。大文字と小文字を区別しない 1～32 文字の文字列を指定します。

verbose: 詳細情報を表示します。このキーワードを指定しない場合、コマンドは簡易情報を表示します。

説明

display wlan rrm baseline コマンドは無線ベースライン情報を表示します。

無線ベースラインのロケーション識別子を使用して無線を管理する権利がない場合、無線ベースラインに関する情報を表示することはできません。

例

無線ベースラインの簡易情報を表示します。

<AC> display wlan rrm baseline all

```
Baseline name  : apbaseline
Radio range    : AP
Created at     : 2015-06-22 19:56:31

Baseline name  : groupbaseline
Radio range    : AP group
Created at     : 2015-06-22 19:56:12

Baseline name  : globalbaseline
Radio range    : Global
Created at     : 2015-06-22 19:55:12
```

表 14-1 コマンド出力

フィールド	説明
Radio range	ベースラインに保存された無線の範囲: • **AP**—AP上の無線 • **AP group**—APグループ内のAP上の無線 • **Global**—ACに関連付けられたすべてのAPの無線
Created at	ベースラインが作成された日時

無線ベースラインの詳細情報を表示します。

<AC> display wlan rrm baseline all verbose

```
--------------------------------------------------------------------------------
Baseline name : apbaseline
Radio range   : AP
Created at    : 2015-06-22 19:56:31
--------------------------------------------------------------------------------
APName           RadioID RadioType Bandwidth Channel Power RegionCode
--------------------------------------------------------------------------------
```

```
ap1             2      dot11gn   20       13      20    CN
------------------------------------------------------------------------------


------------------------------------------------------------------------------
 Baseline name : groupbaseline
 Radio range   : AP group
 Created at    : 2015-06-22 19:56:12
------------------------------------------------------------------------------
 APName           RadioID RadioType Bandwidth Channel Power RegionCode
------------------------------------------------------------------------------
 ap1             1      dot11an   40       64     20    CN
 ap2             1      dot11an   40       56     20    CN
------------------------------------------------------------------------------


------------------------------------------------------------------------------
 Baseline name : globalbaseline
 Radio range   : Global
 Created at    : 2015-06-22 19:55:12
------------------------------------------------------------------------------
 APName           RadioID RadioType Bandwidth Channel Power RegionCode
------------------------------------------------------------------------------
 ap1             1      dot11an   40       64     20    CN
 ap1             2      dot11gn   20       13      20    CN
 ap2             1      dot11an   40       64     20    CN
 ap2             2      dot11gn   20       1       20    CN
------------------------------------------------------------------------------
```

表 14-2 コマンド出力

フィールド	説明
Radio range	ベースラインに保存された無線の範囲: • **AP**—AP上の無線 • **AP group**—APグループ内のAP上の無線 • **Global**—ACに関連付けられたすべてのAPの無線
Created at	ベースラインが作成された日時
Power	無線の送信電力（dBm）
RegionCode	APの地域コード

14.1.46 display wlan rrm baseline apply-result

Syntax

display wlan rrm baseline apply-result

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan rrm baseline apply-result コマンドは無線ベースラインの最新のアプリケーション結果を表示します。

例

無線ベースラインの最新のアプリケーション結果を表示します。

<AC> display wlan rrm baseline apply-result

```
Radio count : 6
Success    : 4
Failure    : 2
Failure reason
  Radio doesn't exist         : 0
  Radio is down              : 0
  Mismatching radio type      : 0
  Mismatching region code     : 1
  No service template         : 0
  Illegal channel            : 0
  Mismatching bandwidth       : 1
  Channel locked             : 0
  Channel fixed              : 0
  Within channel holddown time  : 0
  Mismatching channel gap policy: 0
  Power locked               : 0
  Within power holddown time   : 0
  Power lower than min. power  : 0
  Power greater than max. power : 0
```

表 14-3 コマンド出力

フィールド	説明
Radio count	無線ベースライン内の無線の数です。
Success	成功したアプリケーションの数です。
Failure	失敗したアプリケーションの数です。
Mismatching radio type	ベースラインに保存された無線モードが実際の無線モードと一致しません。
Mismatching region code	ベースラインに保存されたリージョンコードは、APの実際のリージョンコードと一致しません。
Wireless service not effective	サービステンプレートは、ベースラインの無線にバインドされていないか、バインドされたサービステンプレートが無効になっています。
Mismatching channel gap policy	ベースラインのチャネルが、指定されたチャネルギャップと一致しません。
Power lower than min. power	ベースラインの送信電力は、指定された最小送信電力よりも低いです。
Power greater than max. power	ベースラインの送信電力は、指定された最大送信電力よりも高いです。

14.1.47 display wlan rrm-calibration-group

Syntax

display wlan rrm-calibration-group { **all** | *group-id* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: RRM holddown group を指定します。

group-id: ID で RRM holddown group を指定します。この引数の値の範囲は 1~128 です。

説明

display wlan rrm-calibration-group コマンドは RRM holddown group 情報を表示します。

例

RRM holddown group 10 の情報を表示します。

<AC> display wlan rrm-calibration-group 10

```
        RRM Calibration Group Information
-------------------------------------------------------------------------
Group ID             : 10
Description          : office
Channel holddown time   : 720 minutes
Power holddown time    : 60 minutes
Group members         : ap4-radio2, ap3-radio2
-------------------------------------------------------------------------
```

表 14-4 コマンド出力

Field	Description
Group ID	RRM holddown groupのID
Description	RRM holddown groupに対する記述
Channel holddown time	Channel holddown time
Power holddown time	Power holddown time
Group members	RRM holddown group内のRadios

14.1.48 display wlan rrm-history ap

Syntax

display wlan rrm-history ap { **all** | **name** *ap-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

説明

display wlan rrm-history ap コマンドは、チャネルと電力に関する最新 10 件までの変動履歴を表示します。変動履歴には、時間、原因、電力、干渉が含まれます。

例

過去のチャネルと電力の情報を表示します。

<AC> display wlan rrm-history ap name ap1

```
                          AP RRM History
--------------------------------------------------------------------------------
 Flags : I - Interference,   P - Packets discarded,    F - Retransmission,
        R - Radar select,   C - Coverage,           B - Channelbusy,
        M - Manual,        D - Bandwidth,          O - Others
--------------------------------------------------------------------------------

                      AP RRM History : ap1
--------------------------------------------------------------------------------
 Radio : 2                           Basic BSSID : 000f-e2ff-7700
--------------------------------------------------------------------------------
       Ch  Power BW    Load Util Intf Reason    Date        Time
           (dBm) (MHz) (%)  (%)  (%)          (yyyy-mm-dd) (hh:mm:ss)
--------------------------------------------------------------------------------
 Before 132 20    20    5    0    8    ----C---- 2022-11-04   12:57:27
 After  132 17    20    5    0    8    -         -           -
--------------------------------------------------------------------------------
 Before 132 17    20    5    0    8    ----C---- 2022-11-04   13:08:27
 After  132 14    20    5    0    8    -         -           -
--------------------------------------------------------------------------------
 Before 132 14    20    5    0    8    ----C---- 2022-11-04   13:19:27
 After  132 11    20    5    0    8    -         -           -
--------------------------------------------------------------------------------
 Before 124 11    20    22   5    9    ---R----- 2022-11-07   05:58:57
 After  100 11    20    25   2    11   -         -           -
--------------------------------------------------------------------------------
```

表 14-5 コマンド出力

Field	Description
Radio	Radio ID
Basic BSSID	Basic service set identifier
Ch	無線の動作チャネル
Power	無線の伝送電力
BW	無線の帯域幅モード
Load	チャネルロードの割合
Util	チャネル使用の割合
Intf	チャネルで検出された干渉の割合
Reason	チャネルもしくは電力もしくは帯域幅モードの変動理由
Date	チャネルもしくは電力もしくは帯域幅モードの変動した日付
Time	チャネルもしくは電力もしくは帯域幅モードの変動した時間

14.1.49 display wlan rrm-status ap

Syntax

display wlan rrm-status ap { **all** | **name** *ap-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

説明

display wlan rrm-status ap コマンドは詳細な RRM の情報を表示します。

チャネルと電力の両方とも無効な場合、このコマンドは RRM の情報を表示しません。

例

チャネルと電力に関する詳細な情報を表示します。

<AC> display wlan rrm-status ap name ap1

```
                    AP RRM Profile : ap1
-------------------------------------------------------------------------------
 Radio   : 1                          Basic BSSID    : 70f9-6d31-2fe0
 Channel : 157                         Tx Power (dBm) : 18
-------------------------------------------------------------------------------
   Ch    Nbrs    Load    Util    Intf    PER    Retry    Radar
                 (%)     (%)     (%)     (%)     (%)
-------------------------------------------------------------------------------
   36    0       0       -       0       0      -        -
   40    0       0       -       0       0      -        -
   44    0       0       -       0       0      -        -
   48    0       0       -       0       0      -        -
   52    0       0       -       0       0      -        -
   56    0       0       -       0       0      -        -
   60    0       0       -       0       0      -        -
   64    0       0       -       0       0      -        -
   100   0       0       -       0       0      -        -
   104   0       0       -       0       0      -        -
   108   0       0       -       0       0      -        -
   112   0       0       -       0       0      -        -
   116   0       0       -       0       0      -        -
   132   0       0       -       0       0      -        -
   136   0       0       -       0       0      -        -
   140   0       0       -       0       0      -        -
-------------------------------------------------------------------------------
  Nbr-MACAddress   Ch    Intf   SignalStrength   Type
                        (%)    (dBm)
-------------------------------------------------------------------------------
  000f-e212-ff01   52   0      -60              Unmanaged
  5866-ba74-e461   48   0      -72              Unmanaged
```

```
  70f9-6d30-9020   48   0      -40            Managed
  70f9-6d31-3080   44   0      -54            Managed
  70f9-6d31-34e0   52   0      -59            Managed
  7425-8a86-bbe0   48   0      -48            Unmanaged
  7425-8a86-c720   48   0      -63            Unmanaged
--------------------------------------------------------------------------------
 Radio   : 2                          Basic BSSID    : 70f9-6d31-2ff0
 Channel : 1                          Tx Power (dBm) : 19
--------------------------------------------------------------------------------
    Ch    Nbrs    Load    Util    Intf    PER    Retry    Radar
                 (%)     (%)     (%)     (%)     (%)
--------------------------------------------------------------------------------
    1     6       4       0       4       0      0        -
    6     4       2       -       2       0      -        -
    11    6       2       -       2       0      -        -
--------------------------------------------------------------------------------
  Nbr-MACAddress   Ch    Intf   SignalStrength   Type
                         (%)    (dBm)
--------------------------------------------------------------------------------
  000f-e212-ff11   1     49     -77              Unmanaged
  0023-89e1-ed00   11    0      -87              Unmanaged
  006a-55f6-ae10   1     57     -88              Unmanaged
  5866-ba64-aa31   1     10     -60              Unmanaged
  5866-ba74-e471   6     0      -76              Unmanaged
  5866-baa9-a610   11    0      -62              Unmanaged
  70f9-6d30-9030   6     0      -63              Managed
  70f9-6d31-3090   1     51     -86              Managed
  70f9-6d31-34f0   6     0      -85              Managed
  7425-8a86-bbf0   6     0      -73              Unmanaged
  7425-8a86-c731   11    0      -93              Unmanaged
  80f6-2ec0-3330   11    0      -76              Unmanaged
  80f6-2ec0-3331   11    0      -73              Unmanaged
  80f6-2edd-d2d0   1     40     -60              Unmanaged
  80f6-2edd-d2d1   1     44     -68              Unmanaged
  80f6-2ede-0b30   11    0      -74              Unmanaged
```

表 14-6 コマンド出力

Field	Description
Radio	Radio ID
Basic BSSID	Basic service set identifier
Channel	無線の動作チャネル

Field	Description
Tx Power	無線の伝送電力
Ch	無線にサポートされたチャネル
Nbrs	検出された無線の数
Load	チャネルで検出されたロードの割合(%)。チャネルロードは、干渉と同様に、アウトバウンドパケットとインバウンドパケット間の割合を参照します。干渉は無線によって受信されるエラーパケットを参照します。
Util	チャネル使用の割合(%)。チャネル使用はアウトバウンドパケットとインバウンドパケット間の割合を参照します。
Intf	チャネルで検出された干渉の割合(%)。
PER	チャネルで検出されたビットエラーレート(%)。
Retry	チャネルで検出された再伝送レート(%)。
Radar	レーダ検出状況 ● –：チャネルでレーダ信号は検出されませんでした。 ● **Detected**：チャネルでレーダ信号が検出されました。
Nbr-MACAddress	検出された無線のMACアドレス
SignalStrength	無線の信号強度（dBm）
Type	無線のタイプ ● **Managed**—同じACによって管理されている無線です。 ● **Unmanaged**—検出されましたが、同じACによって管理されていない無線です。

14.1.50 interference-threshold

Syntax

interference-threshold *percent*

undo interference-threshold

デフォルト

RRM view：AP group view の設定を使用します。

AP group RRM view：50%(ソフトウェアバージョン 7.2.21 を含む以前)

70%(ソフトウェアバージョン 7.2.27 を含む以降)

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

percent: チャネル干渉しきい値を 0~100%の範囲で指定します。

説明

interference-threshold コマンドはチャネル干渉しきい値を設定します。

undo interference-threshold コマンドはデフォルトに戻します。

すべてのデータパケットの干渉パケットの割合が無線の干渉しきい値に達したことを AC が検出すると、無線は DFS を実行します。干渉パケットは、他の無線に送信されるパケットです。

例

ap1 と名付けた AP の無線 1 に対してチャネル干渉しきい値を 60%で設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] interference-threshold 60

group1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対してチャネル干渉しきい値を 60%で設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] interference-threshold 60

14.1.51 power holddown-time

Syntax

power holddown-time *minutes*

undo power holddown-time

デフォルト

60 分

View

RRM holddown group view

定義済みユーザロール

network-admin

パラメータ

minutes: power holddown time を 10~1440 分の範囲で指定します。

説明

power holddown-time コマンドは power holddown time を設定します。

undo power holddown-time コマンドはデフォルトに戻します。

RRM holddown group 内の無線の電力が変更されるたび、システムは無線に対する power holddown タイマを開始します。RRM holddown group 内のすべての無線に対する電力は、指定された power holddown time 中は保持されます。

例

RRM holddown group 10 に対して power holddown time を 600 分に設定します。

<AC> system-view

[AC] wlan rrm-calibration-group 10

[AC-wlan-rrm-calibration-group-10] power holddown-time 600

14.1.52 power-capability mode

Syntax

power-capability mode { **all** | **none** | **partial** }

undo power-capability mode

デフォルト

radio view：AP group view の設定を使用します。

AP group radio view：チェックなし

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

all: all モードを指定します。クライアントは、クライアントの伝送電力能力がすべて、無線の伝送電力能力と一致するときのみ無線への紐付けを許可されます。

none: none モードを指定します。クライアント伝送電力能力はチェックされません。

partial: partial モードを指定します。クライアントは、クライアントの伝送電力能力のうち 1 つでも、無線の伝送電力能力のうちの 1 つと一致すれば無線への紐付けを許可されます。

説明

power-capability mode コマンドは送信電力機能一致モードを設定します。

undo power-capability mode コマンドはデフォルトに戻します。

このコマンドはスペクトル管理もしくは無線資源計測が有効な場合にのみ反映されます。無線資源計測に関する詳細は、オペレーションマニュアルのセクション 2 *WLAN* を参照してください。

例

ap1 と名付けた AP の無線 1 に対して **all** モードを設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] spectrum-management enable

[AC-wlan-ap-ap1-radio-1] power-capability mode all

apgroup1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して **all** モードを設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] spectrum-management enable

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] power-capability mode all

関連コマンド

- **resource-measure**
- **spectrum-management**

14.1.53 power-constraint mode

Syntax

power-constraint mode { **auto** [**anpi-interval** *anpi-interval-value*] | **manual** *power-constraint* }

undo power-constraint mode

デフォルト

radio view：AP group view の設定を使用します。

AP group radio view：auto

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

auto: auto モードを指定します。

anpi-interval *anpi-interval-value*: 電力制限の値を計算するため、ANPI（Average Noise Power Indicator）に 0~30dBM の範囲で値を追加します。デフォルト値は 10dBm です。

manual *power-constraint*: 電力制限の値を 0~30dBm の範囲で指定します。

説明

power-constraint mode コマンドは電力制約モードを設定します。

undo power-constraint mode コマンドはデフォルトに戻します。

このコマンドは、5GHz 無線でのみ使用できます。

auto モードを指定する場合、装置は以下の数式を用いて電力制限の値を計算します。

power-constraint = RCPI (Received Channel Power Indicator)-(ANPI + *anpi-interval-value*)

このコマンドはスペクトル管理と無線資源計測を有効にした場合のみ効力を持ちます。無線資源計測に関する詳細は、オペレーションマニュアルのセクション 2 *WLAN* を参照してください。

例

ap1 と名付けた AP の無線 1 に対して **manual** モードを設定し、電力制限の値を 5dBm に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] spectrum-management enable

[AC-wlan-ap-ap1-radio-1] power-constraint mode manual 5

apgroup1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して **manual** モードを設定し、電力制限の値を 5dBm に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] spectrum-management enable

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] power-constraint mode manual 5

関連コマンド

- **resource-measure**
- **spectrum-management**

14.1.54 rrm

Syntax

rrm

View

Radio view

定義済みユーザロール

network-admin

説明

rrm コマンドは RRM（Radio Resource Management）view に移行します。

例

RRM view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

14.1.55 scan-only

Syntax

scan-only { **disable** | **enable** }

undo scan-only

デフォルト

RRM view では、AP group RRM view の構成が使用されます。

AP group RRM view では、無線スキャンが無効になっています。

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

disable: 無線スキャンを無効にします。

enable: 無線スキャンを有効にします。

説明

scan-only enable コマンドは無線スキャンを有効にします。

scan-only disable コマンドは無線スキャンを無効にします。

undo scan-only コマンドはデフォルトに戻します。

この機能により、AP は WLAN 環境をスキャンし、収集された統計情報を指定された間隔で AC に報告します。AC は統計を使用してチャネルレポートとネイバーレポートを生成します。

チャネルレポートおよびネイバーレポートを表示するには、**display wlan rrm-status ap** コマンドを使用します。

定期的な auto-DFS、スケジュールされた auto-DFS、または定期的な auto-TPC を設定した場合、この機能をイネーブルにする必要はありません。

例

AP **ap1** の無線 1 に対して無線スキャンを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] scan-only enable

AP グループ **group1** のモデル **QX-W1020** の無線 1 に対して無線スキャンを有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] scan-only enable

関連コマンド

display wlan rrm-status ap

14.1.56 snmp-agent trap enable wlan rrm

Syntax

snmp-agent trap enable wlan rrm

undo snmp-agent trap enable wlan rrm

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan rrm コマンドは WLAN RRM に SNMP 通知を有効にします。

undo snmp-agent trap enable wlan rrm コマンドはデフォルトに戻します。

NMS に WLAN RRM の重要なイベントを通知するために、SNMP 通知を有効にしてください。WLAN RRM 通知を正しく送信するために、オペレーションマニュアルのセクション 11 *システム管理 “SNMP”* に記述されるように SNMP の設定も行わなければなりません。

例

WLAN RRM に SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan rrm

14.1.57 spectrum-management

Syntax

spectrum-management { **enable** | **disable** }

undo spectrum-management

デフォルト

radio view：AP group view の設定を使用します。

AP group radio view：無効

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

enable: スペクトル管理を有効にします。

disable: スペクトル管理を無効にします。

説明

spectrum-management enable コマンドはスペクトル管理を有効にします。

spectrum-management disable コマンドはスペクトル管理を無効にします。

undo spectrum-management コマンドはデフォルトに戻します。

このコマンドは、5GHz 無線でのみ使用できます。

例

ap1 と名付けた AP の無線 1 に対してスペクトル管理を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] spectrum-management enable

apgroup1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対してスペクトル管理を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] spectrum-management enable

14.1.58 tolerance-level

Syntax

tolerance-level *percent*

undo tolerance-level

デフォルト

RRM view：AP group view の設定を使用します。

AP group RRM view：20%(ソフトウェアバージョン 7.2.21 を含む以前)

1%(ソフトウェアバージョン 7.2.27 を含む以降)

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

percent: 許容レベルを範囲で指定します。

ソフトウェアバージョン 7.2.18 を含む以前のソフトウェアでの設定範囲は 1～45%です。

ソフトウェアバージョン 7.2.21 のソフトウェアでの設定範囲は 0~45%です。

ソフトウェアバージョン 7.2.27 を含む以降のソフトウェアでの設定範囲は 0~100%です。説明

tolerance-level コマンドは許容レベルを設定します。

undo t**olerance-level** コマンドはデフォルトに戻します。

現在のチャネルが CRC エラーしきい値、干渉しきい値、または再伝送しきい値に達する場合、AC は最適なチャネルを選択します。最適なチャネルと現在のチャネル間の品質ギャップが許容レベルを超えるまで、AC は無線に最適なチャネルを適用しません。

例

ap1 と名付けた AP の無線 1 に対して許容レベルを 25%で設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] tolerance-level 25

group1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して許容レベルを 25%で設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] tolerance-level 25

14.1.59 wlan calibrate-channel pronto ap all

Syntax

ソフトウェアバージョン 7.2.75 を含む以降のソフトウェア

wlan calibrate-channel pronto ap { **all** | **ap-group** *group-name* } { **2.4g** | **5g** | **6g** | **all** }

🕮 **メモ：**

6GHz 無線のサポートは AP の機種により異なります。

ソフトウェアバージョン 7.2.63 を含む以降のソフトウェア

wlan calibrate-channel pronto ap { **all** | **ap-group** *group-name* } { **2.4g** | **5g** | **all** }

ソフトウェアバージョン 7.2.59 を含む以前のソフトウェア

wlan calibrate-channel pronto ap all

View

System view

定義済みユーザロール

network-admin

パラメータ

ソフトウェアバージョン 7.2.75 を含む以降のソフトウェア

ap all: 全ての AP を指定します。

ap-group *group-name*: 大文字と小文字を区別しない 1~31 文字で AP グループ名を指定します。

2.4g: 2.4GHz 無線を指定します。

5g: 5GHz 無線を指定します。

6g: 6GHz 無線を指定します。

all: 2.4GHz 無線と 5GHz 無線と 6GHz 無線のすべてを指定します。

ソフトウェアバージョン 7.2.63 を含む以降のソフトウェア

ap all: 全ての AP を指定します。

ap-group *group-name*: 大文字と小文字を区別しない 1~31 文字で AP グループ名を指定します。

2.4g: 2.4GHz 無線を指定します。

5g: 5GHz 無線を指定します。

all: 2.4GHz 無線と 5GHz 無線の両方を指定します。

ソフトウェアバージョン 7.2.59 を含む以前のソフトウェア

指定できるパラメータはありません。

説明

⚠ **注意：**

このコマンドはシステム資源を消費します。注意して使用してください。

ソフトウェアバージョン 7.2.63 を含む以降のソフトウェア

wlan calibrate-channel pronto ap コマンドはすべての AP、もしくは指定した AP グループ AP の無線に対して on-demand DFS を実行します。

ソフトウェアバージョン 7.2.59 を含む以前のソフトウェア

wlan calibrate-channel pronto ap all コマンドはすべての AP の無線に対して on-demand DFS を実行します。

例

ソフトウェアバージョン 7.2.63 を含む以降のソフトウェア

すべての AP のすべての無線に対して on-demand DFS を実行します。

<AC> system-view

[AC] wlan calibrate-channel pronto ap all all

すべての AP の無線に対して on-demand DFS を実行します。

<AC> system-view

[AC] wlan calibrate-channel pronto ap all

14.1.60 wlan calibrate-power pronto ap all

Syntax

wlan calibrate-power pronto ap all

View

System view

定義済みユーザロール

network-admin

説明

⚠ **注意：**

このコマンドはシステム資源を消費します。注意して使用してください。

wlan calibrate-power pronto ap all コマンドはすべての AP の無線に対して on-demand TPC を実行します。

例

すべての AP の無線に対して on-demand TPC を実行します。

<AC> system-view

[AC] wlan calibrate-power pronto ap all

14.1.61 wlan rrm baseline apply

Syntax

wlan rrm baseline apply name *baseline-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

name *baseline-name*: ベースライン名を大文字と小文字を区別しない 1～32 文字の文字列で指定します。

説明

wlan rrm baseline apply コマンドは無線ベースラインを適用します。

次のいずれかの条件を満たす場合、無線ベースラインを適用することはできません。

1) 無線ベースラインのロケーション識別子を使用して無線を管理する権利が無い。
2) 無線ベースラインの名前が start_config_baseline.csv。

例

無線ベースラインを適用する。

<AC> system-view

[AC] wlan rrm baseline apply name bl

関連コマンド

- **display wlan rrm baseline apply-result**
- **wlan rrm baseline save**

14.1.62 wlan rrm baseline remove

Syntax

wlan rrm baseline remove name *baseline-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

name baseline-name: ベースライン名を大文字と小文字を区別しない 1～32 文字の文字列で指定します。

説明

wlan rrm baseline remove コマンドは無線ベースラインを削除します。

無線ベースラインのロケーション識別子を使用して無線を管理する権利がない場合、無線ベースラインを適用することはできません。

例

無線ベースラインを削除する。

<AC> system-view

[AC] wlan rrm baseline remove name bl

関連コマンド

wlan rrm baseline save

14.1.63 wlan rrm baseline save

Syntax

wlan rrm baseline save name *baseline-name* { **ap** *ap-name* **radio** *radio-id* | **ap-group** *group-name* **ap-model** *ap-model* **radio** *radio-id* | **global** }

View

System view

定義済みユーザロール

network-admin

パラメータ

name *baseline-name*: ベースライン名を大文字と小文字を区別しない 1～32 文字の文字列で指定します。

ap *ap-name*: AP 名を指定します。AP がオンラインであることを確認します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

radio *radio-id*: 無線 ID を指定します。

ap-group *group-name*: AP グループ名を 1～31 文字の大文字と小文字を区別しない文字で指定します。AP グループが既に存在することを確認してください。

ap-model *ap-model*: AP モデルを指定します。

global: すべての無線を指定します。

説明

wlan rrm baseline save コマンドは現在の無線設定を保存して無線ベースラインを作成します。

無線ベースラインは、無線または複数の無線の現用チャネル、送信レート、および他の無線属性を保存します。現在の無線設定を保存して無線ベースラインを作成し、ベースラインを適用してこれらの設定を使用することができます。

無線ベースラインは、AC 上のファイルシステム内の.csv ファイルに保存されます。

例

AP **ap1** の無線 1 に対して設定を保存し、無線ベースライン **ap1-1** を作成します。

<AC> system-view

[AC] wlan rrm baseline save name ap1-1 ap ap1 radio 1

AP グループ **group1** のモデル **QX-W1020** の AP の無線 1 に対して設定を保存し、無線ベースライン **ap1g1-1** を作成します。

<AC> system-view

[AC] wlan rrm baseline save name ap1g1-1 ap-group group1 ap-model QX-W1020 radio 1

すべての無線の設定を保存し、**global** な無線ベースラインを作成します。

<AC> system-view

[AC] wlan rrm baseline save name global global

14.1.64 wlan rrm calibration-bandwidth interval

🕮 **メモ**：

このコマンドはソフトウェアバージョン 7.2.55 を含む以降のソフトウェアからサポートしています。

Syntax

wlan rrm calibration-bandwidth interval *minutes*

undo wlan rrm calibration-bandwidth interval

デフォルト

13 分

View

System view

定義済みユーザロール

network-admin

パラメータ

minutes: 帯域幅自動調整間隔を 3～1440 分の範囲で指定します。

説明

wlan rrm calibration-bandwidth interval コマンドは帯域幅自動調整間隔を設定します。

undo wlan rrm calibration-bandwidth interval コマンドはデフォルトに戻します。

例

帯域幅自動調整間隔を 10 分に設定します。

<AC> system-view

[AC] wlan rrm calibration-bandwidth interval 10

関連コマンド

calibrate-bandwidth self-decisive

14.1.65 wlan rrm calibration-channel interval

Syntax

wlan rrm calibration-channel interval *minutes*

undo wlan rrm calibration-channel interval

デフォルト

ソフトウェアバージョンにより異なります。

ソフトウェアバージョン 7.2.21 を含む以前のソフトウェアでは 8 分です。

ソフトウェアバージョン 7.2.27 を含む以降のソフトウェアでは 23 分です。

View

System view

定義済みユーザロール

network-admin

パラメータ

minutes: チャネルキャリブレーション間隔を 3～1440 分の範囲で指定します。

説明

wlan rrm calibration-channel interval コマンドはチャネルキャリブレーション間隔を設定します。

undo wlan rrm calibration-channel interval コマンドはデフォルトに戻します。

例

チャネルキャリブレーション間隔を 10 分に設定します。

<AC> system-view

[AC] wlan rrm calibration-channel interval 10

関連コマンド

calibrate-channel self-decisive

14.1.66 wlan rrm-calibration-group

Syntax

wlan rrm-calibration-group *group-id*

undo wlan rrm-calibration-group { **all** | *group-id* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

all: すべての RRM holddown group を指定します。

group-id: RRM holddown group ID を 1~128 の範囲で指定します。

説明

wlan rrm-calibration-group コマンドは新規に RRM holddown group を作成、または既存の RRM holddown group の view を入力して、その view に移行します。

undo wlan rrm-calibration-group コマンドは RRM holddown group を取り除きます。

例

RRM holddown group 10 を作成します。

<AC> system-view

[AC] wlan rrm-calibration-group 10

[AC-wlan-rrm-calibration-group-10]

14.1.67 wlan rrm calibration-power interval

Syntax

wlan rrm calibration-power interval *minutes*

undo wlan rrm calibration-power interval

デフォルト

8 分

View

System view

定義済みユーザロール

network-admin

パラメータ

minutes: パワーキャリブレーション間隔を 3~180 分の間隔で指定します。

説明

wlan rrm calibration-power interval コマンドはパワーキャリブレーション間隔を設定します。

undo wlan rrm calibration-power interval コマンドはデフォルトに戻します。

例

パワーキャリブレーション間隔を 10 分で設定します。

<AC> system-view

[AC] wlan rrm calibration-power interval 10

関連コマンド

calibrate-power self-decisive

目次

このセクションのページは **2-x-x** です。

15 章 WLAN IP スヌーピング 15-1
15.1 WLAN IP スヌーピングコマンド 15-1
15.1.1 client ipv4-snooping arp-learning enable 15-1
15.1.2 wlan client ip-conflict-detection enable 15-2

15章 WLAN IP スヌーピング

15.1 WLAN IPスヌーピングコマンド

15.1.1 client ipv4-snooping arp-learning enable

Syntax

client ipv4-snooping arp-learning enable

undo client ipv4-snooping arp-learning enable

デフォルト

有効

View

Service template view

定義済みユーザロール

network-admin

説明

client ipv4-snooping arp-learning enable コマンドは ARP パケットのスヌーピングを有効にします。

undo client ipv4-snooping arp-learning enable コマンドは ARP パケットのスヌーピングを無効にします。

このコマンドを実行する前に、サービステンプレートが無効になっていることを確認してください。

例

ARP パケットのスヌーピングを無効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] undo client ipv4-snooping arp-learning enable

15.1.2 wlan client ip-conflict-detection enable

🕮 メモ：

undo wlan client ip-conflict-detection enable 実行時に IP アドレス競合検出された IP アドレスがある場合は、そのクライアントのキャッシュ情報がクリアされるまで、その IP アドレスの競合検出は行いません。クライアントのキャッシュ情報の保持時間は、client cache aging-time コマンドで設定した時間（初期値は 180 秒）です。

Syntax

wlan client ip-conflict-detection enable

undo wlan client ip-conflict-detection enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

wlan client ip-conflict-detection enable コマンドは、IP アドレス競合検出機能を有効にします。

undo wlan client ip-conflict-detection enable コマンドは、IP アドレス競合検出機能を無効にします。

この機能により、システムはオンライン要求したクライアントと既にオンライン中のクライアントの間で IP アドレスの競合を検出することができます。システムはオンライン要求したクライアントと同じ IP アドレスを使用しているオンライン中のクライアントをログオフし、そのクライアント用に IP アドレス競合のエントリを作成します。クライアントのキャッシュが期限切れになるか、クライアントの IP アドレスが変更されると、システムはそのクライアントの IP アドレス競合エントリを削除します。

例

IP アドレス競合検出を無効にします。

<AC> system-view

[AC] undo wlan client ip-conflict enable

関連コマンド

client cache aging-time

目次

このセクションのページは **2-x-x** です。

16 章 WLAN 最適化 16-1
16.1 WLAN 最適化コマンド 16-1
16.1.1 option broadcast-multicast-buffer 16-1
16.1.2 option client hide-node-protection 16-2
16.1.3 option client reconnect 16-3
16.1.4 option keep-active 16-5
16.1.5 rrop anti-bmc network 16-6
16.1.6 rrop anti-bmc rate-limit 16-8
16.1.7 rrop anti-bmc rate-limit pps 16-9
16.1.8 rrop anti-bmc upstream client-rate-limit 16-10
16.1.9 rrop anti-bmc upstream client-rate-limit pps 16-12
16.1.10 rrop arp ap-proxy-gateway enable 16-13
16.1.11 rrop client fast-keep-alive 16-14
16.1.12 rrop flow-schedule mode 16-15
16.1.13 rrop software-retry 16-17
16.1.14 sacp roam-optimize packet-loss-improve enable 16-18

16章 WLAN 最適化

16.1 WLAN最適化コマンド

16.1.1 option broadcast-multicast-buffer

Syntax

option broadcast-multicast-buffer { **disable** | **enable** [**limit** *limit*] }

undo option broadcast-multicast-buffer

デフォルト

Radio view: AP group radio view の設定を使用します。

AP group radio view: 有効

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

limit *limit*: マルチキャストパケットもしくはブロードキャストパケットをバッファできる最大数を指定します。値の範囲は 1～600 です。デフォルトの値は 100 です。

disable: マルチキャストとブロードキャストのバッファを無効にします。

enable: マルチキャストとブロードキャストのバッファを有効にします。

説明

option broadcast-multicast-buffer enable コマンドはマルチキャストとブロードキャストのバッファを有効にします。

option broadcast-multicast-buffer disable コマンドはマルチキャストとブロードキャストのバッファを無効にします。

undo option broadcast-multicast-buffer コマンドはデフォルトに戻します。

この機能を有効にすると、関連付いたクライアントがスリープモードになった場合、ACはブロードキャストパケットとマルチキャストパケットの送信を停止し、これらのパケットをバッファします。

この機能を無効にすると、関連付いたクライアントがスリープモードであるかどうかにかかわらず、AC はすべてのブロードキャストパケットとマルチキャストパケットをクライアントに直接送信します。

limit の引数の値をデフォルトで使用する場合、**limit** *limit* を指定せずに **option broadcast-multicast-buffer enable** コマンドを設定してください。

例

ap1 でマルチキャストとブロードキャストのバッファを無効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] option broadcast-multicast-buffer disable

AP group 1 の **QX-W1020** でマルチキャストとブロードキャストのバッファを無効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] option broadcast-multicast-buffer disable

16.1.2 option client hide-node-protection

Syntax

option client hide-node-protection { **disable** | **enable** }

undo option client hide-node-protection

デフォルト

Radio view: AP group radio view の設定を使用します。

AP group radio view: 無効

View

Radio view

AP group の radio view

定義済みユーザロール

network-admin

パラメータ

disable: 隠れ端末保護を無効にします。

enable: 隠れ端末保護を有効にします。

説明

option client hide-node-protection enable コマンドは隠れ端末保護を有効にします。

option client hide-node-protection disable コマンドは隠れ端末保護を無効にします。

undo option client hide-node-protection コマンドはデフォルトに戻します。

このコマンドは、802.11g、802.11n、802.11ac、802.11ax クライアントにのみ適用可能です。

この機能を有効にすると、クライアントは隠れ端末からの干渉を避けるために RTS/CTS フレームを送信します。

本機能によって複数端末の通信衝突を軽減させることが可能です。

Radio view での設定は、AP group radio view での設定より優先されます。

例

AP**ap1** に対して隠れ端末保護を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] option client hide-node-protection enable

AP group 1 の **QX-W1020** に対して隠れ端末保護を有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] option client hide-node-protection enable

16.1.3 option client reconnect

Syntax

option client reconnect { **disable** | **enable** [**rssi** *rssi-value*] [**interval** *interval*] }

undo option client reconnect

デフォルト

Radio view: AP group view の設定を使用します。

AP group radio view: 無効

View

Radio view

AP group の radio view

定義済みユーザロール

network-admin

パラメータ

rssi *rssi-value*: RSSI しきい値を 5～100 の範囲で指定します。RSSI しきい値のデフォルト値および推奨値は、それぞれ 10 と 20 です。

interval *interval*: AP がクライアントの信号強度を検出する間隔を 3～10 秒の範囲で指定します。デフォルト設定は 3 秒です。

disable: AP トリガのクライアント再関連付けを無効にします。

enable: AP トリガのクライアント再関連付けを有効にします。

説明

option client reconnect enable コマンドは AP トリガのクライアント再関連付けを有効にします。

option client reconnect disable コマンドは AP トリガのクライアント再関連付けを無効にします。

undo option client reconnect コマンドはデフォルトに戻します。

この機能により、クライアントの信号強度が指定した RSSI しきい値よりも小さいと AP が検知したとき、AP は再認証フレームをクライアントに送信できます。再認証フレームを受信したクライアントは、AP に再関連付け、あるいは別の AP にローミングできます。

Radio view での設定は、AP group radio view での設定より優先されます。

例

#AP トリガのクライアント再関連付けを **ap1** で有効にします。RSSI しきい値を 30、検出間隔を 5 秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] option client reconnect enable rssi 30 interval 5

#AP トリガのクライアント再関連付けを AP **ap1** で有効にします。RSSI しきい値を 30、検出間隔を 5 秒に設定します。

AP トリガのクライアント再関連付けを AP group 1 の **QX-W1020** で有効にします。RSSI しきい値を 30、検出間隔を 5 秒に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] option client reconnect enable rssi 30 interval 5

16.1.4 option keep-active

Syntax

option keep-active { disable | enable }

undo option keep-active

デフォルト

Radio view : : AP グループの設定を引き継ぎます。

AP group の radio view：無効

View

Radio view

AP group の radio view

定義済みユーザロール

network-admin

説明

option keep-active enable コマンドは無線クライアントのスリープ時間を短縮する機能を有効にします。

option keep-active disable コマンドは、無線クライアントのスリープ時間を短縮する機能を無効にします。

undo option keep-active コマンドはデフォルトに戻します。

スリープ状態の無線クライアントは、ビーコンフレーム内の TIM（トラフィック通知メッセージ）情報を定期的にリスニングすることで、接続している AP が無線クライアントのパケットをバッファしているかどうかを判断します。AP が無線クライアントのパケットをバッファしている場合、スリープ状態は終了し、AP とデータ通信を行います。本機能を有効にすると、AP はビーコンフレーム内の TIM を変更し、端末のスリープ時間を短縮して、伝送効率を向上させます。

例

ap1 で無線クライアントのスリープ時間短縮機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] option keep-active enable

apgroup1 でクライアントのスリープ時間短縮機能を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] option keep-active enable

16.1.5 rrop anti-bmc network

🕮 **メモ：**

- **rrop anti-bmc network** コマンドはソフトウェアバージョン 7.2.46 を含む以降のソフトウェアからサポートしています。
- **rrop anti-bmc network** コマンドの System view への設定はソフトウェアバージョン 7.2.85a を含む以降のソフトウェアからサポートしています。
- **ipv4-and-ipv6-simple enable** のパラメータはソフトウェアバージョン 7.2.85a を含む以降のソフトウェアからサポートしています。

Syntax

rrop anti-bmc network { disable | ipv4-simple enable | ipv4-and-ipv6-simple enable }

undo rrop anti-bmc network

デフォルト

AP view：AP group view の設定を使用します。

AP group view：ソフトウェアバージョンにより異なります。

ソフトウェアバージョン V7.2.50 を含む以前のソフトウェアでは有効です。

ソフトウェアバージョン V7.2.52 を含む以降のソフトウェアでは無効です。

ソフトウェアバージョン V7.2.85a を含む以降のソフトウェアでは System view の設定を使用します。

System view：ソフトウェアバージョンにより異なります。

ソフトウェアバージョン V7.2.85a のソフトウェアでは有効(**ipv4-and-ipv6-simple enable**)です。

ソフトウェアバージョン V7.2.89 を含む以降のソフトウェアでは無効です。

View

AP view

AP group view

System View

定義済みユーザロール

network-admin

パラメータ

disable: ブロードキャストパケットおよびマルチキャストパケットの制御を無効にします

ipv4-simple enable: IPv4 ネットワークでブロードキャストパケットおよびマルチキャストパケットの制御を有効にします

ipv4-and-ipv6-simple enable: IPv4 と IPv6 ネットワークでブロードキャストパケットおよびマルチキャストパケットの制御を有効にします。

説明

rrop anti-bmc network disable コマンドはブロードキャストパケットおよびマルチキャストパケットの制御を無効にします。

rrop anti-bmc network ipv4-simple enable コマンドはブロードキャストパケットおよびマルチキャストパケットの制御を有効にします。

undo rrop anti-bmc network コマンドはデフォルトに戻します。

- IPv4 ネットワークで基本的なブロードキャストおよびマルチキャストパケットを制御します。AP は ARP ブロードキャストパケットに応答し、DHCP ブロードキャストパケットを廃棄し、他のパケットを正常に処理します。
- IPv6 ネットワークで基本的なブロードキャストおよびマルチキャストパケット制御を制御します。AP は RS および DHCPv 6 ブロードキャストパケットを廃棄し、RA パケットをユニキャストで転送、NS パケットに応答し、その他のパケットを正常に処理します。

例

#ブロードキャストパケットおよびマルチキャストパケットの制御を ap1 で有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] rrop anti-bmc network ipv4-simple enable

#マルチキャストパケットのレート制限を AP group 1 で有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rrop anti-bmc network ipv4-simple enable

16.1.6 rrop anti-bmc rate-limit

🕮 **メモ：**

- rrop anti-bmc rate-limit コマンドはソフトウェアバージョン 7.2.50 を含む以降のソフトウェアからサポートしています。

Syntax

rrop anti-bmc { broadcast | multicast } rate-limit { disable | enable }

undo rrop anti-bmc { broadcast | multicast } rate-limit

デフォルト

AP view：AP group view の設定を使用します。

AP group view：無効

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

broadcast: ブロードキャストパケットのレート制限を設定します

multicast: マルチキャストパケットのレート制限を設定します

説明

rrop anti-bmc rate-limit enable コマンドはブロードキャストまたはマルチキャストパケットのレート制限を有効にします。

rrop anti-bmc rate-limit disable コマンドはブロードキャストまたはマルチキャストパケットのレート制限を無効にします。

undo rrop anti-bmc rate-limit コマンドはデフォルトに戻します。

例

#ブロードキャストパケットのレート制限を ap1 で有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] rrop anti-bmc broadcast rate-limit enable

#マルチキャストパケットのレート制限を AP group 1 で有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rrop anti-bmc multicast rate-limit enable

16.1.7 rrop anti-bmc rate-limit pps

🕮 **メモ：**

- rrop anti-bmc rate-limit pps コマンドはソフトウェアバージョン 7.2.50 を含む以降のソフトウェアからサポートしています。

Syntax

rrop anti-bmc { broadcast | multicast } rate-limit pps *max-pps*

undo rrop anti-bmc { broadcast | multicast } rate-limit pps

デフォルト

AP view：AP group view の設定を使用します。

AP group view：AP が 1 秒あたりに送信できるブロードキャストまたはマルチキャストパケットの最大数は指定されていません。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

broadcast: 1 秒間に送信可能なブロードキャストパケットの最大数を設定します

multicast: 1 秒間に送信可能なブロードキャストパケットの最大数を設定します

max-pps: AP が 1 秒あたりに送信できるブロードキャストまたはマルチキャストパケットの最大数を 1～1410000 の範囲で指定します。AP は、指定された制限を超えるブロードキャストまたはマルチキャストパケットを破棄します。

説明

rrop anti-bmc rate-limit pps コマンドはブロードキャストまたはマルチキャストパケットの 1 秒間に送信できる最大数を設定します。

undo rrop anti-bmc rate-limit pps コマンドはデフォルトに戻します。

このコマンドは、rrop **anti-bmc rate-limit enable** が設定されている場合のみ有効です。

例

ap1 でブロードキャストパケットを 1 秒間に最大 200 個に制限します

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] rrop anti-bmc broadcast rate-limit pps 200

#AP group 1 でマルチキャストパケットを 1 秒間に最大 200 個に制限します

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rrop anti-bmc multicast rate-limit pps 200

16.1.8 rrop anti-bmc upstream client-rate-limit

🕮 **メモ：**

- **rrop anti-bmc upstream client-rate-limit** コマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。
- **disable** パラメータは System view では指定できません。

Syntax

rrop anti-bmc { broadcast | multicast } upstream client-rate-limit enable

rrop anti-bmc { broadcast | multicast } upstream client-rate-limit disable

undo rrop anti-bmc { broadcast | multicast } upstream client-rate-limit

デフォルト

AP view：AP group view の設定を使用します。AP group view に設定がない場合、AP は System view の設定を使用します。

AP group view：System view の設定を使用します。

System view：無効

View

AP view

AP group view

System view

定義済みユーザロール

network-admin

パラメータ

broadcast: アップリンクのブロードキャストパケットのレートを制限します。

multicast: アップリンクのマルチキャストパケットのレートを制限します。

説明

rrop anti-bmc { broadcast | multicast } upstream client-rate-limit enable コマンドはアップリンクのブロードキャストまたはマルチキャストパケットのレート制限を有効にします。

rrop anti-bmc { broadcast | multicast } upstream client-rate-limit disable コマンドはアップリンクのブロードキャストまたはマルチキャストパケットのレート制限を無効にします。

undo rrop anti-bmc { broadcast | multicast } upstream client-rate-limit コマンドはデフォルトに戻します。

このコマンドは、制限するレートの値を指定した場合にのみ有効です。

例

System view でアップリンクのブロードキャストパケットのレートを制限します。

<AC> system-view

[AC] rrop anti-bmc broadcast upstream client-rate-limit enable

#AP group 1 でアップリンクのブロードキャストパケットのレートを制限します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rrop anti-bmc broadcast upstream client-rate-limit enable

16.1.9 rrop anti-bmc upstream client-rate-limit pps

🕮 **メモ：**

- **rrop anti-bmc upstream client-rate-limit pps** コマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

rrop anti-bmc { broadcast | multicast } upstream client-rate-limit pps *max-pps*

undo rrop anti-bmc { broadcast | multicast } upstream client-rate-limit pps

デフォルト

AP view：AP group view の設定を使用します。AP group view に設定がない場合、AP は System view の設定を使用します。

AP group view：System view の設定を使用します。

System view：AP が各クライアントからブロードキャストもしくはマルチキャストパケットを受信するレートに制限はありません。

View

AP view

AP group view

System view

定義済みユーザロール

network-admin

パラメータ

broadcast: ブロードキャストパケットのレートを制限します。

multicast: マルチキャストパケットのレートを制限します。

pps *max-pps*: AP が各クライアントから 1 秒あたりに受信できるブロードキャストまたはマルチキャストパケットの最大数を 1～1410000 の範囲で指定します。AP は、指定された制限を超えるブロードキャストまたはマルチキャストパケットを破棄します。

説明

rrop anti-bmc upstream client-rate-limit pps コマンドは AP が各クライアントからブロードキャストまたはマルチキャストパケットを受信するレートの最大数を設定します。

undo rrop anti-bmc upstream client-rate-limit pps コマンドはデフォルトに戻します。

例

#AP が各クライアントから 1 秒あたりに受信できるブロードキャストパケットの最大数を System view で 1024 に制限します

<AC> system-view

[AC] rrop anti-bmc broadcast upstream client-rate-limit pps 1024

16.1.10 rrop arp ap-proxy-gateway enable

🕮 **メモ：**

rrop arp ap-proxy-gateway enable コマンドはソフトウェアバージョン 7.2.85a を含む以降のソフトウェアからサポートしています。

Syntax

rrop arp ap-proxy-gateway enable [count *count* **]**

undo rrop arp ap-proxy-gateway enable

デフォルト

ソフトウェアバージョンにより異なります。

ソフトウェアバージョン 7.2.85a では有効です。

ソフトウェアバージョン 7.2.89 を含む以降のソフトウェアでは無効です。

View

System View

定義済みユーザロール

network-admin

パラメータ

count *count*: AP がゲートウェイに代わって応答期間中に応答できる ARP 要求の最大数を 1 から 4096 の範囲で設定します。デフォルト値は 10 です。

説明

rrop arp ap-proxy-gateway enable コマンドは AP がゲートウェイに代わってクライアントの ARP 要求に応答できるようにします。

undo arp ap-proxy-gateway enable コマンドはデフォルトに戻します。

この機能を有効にすると、AP はゲートウェイに代わってクライアントの ARP 要求に応答します。

応答期間中にゲートウェイの MAC アドレスが変更されると、ARP が失敗する可能性があります。応答期間中に AP がゲートウェイに代わって応答できる ARP 要求の数を制限することでこの問題を解決します。

AP が応答した ARP 要求数が制限に達すると、AP は ARP 要求をゲートウェイに転送し、下記のいずれかの処理を実行します。

- ゲートウェイが ARP 要求に応答した場合、AP は新しいゲートウェイの MAC アドレスで新しい応答期間を開始します。
- ゲートウェイが ARP 要求に応答しなかった場合、AP は元のゲートウェイの MAC アドレスで新しい応答期間を開始します。

例

AP がゲートウェイに代わってクライアントの ARP 要求に応答できるようにします。

<AC> system-view

[AC] rrop arp ap-proxy-gateway enable

16.1.11 rrop client fast-keep-alive

🕮 **メモ：**

rrop client fast-keep-alive コマンドはソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。ソフトウェアバージョン 7.2.63 以前は本機能がデフォルトのパラメータ値で動作しており、無効にすることはできません。

Syntax

rrop client fast-keep-alive { **disable** | **enable** [**count** *count-value*] [**interval** *interval-value*]

undo rrop client fast-keep-alive

デフォルト

有効

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

count *count-value*: キープアライブカウントを 128~2048 の範囲で指定します。デフォルト値は 1024 です。

interval *interval-value*: キープアライブ間隔を 3~60 秒の範囲で指定します。デフォルト値は 10 です。

説明

rrop client fast-keep-alive enable コマンドはクライアント高速キープアライブを有効にします。

rrop client fast-keep-alive disable コマンドはクライアント高速キープアライブを無効にします。

undo rrop client fast-keep-alive コマンドはデフォルトに戻します。

この機能により、AP は、クライアントに送信されたユニキャストパケットの確認応答状態に基づいて、クライアントがまだオンラインであるかどうかを確認できます。AP はユーザーデータを 3 つのグループに分けて個別にカウントします。キープアライブ間隔 (*interval-value* パラメータで設定) 中に、3 グループのユニキャストパケットの確認応答が受信されなかった場合、AP はクライアントがオフラインであると判断し、クライアントへの接続を終了します。これにより、無線リソースの使用率が向上します。グループ内のユニキャストパケットの数は、*count-value* パラメータで設定します。

この機能は、クライアントの移動性が高いシナリオに適用できます。ネットワーク品質が悪い場合は、キープアライブカウントを減らすか、キープアライブ間隔を短くしてください。

例

#AP グループ 1 の QX-W1120 の Radio1 のクライアントの高速キープアライブを有効にし、キープアライブ数を 300 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1120

[AC-wlan-ap-group-1-ap-model-QX-W1120] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1120-radio-1] rrop client fast-keep-alive 300

16.1.12 rrop flow-schedule mode

🕮 **メモ**:

- **rrop flow-schedule mode** コマンドはソフトウェアバージョン 7.2.89 を含む以降のソフトウェアからサポートしています。
- この機能と、クライアントのレート制限機能が同時に設定されている場合、**client-rate-limit** コマンドを使用して設定された無線クライアントレート制限が有効になります。

Syntax

rrop flow-schedule mode { **balanced** | **quick-speed** | **intelligent** [**channel-usage-threshold** *threshold-value* | **max** *max-value* | **min** *min-value*] }

undo rrop flow-schedule mode

デフォルト

Radio view: AP group radio view の設定を使用します。

AP group radio view: **quick-speed** モード

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

Balanced： バランスモードを指定します。このモードでは、AC はクライアントに帯域幅を均等に割り当てます。

quick-speed : quick-speed モードを指定します。このモードでは、クライアントが自分のトラフィックに基づいて帯域幅を競います。

Intelligent : インテリジェントモードを指定します。このモードでは、AC はクライアントに帯域幅を均等に割り当て、アイドリングクライアントの余剰帯域幅を大きなトラフィックのクライアントにアルゴリズム計算に基づいて再割り当てできます。

channel-usage-threshold *threshold-value* **:**インテリジェントスケジューリングのしきい値を 1 から 99 の範囲で指定します。チャネル使用率が設定されたしきい値以上になると、インテリジェントスケジューリングモードが自動的に有効になります。

チャネル使用率がしきい値を下回ると、インテリジェントスケジューリングモードが自動的に無効になります。インテリジェントスケジューリングしきい値を指定しない場合、インテリジェントスケジューリングモードは常に有効になります。

max *max-value* **:** 最大クライアント速度を 16 から 1700000Kbps の範囲で指定します。

min *min-value* **:** 最小クライアント速度を 16 から 1700000Kbps の範囲で指定します。最大クライアント速度は最小クライアント速度より高い値を設定します。

説明

rrop flow-schedule mode コマンドは AP のトラフィックスケジューリングモードを設定します。

undo rrop flow-schedule mode コマンドはデフォルトに戻します。

例

#AP ap1 の radio 1 のトラフィックスケジューリングモードをインテリジェントモードに設定します。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1240

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrop flow-schedule mode Intelligent

#AP グループ 1 の QX-W1240 の Radio1 のトラフィックスケジューリングモードを quick-speed モードに設定します。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1240

[AC-wlan-ap-group-1-ap-model-QX-W1240] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1240-radio-1] rrop flow-schedule mode quick-speed

16.1.13 rrop software-retry

Syntax

rrop software-retry enable { **unicast** [**eap**] | **broadcast-multicast** } **count** *count*

rrop software-retry disable { **unicast** [**eap**] | **broadcast-multicast** }

undo rrop software-retry { **unicast** [**eap**] | **broadcast-multicast** }

デフォルト

Radio view: AP group radio view の設定を使用します。

AP group radio view: ソフトウェア再転送の最大数は装置のモデルにより異なります。

View

Radio view

AP group の radio view

定義済みユーザロール

network-admin

パラメータ

unicast: ユニキャストパケットに対してソフトウェア再転送を設定します。

eap: EAP パケットに対してソフトウェア再転送を設定します。

broadcast-multicast: ブロードキャストパケットとマルチキャストパケットに対してソフトウェア再転送を設定します。

count *count*: ソフトウェア再転送の最大数を指定します。

disable: ソフトウェア再転送を無効にします。

enable: ソフトウェア再転送を有効にします。

説明

rrop software-retry enable コマンドはソフトウェア再転送を有効にします。

rrop software-retry disable コマンドはソフトウェア再転送を無効にします。

undo rrop software-retry コマンドはデフォルトに戻します。

例

ap1 の radio1 で、EAP パケットに対してソフトウェア再転送の最大数をデフォルトで設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] undo rrop software-retry unicast eap

AP group 1 の **QX-W1020** で EAP パケットに対してソフトウェア再転送の最大数をデフォルトで設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] undo rrop software-retry unicast eap

16.1.14 sacp roam-optimize packet-loss-improve enable

🕮 **メモ**:

- **sacp roam-optimize packet-loss-improve enable** コマンドはソフトウェアバージョン 7.2.82 を含む以降のソフトウェアからサポートしています。
- ソフトウェアバージョン 7.2.82 および 7.2.82b のソフトウェアでは、中央転送モードの SSID での利用のみをサポートしています。
- ソフトウェアバージョン 7.2.85a を含む以降のソフトウェアでは、ローカル転送モードの SSID での利用をサポートしています。

Syntax

sacp roam-optimize packet-loss-improve enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

sacp roam-optimize packet-loss-improve enable コマンドはクライアントローミング中のパケットロス最適化を有効にします。

undo sacp roam-optimize packet-loss-improve enable コマンドはデフォルトに戻します。

クライアントが AC 内ローミングした際に発生する転送エントリの切り替えが原因でパケットロスが発生する可能性があります。この機能を有効にすると、クライアントが BTM によってローミングを指示された際、AC は事前にローミング先の AP の BSS にクライアント情報を作成し、転送エントリをターゲット AP に切り替えてクライアントのトラフィックをキャッシュします。クライアントがローミングを完了すると、ターゲット AP はキャッシュされたトラフィックを直ちにクライアントに送信することにより、ローミング中のパケットロスを軽減します。

例

サービステンプレート **service1** で、クライアントローミング中のパケットロス最適化を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] sacp roam-optimize packet-loss-improve enable

目次

このセクションのページは **2-x-x** です。

17 章 WLAN 無線ロードバランス 17-1
17.1.1 radio-load-balance band-navigation association-reject 17-1
17.1.2 radio-load-balance band-navigation enable 17-2
17.1.3 radio-load-balance band-navigation rssi 17-3
17.1.4 wlan radio-load-balance overload-5g ssid-hide 17-5

17章 WLAN 無線ロードバランス

17.1.1 radio-load-balance band-navigation association-reject

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.79 を含む以降のソフトウェアからサポートしています。

Syntax

radio-load-balance band-navigation association-reject [**6g-capability** *6g-count*] **5g-capability** *5g-count* **unknown-capability** *unknown-count*

undo radio-load-balance band-navigation association-reject

デフォルト

AP view では、AP は AP group view の設定を使用します。

AP group view では、無効です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

6g-capability *6g-count*: 6GHz 対応の 802.11v 以外のクライアントのアソシエーション拒否数を指定します。値の範囲は 1~5 で、デフォルト値は 1 です。

5g-capability *5g-count*: 5GHz 対応の 802.11v 以外のクライアントのアソシエーション拒否数を指定します。値の範囲は 1~5 で、デフォルト値は 1 です。

unknown-capability *unknown-count*: 6GHz、5GHz 対応か不明な 802.11v 以外のクライアントのアソシエーション拒否数を指定します。

値の範囲はソフトウェアバージョンにより異なります。

ソフトウェアバージョン 7.2.82b を含む以前のソフトウェアでは、値の範囲は 1~5 で、デフォルト値は 1 です。

ソフトウェアバージョン 7.2.85a を含む以降のソフトウェアでは、値の範囲は 0～5 で、デフォルト値は 1 です。

説明

radio-load-balance band-navigation association-reject コマンドは 802.11v 以外のクライアントのアソシエーション拒否を有効にし、最大拒否回数を設定します。

undo radio-load-balance band-navigation association-reject コマンドはデフォルトに戻します。

この機能を有効にすると、6GHz に対応した 802.11v 非対応のクライアントは、拒否回数が上限に達したときに 6GHz 以外の無線に接続できます。クライアントが接続した後、拒否カウンターはリセットされます。クライアントがオフラインになり、再び 6GHz 以外の無線に接続しようとした場合、再度拒否されます。

5GHz に対応した 802.11v 非対応のクライアントは、拒否回数が上限に達したときに 2.4GHz の無線に接続できます。クライアントが接続した後、拒否カウンターはリセットされます。クライアントがオフラインになり、再び 2.4GHz の無線に接続しようとした場合、再度拒否されます。

クライアントの拒否カウンターは 10 分間有効であり、最終拒否から 10 分後にリセットされます。

例

ap-group で、802.11v 以外のクライアントのアソシエーション拒否を有効にし、6GHz 対応クライアントの最大拒否回数を 3 回、5GHz 対応クライアントの最大拒否回数を 3 回、6GHz、5GHz 対応か不明なクライアントの最大拒否回数を 3 回に設定します。

<AC> system-view

[AC] wlan ap-group default-group

[AC] radio-load-balance band-navigation association-reject 6g-capability 3 5g-capability 3 unknown-capability 3

17.1.2 radio-load-balance band-navigation enable

🕮 **メモ：**

- このコマンドはソフトウェアバージョン 7.2.52 を含む以降のソフトウェアからサポートしています。

Syntax

radio-load-balance band-navigation { **disable** | **enable** }

undo radio-load-balance band-navigation

デフォルト

AP view では、AP は AP group view の設定を使用します。

AP group view では、有効です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: 無線ロードバランスでのバンドナビゲーション機能を無効にします

enable: 無線ロードバランスでのバンドナビゲーション機能を有効にします。

説明

radio-load-balance band-navigation enable コマンドは無線ロードバランスでのバンドナビゲーション機能を有効にします。

radio-load-balance band-navigation disable コマンドは無線ロードバランスでのバンドナビゲーション機能を無効にします。

undo radio-load-balance band-navigation コマンドはデフォルトに戻します。

この機能を有効にすると、2.4 GHz 無線に関連付けられたオンライン 802.11v クライアントに BSS スイッチオーバー要求を送信します。次に、802.11v クライアントは、802.11v サービスで設定された 5 GHz 無線に切り替えるかどうかを選択できます。

802.11v クライアントのデータ伝送レートを改善する為、多数の 802.11v クライアントが 2.4 GHz 無線に関連付けられている場合は、この機能を有効にします。2.4 GHz 無線に関連付けられている 802.11v クライアントの数を表示するには、display wlan client verbose コマンドを実行します。

例

ap-group で、無線ロードバランスでのバンドナビゲーション機能を有効にします。

<AC> system-view

[AC] wlan ap-group default-group

[AC] radio-load-balance band-navigation enable

17.1.3 radio-load-balance band-navigation rssi

🕮 **メモ**:

radio-load-balance band-navigation rssi コマンドはソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

radio-load-balance band-navigation rssi *rssi-value*

undo radio-load-balance band-navigation rssi

デフォルト

AP view では、AP は AP group view の設定を使用します。

AP group view では、RSSI のしきい値は 30 です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

rssi-value: RSSI のしきい値を 5～40 の範囲で指定します。

説明

radio-load-balance band-navigation rssi コマンドは RSSI のしきい値を設定します。

undo radio-load-balance band-navigation rssi コマンドはデフォルトに戻します。

無線ロードバランスのバンドナビゲーションが有効になっている場合、クライアントが 2.4 GHz 無線との関連付けを試みると、装置は次の値を比較して、クライアントを 5 GHz 無線に誘導するかどうかを判断します。

- クライアントの RSSI
- このコマンドで指定された RSSI しきい値
- **client anti-sticky** コマンドで指定した RSSI しきい値（デフォルトは 20）
  詳細については、コマンドマニュアルのセクション 2 *WLAN の "WLAN ローミングの設定"* を参照してください。

無線ロードバランスのバンドナビゲーションは、クライアントの RSSI が他の 2 つの値の両方よりも大きい場合にのみ有効になります。その後、装置はクライアントを 5 GHz 無線に誘導します。

例

AP ap 1 の RSSI しきい値を設定します。

<AC> system-view

[AC] wlan ap ap 1

[AC-wlan-ap-ap 1] radio-load-balance band-navigation rssi 35

AP group の group 1 の RSSI しきい値を設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] radio-load-balance band-navigation rssi 31

17.1.4 wlan radio-load-balance overload-5g ssid-hide

🕮 **メモ：**

- このコマンドはソフトウェアバージョン 7.2.21 を含む以降のソフトウェアからサポートしています。
- このコマンドは QX-W1110 および QX-W1010 では利用できません。

Syntax

wlan radio-load-balance overload-5g ssid-hide { **disable** | **enable** [**session value** [**gap gap-value**]] } [**force-logoff**]

undo wlan radio-load-balance overload-5g ssid-hide

デフォルト

AP view では、AP は AP group view の設定を使用します。

AP group view では、有効です。

View

System view

定義済みユーザロール

network-admin

パラメータ

session *value*: セッションしきい値を指定します。範囲は 1～120 で、デフォルトは 5 です。

gap *gap-value*: セッションギャップしきい値を指定します。範囲は 1～24 で、デフォルトは 4 です。

force-logoff: レーダー回避が発生して 1 つの 5GHz 無線が使用不可状態になることでクライアントの接続が残った 5GHz 無線に片寄ることを想定し、使用不可状態になったラジオが復旧した際に、クライアントを均等に接続しなおすために強制的に半数のクライアントを切断します。デフォルトは無効です。

disable: 5GHz 無線ロードバランスを無効にします。

enable: 5GHz 無線ロードバランスを有効にします。

説明

wlan radio-load-balance overload-5g ssid-hide enable コマンドは 5GHz 無線ロードバランスを有効にします。

wlan radio-load-balance overload-5g ssid-hide disable コマンドは 5GHz 無線ロードバランスを無効にします。

undo wlan radio-load-balance overload-5g ssid-hide コマンドはデフォルトに戻します。

このコマンドは、2 つの 5GHz 無線で同一の SSID を使用している時、それぞれの 5GHz 無線にクライアントがバランスよく接続するように設定することができます。

このコマンドを設定した後、次の 2 つの条件が満たされると、5GHz 無線はビーコンフレームの SSID を非表示にします。

- 5GHz 無線に関連付けられているクライアントの数がしきい値に達した場合
- 同じ AP 内の 2 つの 5GHz 無線の間のセッションギャップが、しきい値に達した場合

5GHz 無線に関連付けられているクライアントの数がセッションしきい値を下回ると、5GHz 無線はビーコンフレームの SSID の非表示を停止します。

なお、5GHz 無線でレーダー検知をするとその 5GHz 無線が一定時間利用できなくなるため、その 5GHz 無線に接続されていたすべてのクライアントが、同じ SSID の残された 5GHz 無線に接続され、5GHz 無線が過負荷になる可能性があります。レーダー検知をした 5GHz 無線が復旧した際、クライアントの接続状態を均等に戻す場合、**force-logoff** を設定しておくことでクライアントの半分を強制的にログオフし、再接続させます。再接続は端末に依存するため、必要な場合にのみこのキーワードを指定してください。

例

ap-group で、クライアント数 1 ギャップ 1、かつ、レーダー回避後に再バランスするように 5GHz 無線ロードバランスを有効にします。

<AC> system-view

[AC] wlan ap-group default-group

[AC] wlan radio-load-balance overload-5g ssid-hide enable session 1 gap 1 force-logoff

目次

このセクションのページは **2-x-x** です。

18 章 WLAN メッシュの設定 18-1
18.1 WLAN メッシュコマンド 18-1
18.1.1 akm mode sae 18-1
18.1.2 display wlan mesh-link ap 18-2
18.1.3 display wlan mesh-policy 18-4
18.1.4 display wlan mesh-profile 18-5
18.1.5 interface wlan-mesh 18-7
18.1.6 link-hold-rssi 18-8
18.1.7 link-initiation enable 18-8
18.1.8 link-keepalive 18-9
18.1.9 link-maximum-number 18-10
18.1.10 link-rate-mode 18-11
18.1.11 link-saturation-rssi 18-12
18.1.12 mesh-id 18-13
18.1.13 mesh-interface 18-14
18.1.14 mesh peer-mac-address 18-15
18.1.15 mesh-peer intra-ac-mpp enable 18-17
18.1.16 mesh-policy 18-17
18.1.17 mesh-port access vlan 18-19
18.1.18 mesh-port hybrid pvid 18-20
18.1.19 mesh-port hybrid vlan 18-21
18.1.20 mesh-port link-type 18-23
18.1.21 mesh-port trunk permit vlan 18-24
18.1.22 mesh-port trunk pvid 18-25
18.1.23 mesh-profile 18-27
18.1.24 mesh-profile enable 18-28
18.1.25 preshared-key 18-29
18.1.26 probe-request-interval 18-30
18.1.27 portal-service enable 18-30
18.1.28 temporary-link enable 18-32
18.1.29 wlan mesh-policy 18-33
18.1.30 wlan mesh-profile 18-33

18章 WLAN メッシュの設定

🕮 **メモ：**

WLAN メッシュの設定は、ソフトウェアバージョン 7.2.21 を含む以降のソフトウェアからサポートしています。

18.1 WLAN メッシュコマンド

18.1.1 akm mode sae

Syntax

akm mode sae

undo akm mode

デフォルト

設定なし

View

Mesh profile view

定義済みユーザロール

network-admin

説明

akm mode sae コマンドは akm（authentication and key management）モードを SAE（simultaneous authentication of equals）に設定します。

undo akm mode コマンドはデフォルトに戻します。

akm モードを設定する、あるいは削除する前に、メッシュプロファイルが無効であることを確認してください。

例

メッシュプロファイル 1 の akm モードを SAE に設定します。

<AC> system-view

[AC] wlan mesh-profile 1

[AC-wlan-mesh-profile-1] akm mode sae

関連コマンド

display wlan mesh-profile

18.1.2 display wlan mesh-link ap

Syntax

display wlan mesh-link ap [**name** *ap-name*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

verbose: メッシュリンクの詳細情報を表示します。このパラメータを指定しない場合、簡易情報を表示します。

説明

display wlan mesh-link コマンドはメッシュリンク情報を表示します。

パラメータを指定しない場合、すべてのメッシュリンクの情報を表示します。

例

AP **ap1** のメッシュリンクの簡易情報を表示します。

<AC> display wlan mesh-link ap name ap1

```
AP name: ap1
 Peer          Local         Status     RSSI  Packets(Rx/Tx)
 4ab7-c78a-22ff  75bb-c36d-4ef8  Forwarding  22    0/0
```

表 18-1 コマンド出力

フィールド	説明
Peer	ピアMPのMACアドレス
Local	ローカルAPのMACアドレス
Status	リンクのステータス。メッシュリンクがトラフィックを転送している場合、**Forwarding**と表示されます。
RSSI	メッシュリンクのRSSI
Packets(Rx/Tx)	メッシュリンクのパケット統計情報： • **Rx**－受信パケット数 • **Tx**－送信パケット数

すべての AP のメッシュリンクの詳細情報を表示します。

<AC> display wlan mesh-link ap verbose

```
AP name: ap1
 Peer MAC               : 84d9-317d-9710
 Local MAC              : 70f9-6dd7-cf00
 Status                 : Forwarding
 Link mode              : dot11an
 RSSI                   : 67
 SNR                    : 67
 Noise                  : 0 dBm
 Cost                   : 0
 Incorrect packet         : 0.00 %
 Packets
   Received             : 1508
   Sent                 : 14617
   Resent               : 162
   Lost                 : 0

AP name: ap2
 Peer MAC               : 84d9-317d-9710
 Local MAC              : 0606-e203-1111
 Status                 : Forwarding
 Link mode              : dot11an
 RSSI                   : 62
 SNR                    : 62
 Noise                  : 0 dBm
 Cost                   : 0
 Incorrect packet         : 0.03 %
 Packets
```

```
Received              : 2921
Sent                  : 2877
Resent                : 178
Lost                  : 1
```

表 18-2 コマンド出力

フィールド	説明
Peer MAC	ピアMPのMACアドレス
Local MAC	ローカルAPのMACアドレス
Status	リンクのステータス。メッシュリンクがトラフィックを転送している場合、**Forwarding**と表示されます。
Link mode	無線モード
RSSI	メッシュリンクのRSSI
SNR	信号対雑音比
Cost	リンクコスト
Incorrect packets	送信エラーが発生した送信パケットの割合
Received	受信パケットの総数
Sent	送信されたパケットの総数
Resent	再送信されたパケット数
Lost	ロスしたパケット数

18.1.3 display wlan mesh-policy

Syntax

display wlan mesh-policy [*mesh-policy-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mesh-policy-name: 大文字と小文字を区別しない 1～31 文字でメッシュポリシ名を指定します。ポリシ名を指定しない場合、すべてのメッシュポリシの情報を表示します。

説明

display wlan mesh-policy コマンドはメッシュポリシ情報を表示します。

例

全てのメッシュポリシの情報を表示します。

<AC> display wlan mesh-policy

```
Mesh policy name                 : default_mesh_policy
Mesh link initiation              : Enabled
Max links                        : 2
Probe request interval            : 1000 ms
Link hold RSSI                   : 15 dBm
Link saturation RSSI              : 150 dBm
Link establish threshold          : 5
Link rate mode                   : fixed
Temporary link establish          : Enabled
Transmission method              : Air
Active link keepalive transmit level : 0
```

表 18-3 コマンド出力

フィールド	説明
Mesh link initiation	メッシュリンク開始機能の状況： ● 有効 ● 無効
Max links	リンクの最大数
Link hold RSSI	メッシュリンクホールドRSSI
Link rate mode	リンクレートモード： ● Fixedーリンクは固定レートで動作しています。 ● Real-timeーリンクレートはリアルタイムでRSSIに適応しています。

18.1.4 display wlan mesh-profile

Syntax

display wlan mesh-profile [*mesh-profile-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mesh-profile-number: メッシュプロファイルの番号を指定します。値の範囲は 1～32 です。メッシュプロファイルを指定しない場合、すべてのメッシュプロファイルの情報を表示します。

説明

display wlan mesh-profile コマンドはメッシュプロファイル情報を表示します。

例

全てのメッシュプロファイルの情報を表示します。

<AC> display wlan mesh-profile

```
Mesh profile number         : 1
Mesh ID                   : 11
Link keepalive interval     : 2 s
Link backhaul rate          : 18 Mbps
Mesh profile status         : Enabled
Link metric type           : Not Configured
AKM mode                  : None
PSK status                : Disabled

Mesh profile number         : 2
Mesh ID                   : 22
Link keepalive interval     : 2 s
Link backhaul rate          : 18 Mbps
Mesh profile status         : Enabled
Link metric type           : Not Configured
AKM mode                  : None
PSK status                : Disabled
```

表 18-4 コマンド出力

フィールド	説明
Mesh profile status	メッシュプロファイルの状況： ● 有効 ● 無効
AKM mode	akmモード ● None－akmモードは指定されていません。 ● SAE－SAEモードが指定されています。
PSK status	事前共有鍵設定状況： ● Enabled－事前共有鍵が設定されています。 ● Disabled－事前共有鍵は設定されていません。

18.1.5 interface wlan-mesh

Syntax

interface wlan-mesh *interface-number*

undo interface wlan-mesh *interface-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-number: メッシュインタフェースの番号を指定します。値の範囲は 0～1023 です。

説明

interface wlan-mesh コマンドはメッシュインタフェースを作成し、その view に移行します。あるいは既存のメッシュインタフェースの view に移行します。

undo interface wlan-mesh コマンドはメッシュインタフェースを削除します。

例

AP **ap1** にメッシュインタフェース 1 を作成し、WLAN メッシュインタフェース view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1030

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-mesh1]

AP グループ **g1** のすべての AP にメッシュインタフェース 2 を作成し、AP グループ view の WLAN メッシュインタフェース view に移行します。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2]

関連コマンド

mesh-interface

18.1.6 link-hold-rssi

Syntax

link-hold-rssi *value*

undo link-hold-rssi

デフォルト

15 dBm

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

value: メッシュリンクホールド RSSI を指定します。値の範囲は 5～100dBm です。

説明

link-hold-rssi コマンドはメッシュリンクホールド RSSI（メッシュリンクを保持するための最小信号強度）を設定します。

undo link-hold-rssi コマンドはデフォルトに戻します。

例

メッシュリンク **abc** に対してメッシュリンクホールド RSSI を 24dBm に設定します。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] link-hold-rssi 24

関連コマンド

display wlan mesh-policy

18.1.7 link-initiation enable

Syntax

link-initiation enable

undo link-initiation enable

デフォルト

有効

View

Mesh policy view

定義済みユーザロール

network-admin

説明

link-initiation enable コマンドはメッシュリンク開始を有効にします。

undo link-initiation enable コマンドはメッシュリンク開始を無効にします。

メッシュリンク開始を有効にすることで、MP はリンクオープン要求を送信していないピアに対してリンクオープン要求を送信します。この機能が無効の場合、MP はピアがリンクオープン要求を送信するまで、ピアに対してリンクオープン要求を送信しません。

例

メッシュリンク開始を無効にします。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] undo link-initiation enable

関連コマンド

display wlan mesh-policy

18.1.8 link-keepalive

Syntax

link-keepalive *keepalive-interval*

undo link-keepalive

デフォルト

2 秒

View

Mesh profile view

定義済みユーザロール

network-admin

パラメータ

keepalive-interval: keepalive 間隔を指定します。値の範囲は 1～1800 秒です。

説明

link-keepalive コマンドはメッシュリンク keepalive 間隔を設定します。

undo link-keepalive コマンドはデフォルトに戻します。

メッシュリンクの MP はメッシュリンク状態を検出するために keepalive パケットを使用します。大きい MAC アドレスをもつ MP は、keepalive 間隔で keepalive パケットをピアの端に送信します。keepalive パケットを送信した MP は、連続して 3 回の keepalive 間隔終了前に応答を受信しない場合、メッシュリンクを切断します。また、keepalive パケットを受信した MP は、連続して 3 回の keepalive 間隔終了前に keepalive パケットを受信しない場合、メッシュリンクを切断します。リンク状態を正しく検出するため、送信側の keepalive 間隔は、受信側の keepalive 間隔の 3 倍以下に設定してください。

例

メッシュプロファイル 1 でメッシュリンク keepalive 間隔を 6 秒に設定します。

<AC> system-view

[AC] wlan mesh-profile 1

[AC-wlan-mesh-profile-1] link-keepalive 6

関連コマンド

display wlan mesh-profile

18.1.9 link-maximum-number

🕮 **メモ**:

ホップ数（ネットワーク内のメッシュリンクの最長経路）が増加するにつれてスループットは低下します。

Syntax

link-maximum-number *max-link-number*

undo link-maximum-number

デフォルト

2

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

max-link-number: メッシュリンクの最大数を指定します。値の範囲は 1～8 です。

説明

link-maximum-number コマンドは無線のメッシュリンクの最大数を設定します。

undo link-maximum-number コマンドはデフォルトに戻します。

MP はメッシュリンクが最大数に達すると、無線での新規メッシュリンクの確立を停止します。

例

メッシュポリシ **abc** に対してメッシュリンクの最大数を 5 に設定します。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] link-maximum-number 5

関連コマンド

display wlan mesh-policy

18.1.10 link-rate-mode

Syntax

link-rate-mode { **fixed** | **real-time** }

undo link-rate-mode

デフォルト

fixed モード

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

fixed: fixed モードを指定します。fixed モードでは、メッシュリンクのインタフェースレートは、無線インタフェースレートの現在の設定の最大値に固定します。

real-time: real-time モードを指定します。real-time モードでは、メッシュリンクのインタフェースレートは自動的に RSSI に適応します。

説明

link-rate-mode コマンドはメッシュリンクに対してリンクレートモードを設定します。

undo link-rate-mode コマンドはデフォルトに戻します。

例

メッシュポリシ **abc** に対して、メッシュリンクレートモードを real-time に指定します。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] link-rate-mode real-time

関連コマンド

display wlan mesh-policy

18.1.11 link-saturation-rssi

Syntax

link-saturation-rssi *value*

undo link-saturation-rssi

デフォルト

150 dBm

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

value: リンク飽和 RSSI 値を 30～150 dBm の範囲で指定します。

説明

link-saturation-rssi コマンドはリンク飽和 RSSI を設定します。

undo link-saturation-rssi コマンドはデフォルトに戻します。

強力な信号強度がチップのパフォーマンスに影響を与えないように、リンクの RSSI がリンク飽和 RSSI を超えた場合に MP はアクティブ リンクを終了します。

例

メッシュポリシ **abc** に対して、リンク飽和 RSSI を 50 dBm に設定します。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] link-saturation-rssi 50

関連コマンド

display wlan mesh-policy

18.1.12 mesh-id

Syntax

mesh-id *mesh-id*

undo mesh-id

デフォルト

設定なし

View

Mesh profile view

定義済みユーザロール

network-admin

パラメータ

mesh-id: メッシュ ID を指定します。大文字と小文字を区別する 1～32 文字で指定できます。

説明

mesh-id コマンドはメッシュプロファイルにメッシュ ID に割り当てます。

undo interface wlan-mesh コマンドはデフォルトに戻します。

例

メッシュプロファイル 1 にメッシュ ID を割り当てます。

<AC> system-view

[AC] wlan mesh-profile 1

[AC-wlan-mesh-profile-1] mesh-id mesh

関連コマンド

display wlan mesh-profile

18.1.13 mesh-interface

Syntax

Radio view:

mesh-interface { *interface-number* | **disable** }

undo mesh-interface

AP グループの Radio view:

mesh-interface *interface-number*

undo mesh-interface

デフォルト

Radio view：AP グループの Radio view の設定を使用します。

AP グループの Radio view：設定なし

View

Radio view

AP グループの Radio view

定義済みユーザロール

network-admin

パラメータ

interface-number: メッシュインタフェースの番号を指定します。値の範囲は 0～1023 です。

説明

mesh-interface コマンドは無線にメッシュインタフェースをバインドします。

mesh-interface disable コマンドは無線からメッシュインタフェースのバインドを解除し、AP が AP グループの Radio view の設定を引き継がないようにします。

undo mesh-interface コマンドはデフォルトに戻します。

1 つの無線に対して 1 つのメッシュインタフェースをバインドできます。このコマンドを複数回実行した場合、最後に実行したものが適用されます。

AP view で作成されたメッシュインタフェースは、AP view の無線にのみバインドできます。AP グループ view で作成されたメッシュインタフェースは、AP view の無線と AP グループ View の無線の両方にバインドできます。

例

AP **ap1** の radio 1 にメッシュインタフェース 1 をバインドします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mesh-interface 1

AP グループ **g1** の AP の radio 1 にメッシュインタフェース 2 をバインドする。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] ap-model QX-W1030

[AC-wlan-ap-group-g1-ap-model-QX-W1030] radio 1

[AC-wlan-ap-group-g1-ap-model-QX-W1030-radio-1] mesh-interface 2

関連コマンド

interface wlan-mesh

18.1.14 mesh peer-mac-address

Syntax

Radio view:

mesh peer-mac-address [**blacklist**] { *mac-address* | **disable** }

undo mesh peer-mac-address [**blacklist**] [*mac-address*]

AP グループの Radio view:

mesh peer-mac-address [**blacklist**] *mac-address*

undo mesh peer-mac-address [**blacklist**] [*mac-address*]

デフォルト

Radio view：AP グループの Radio view の設定を使用します。

AP グループの Radio view：設定なし

View

Radio view

AP グループの Radio view

定義済みユーザロール

network-admin

パラメータ

blacklist: MP の MAC アドレスをメッシュピアブラックリストに追加します。このパラメータを指定しない場合、MAC アドレスはメッシュピアホワイトリストに追加されます。

mac-address: MP の MAC アドレスを H-H-H 形式で指定します。

説明

mesh peer-mac-address コマンドはメッシュピアブラックリストもしくはホワイトリストに MP を追加します。

mesh peer-mac-address disable コマンドはすべての MP からメッシュピアブラックリストもしくはホワイトリストを削除し、AP が AP グループ view の設定を引き継がないようにします。

undo mesh peer-mac-address コマンドはメッシュピアブラックリストもしくはホワイトリストから MP を削除します。

ブラックリストとホワイトリストの両方を設定した場合、ホワイトリストのみ適用されます。

同じ MAC アドレスをホワイトリストもしくはブラックリストに追加するために、このコマンドを複数回実行した場合、最後の設定が適用されます。

Radio view の設定は AP グループの Radio view の設定より優先されます。

例

AP **ap1** のメッシュピアホワイトリストに MP の MAC アドレスを追加します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mesh peer-mac-address 4ab7-c78a-22ff

AP **ap1** のメッシュピアブラックリストに MP の MAC アドレスを追加します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mesh peer-mac-address blacklist 4ab7-c78a-22ff

AP グループ **g1** の AP のメッシュピアホワイトリストに MP の MAC アドレスを追加します。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] ap-model QX-W1030

[AC-wlan-ap-group-g1-ap-model-QX-W1030] radio 1

[AC-wlan-ap-group-g1-ap-model-QX-W1030-radio-1] mesh peer-mac-address 4ab7-c78a-22ff

18.1.15 mesh-peer intra-ac-mpp enable

Syntax

mesh-peer intra-ac-mpp enable

undo mesh-peer intra-ac-mpp enable

デフォルト

ループを防ぐため、同一の AC に関連付いている MPP はメッシュピアになることはできません。

View

Global configuration view

定義済みユーザロール

network-admin

説明

mesh-peer intra-ac-mpp enable コマンドは同一の AC に関連付いた MPP がメッシュピアになることを有効にします。

undo mesh-policy コマンドはデフォルトに戻します。

同一の AC に関連付いた MPP が VLAN1 でメッシュリンクを確立しないようにしてください。

例

同一の AC に関連付いた MPP がメッシュピアになるように設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] mesh-peer intra-ac-mpp enable

18.1.16 mesh-policy

Syntax

Radio view:

mesh-policy name { **default** | **name** *policy-name* }

undo mesh-policy

AP グループの Radio view:

mesh-policy name *policy-name*

undo mesh-policy

デフォルト

Radio view：AP グループの Radio view の設定を使用します。

AP グループの Radio view：デフォルトメッシュポリシの **default_mesh_policy** が無線にバインドされています。

View

Radio view

AP グループの Radio view

定義済みユーザロール

network-admin

パラメータ

policy-name: メッシュポリシ名を指定します。大文字と小文字を区別しない 1～31 文字で指定できます。

default: デフォルトメッシュポリシの **default_mesh_policy** を指定します。

説明

mesh-policy コマンドはメッシュポリシを無線にバインドします。

undo mesh-policy コマンドはデフォルトに戻します。

1 つの無線に 1 つのメッシュポリシをバインドできます。このコマンドを複数回実行した場合、最後に実行したものが適用されます。

Radio view の設定は AP グループの Radio view の設定より優先されます。

例

AP **ap1** の radio 1 にメッシュポリシ **policy1** をバインドします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mesh-policy name policy1

AP グループ **g1** の AP の radio1 にメッシュポリシ **policy2** をバインドします。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] ap-model QX-W1030

[AC-wlan-ap-group-g1-ap-model-QX-W1030] radio 1

[AC-wlan-ap-group-g1-ap-model-QX-W1030-radio-1] mesh-policy name policy2

AP **ap1** の radio 1 にデフォルトメッシュポリシをバインドします。

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mesh-policy default

関連コマンド

wlan mesh-policy

18.1.17 mesh-port access vlan

Syntax

mesh-port access vlan *vlan-id*

undo mesh-port access vlan

デフォルト

VLAN 1

View

WLAN-mesh interface view

AP グループの WLAN-mesh interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を 1～4094 の範囲で指定します。

説明

mesh-port access vlan コマンドはアクセスタイプのメッシュインタフェースに VLAN を割り当てます。

undo mesh-port access vlan コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN が存在することを確認してください。

例

AP **ap1** の WLAN メッシュ 1 に VLAN 2 を割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port access vlan 2

AP グループ **g1** の AP の WLAN メッシュ 2 に VLAN 2 を割り当てます。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port access vlan 2

関連コマンド

- **interface wlan-mesh**
- **remote-configuration enable**

18.1.18 mesh-port hybrid pvid

Syntax

mesh-port hybrid pvid vlan *vlan-id*

undo mesh-port hybrid pvid

デフォルト

ハイブリッドポートの PVID は、ポートのリンクタイプがアクセスだったときに属していた VLAN の値です。

View

WLAN-mesh interface view

AP グループの WLAN-mesh interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を 1～4094 の範囲で指定します。

説明

mesh-port hybrid pvid vlan コマンドはハイブリッドタイプのメッシュインタフェースの PVID を設定します。

undo mesh-port hybrid pvid コマンドはハイブリッドタイプのメッシュインタフェースの PVID を VLAN 1 に設定します

2 つの MP が互いにメッシュリンクを確立するために使用するメッシュインタフェースが同じ PVID を持っていることを確認してください。

ハイブリッドポートがポート VLAN からパケットを転送できるように、ハイブリッドポートにポート VLAN を割り当ててください。

例

AP **ap1** の WLAN メッシュ 1 の PVID を VLAN 100 に設定し、タグなしメンバとして割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port link-type hybrid

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port hybrid pvid vlan 100

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port hybrid vlan 100 untagged

AP グループ **g1** の AP の WLAN メッシュ 2 の PVID を VLAN 100 に設定し、タグなしメンバとして割り当てます。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port link-type hybrid

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port hybrid pvid vlan 100

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port hybrid vlan 100 untagged

関連コマンド

- **mesh-port hybrid vlan**
- **mesh-port link-type**

18.1.19 mesh-port hybrid vlan

Syntax

mesh-port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo mesh-port hybrid vlan *vlan-id-list*

デフォルト

ハイブリッドポートは、ポートのリンクタイプがアクセスのときに属していた VLAN のタグなしメンバです。

View

WLAN-mesh interface view

AP グループの WLAN-mesh interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: スペースで区切られた VLAN の値を最大 10 個まで指定します。各項目は VLAN ID、もしくは VLAN ID の範囲を vlan-id1 から vlan-id2 の形式で指定します。VLAN ID の値の範囲は 1～4094 です。vlan-id2 パラメータの値は、vlan-id1 パラメータの値以上である必要があります。指定した VLAN は、装置に既に存在している必要があります。

tagged: 指定した VLAN のタグ付きメンバとしてポートを設定します。VLAN のタグ付きメンバは、VLAN タグを削除せずに VLAN からパケットを送信します。

untagged: 指定した VLAN のタグなしメンバとしてポートを設定します。VLAN タグを削除した後、VLAN のタグなしメンバが VLAN からパケットを送信します。

説明

mesh-port hybrid vlan コマンドはハイブリッドタイプのメッシュインタフェースに VLAN を割り当てます。

undo mesh-port hybrid vlan コマンドは指定された VLAN からハイブリッドタイプのメッシュインタフェースを除外します。

ハイブリッドポートでは、複数の VLAN を許可できます。ハイブリッドポートでこのコマンドを複数回実行すると、ハイブリッドポートは指定された VLAN をすべて許可します。

例

AP **ap1** で WLAN メッシュ 1 をハイブリッドポートとして作成し、タグ付きメンバとして VLAN 2、VLAN 4、VLAN 50～VLAN 100 を割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-1020

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port link-type hybrid

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port hybrid vlan 2 4 50 to 100 tagged

AP グループ **g1** の AP で WLAN メッシュ 2 をハイブリッドポートとして作成し、タグ付きメンバとして VLAN 2、VLAN 4、VLAN 50～VLAN 100 を割り当てます。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port link-type hybrid

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port hybrid vlan 2 4 50 to 100 tagged

関連コマンド

- **mesh-port hybrid pvid**
- **mesh-port link-type**

18.1.20 mesh-port link-type

Syntax

mesh-port link-type { **access** | **hybrid** | **trunk** }

undo mesh-port link-type

デフォルト

アクセスポート

View

WLAN-mesh interface view

AP グループの WLAN-mesh interface view

定義済みユーザロール

network-admin

パラメータ

access: ポートリンクタイプをアクセスに設定します。

hybrid: ポートリンクタイプをハイブリッドに設定します。

trunk: ポートリンクタイプをトランクに設定します。

説明

mesh-port link-type コマンドはメッシュインタフェースのリンクタイプを設定します。

undo mesh-port link-type コマンドはデフォルトに戻します。

ポートのリンクタイプをトランクとハイブリッド間で変更する場合、まずアクセスポートに設定する必要があります。

例

AP **ap1** で WLAN メッシュ 1 をトランクポートに設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port link-type trunk

AP グループ **g1** の AP で WLAN メッシュ 2 をトランクポートに設定します。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port link-type trunk

18.1.21 mesh-port trunk permit vlan

Syntax

mesh-port trunk permit vlan { *vlan-id-list* | **all** }

undo mesh-port trunk permit vlan { *vlan-id-list* | **all** }

デフォルト

VLAN 1

View

WLAN-mesh interface view

AP グループの WLAN-mesh interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: スペースで区切られた VLAN の値を最大 10 個まで指定します。各項目は VLAN ID、もしくは VLAN ID の範囲を vlan-id1 から vlan-id2 の形式で指定します。VLAN ID の値の範囲は 1～4094 です。vlan-id2 パラメータの値は、vlan-id1 パラメータの値以上である必要があります。指定した VLAN は、装置に既に存在している必要があります。

tagged: 指定した VLAN のタグ付きメンバとしてポートを設定します。VLAN のタグ付きメンバは、VLAN タグを削除せずに VLAN からパケットを送信します。

untagged: 指定した VLAN のタグなしメンバとしてポートを設定します。VLAN タグを削除した後、VLAN のタグなしメンバが VLAN からパケットを送信します。

説明

mesh-port trunk permit vlan コマンドはトランクタイプのメッシュインタフェースに VLAN を割り当てます。

undo mesh-port trunk permit vlan コマンドは指定された VLAN からトランクタイプのメッシュインタフェースを除外します。

トランクポートでは、複数の VLAN を許可できます。トランクポートでこのコマンドを複数回実行すると、トランクポートは指定された VLAN をすべて許可します。

トランクポートでは、PVID からのパケットのみがタグなしで通過できます。

例

AP **ap1** で WLAN メッシュ 1 をトランクポートとして作成し、VLAN 2、VLAN 4、VLAN 50～VLAN 100 を割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-1020

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port link-type trunk

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port trunk permit vlan 2 4 50 to 100

AP グループ **g1** の AP で WLAN メッシュ 2 をトランクポートとして作成し、VLAN 2、VLAN 4、VLAN 50～VLAN 100 を割り当てます。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port link-type trunk

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port trunk permit vlan 2 4 50 to 100

関連コマンド

- **mesh-port link-type**
- **mesh-port trunk pvid**

18.1.22 mesh-port trunk pvid

Syntax

mesh-port trunk pvid *vlan-id*

undo mesh-port trunk pvid

デフォルト

トランクポートの PVID は VLAN 1 です。

View

WLAN-mesh interface view

AP グループの WLAN-mesh interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を 1～4094 の範囲で指定します。

説明

mesh-port trunk pvid コマンドはトランクタイプのメッシュインタフェースの PVID を設定します。

undo mesh-port trunk pvid コマンドはデフォルトに戻します。

存在しない VLAN をトランクポートのポート VLAN として指定できます。

2 つの MP が互いにメッシュリンクを確立するために、使用するメッシュインタフェースが同じ PVID を持っていることを確認してください。

トランクポートがポート VLAN からパケットを送信できるようにするには、トランクポートをポート VLAN に割り当てる必要があります。

例

AP **ap1** の WLAN メッシュ 1 の PVID を VLAN 100 に設定し、タグなしメンバとして割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-1020

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port trunk pvid vlan 100

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port trunk permit vlan 100

AP グループ **g1** の AP の WLAN メッシュ 2 の PVID を VLAN 100 に設定し、タグなしメンバとして割り当てます。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port trunk pvid vlan 100

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port trunk permit vlan 100

関連コマンド

- **mesh-port link-type**
- **mesh-port trunk permit vlan**

18.1.23 mesh-profile

Syntax

Radio view:

mesh-profile { *mesh-profile-number* | **disable** }

undo mesh-profile

AP グループの Radio view:

mesh-profile *mesh-profile-number*

undo mesh-profile

デフォルト

Radio view：AP グループの Radio view の設定を使用します。

AP グループの Radio view：設定なし

View

Radio view

AP グループの Radio view

定義済みユーザロール

network-admin

パラメータ

mesh-profile-number: メッシュインタフェースの番号を指定します。値の範囲は 1～32 です。

説明

mesh-profile コマンドはメッシュイプロファイルを作成し、無線にバインドします。

mesh-profile disable コマンドは無線からメッシュプロファイルのバインドを解除し、AP が AP グループの設定を引き継がないようにします。

undo interface wlan-mesh コマンドはデフォルトに戻します。

Radio view の設定は AP グループの Radio view の設定より優先されます。

例

AP **ap1** の radio 1 にメッシュプロファイル 1 をバインドします。

<AC> system-view

[AC] wlan ap ap1 model QX-1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mesh-profile 1

AP グループ **g1** の AP の radio 1 にメッシュプロファイル 2 をバインドします。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] ap-model QX-1020

[AC-wlan-ap-group-g1-ap-model-QX-1020] radio 1

[AC-wlan-ap-group-g1-ap-model-QX-1020-radio-1] mesh-profile 2

関連コマンド

- **mesh-profile enable**
- **wlan mesh-profile**

18.1.24 mesh-profile enable

Syntax

mesh-profile enable

undo mesh-profile enable

デフォルト

無効

View

Mesh profile view

定義済みユーザロール

network-admin

説明

mesh-profile enable コマンドはメッシュプロファイルを有効にします。

undo mesh-profile enable コマンドはメッシュプロファイルを無効にします。

メッシュプロファイルを有効にする前に、メッシュ ID を割り当てる必要があります。

例

メッシュプロファイル 1 を有効にします。

<AC> system-view

[AC] wlan mesh-profile 1

[AC-wlan-mesh-profile-1] mesh-profile enable

関連コマンド

mesh-id

18.1.25 preshared-key

Syntax

preshared-key { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*

undo preshared-key

デフォルト

設定なし

View

Mesh profile view

定義済みユーザロール

network-admin

パラメータ

pass-phrase: 文字列形式で鍵を設定します。

raw-key: 16 進数形式で鍵を設定します。

cipher: 暗号化形式で鍵を指定します。

simple: 平文形式で鍵を指定します。安全のため、平文形式で指定された鍵は暗号化形式で格納されます。

string: 大文字と小文字を区別する鍵列を指定します。鍵の長さの範囲は以下の通りです。

- **pass-phrase plaintext**－8～63 文字
- **pass-phrase ciphertext**－41～117 文字
- **raw-key plaintext**－64 桁の 16 進数字
- **raw-key ciphertext**－117 文字

説明

preshared-key コマンドはメッシュプロファイルに事前共有鍵を追加します。

undo preshared-key コマンドはデフォルトに戻します。

このコマンドを使用する前に、メッシュプロファイルが無効であることを確認してください。

メッシュプロファイルに設定できる事前共有鍵は 1 つです。このコマンドを複数回実行した場合、最後の設定が適用されます。

例

メッシュプロファイル 1 に平文の事前共有鍵 **abcdefghij** を追加します。

<AP> system-view

[AP] wlan mesh-profile 1

[AP-wlan-mesh-profile-1] preshared-key pass-phrase simple abcdefghij

関連コマンド

display wlan mesh-profile

18.1.26 probe-request-interval

Syntax

probe-request-interval *interval-value*

undo probe-request-interval

デフォルト

1000 ミリ秒

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

interval-value: 100～8191 ミリ秒の範囲で間隔を指定します。

説明

probe-request-interval コマンドはプローブ要求間隔を設定します。

undo probe-request-interval コマンドはデフォルトに戻します。

例

メッシュポリシ a**bc** に対してプローブ要求間隔を 500 ミリ秒に設定します。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] probe-request-interval 500

関連コマンド

display wlan mesh-policy

18.1.27 portal-service enable

Syntax

AP view もしくは AP グループ view:

portal-service { **disable** | **enable** }

undo portal-service

Global configuration view:

portal-service enable

undo portal-service

デフォルト

AP view では、AP グループ view の設定を使用します。AP グループ view に設定が存在しない場合、global configuration view の設定を使用します。

AP グループ view では、global configuration view の設定を使用します。

Global configuration view では、MPP はプローブ要求を送信します。

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

disable: MPP がプローブ要求を送信し、AP group view もしくは global configuration view の設定を引き継がないようにします。

enable: MPP がプローブ要求を送信するのを無効にします。

説明

portal-service enable コマンドは MPP がプローブ要求を送信するのを無効にします。

portal-service disable コマンドは MPP がプローブ要求を送信し、AP group view もしくは global configuration view の設定を引き継がないようにします。

undo probe-service コマンドはデフォルトに戻します。

WLAN メッシュネットワークを有線ネットワークに接続するメッシュポイントとして、MPP は多数のメッシュリンクを確立する必要があります。パフォーマンスを維持するために、MPP がネイバ検出のプローブ要求を送信しないように無効にできます。MPP は、他の MP からのプローブ要求にのみ応答します。

例

AP **ap1** でプローブ要求を送信しないようにします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] portal-service enable

AP グループ **group1** の AP でプローブ要求を送信しないようにします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] portal-service enable

グローバルでプローブ要求を送信しないようにします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] portal-service enable

18.1.28 temporary-link enable

Syntax

temporary-link enable

undo temporary-link enable

デフォルト

有効

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

interval-value: 100～8191 ミリ秒の範囲で間隔を指定します。

説明

temporary-link enable コマンドはテンポラリメッシュリンクの確立を有効にします。

undo temporary-link enable コマンドはデフォルトに戻します。

例

テンポラリメッシュリンクの確立を有効にします。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] temporary-link enable

18.1.29 wlan mesh-policy

Syntax

wlan mesh-policy *policy-name*

undo wlan mesh-policy *policy-name*

デフォルト

システム定義のポリシ「**default_mesh_policy**」が存在します。

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-name: メッシュポリシ名を指定します。大文字と小文字を区別しない 1～31 文字で指定できます。

説明

wlan mesh-policy コマンドはメッシュポリシを作成し、その view に移行します。あるいは既存のメッシュポリシの view に移行します。

undo wlan mesh-policy コマンドはメッシュポリシを削除します。

無線で使用中のメッシュポリシ内の属性設定を削除、修正する前に、無線にバインドされたメッシュプロファイルを無効にしてください。

システム定義のメッシュポリシを修正もしくは削除することはできません。

例

メッシュポリシ **abc** を作成し、その view に移行します。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc]

18.1.30 wlan mesh-profile

Syntax

wlan mesh-profile *mesh-profile-number*

undo wlan mesh-profile *mesh-profile-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mesh-profile-number: メッシュプロファイルの番号を指定します。値の範囲は 1～32 です。

説明

wlan mesh-profile コマンドはメッシュプロファイルを作成し、その view に移行します。あるいは既存のメッシュプロファイルの view に移行します。

undo wlan mesh-profile コマンドはメッシュプロファイルを削除します。

メッシュプロファイル内の属性設定を修正するには、メッシュプロファイルを無効にする必要があります。

例

メッシュプロファイル 1 を作成し、その view に移行します。

<AC> system-view

[AC] wlan mesh-profile 1

[AC-wlan-mesh-profile-1]

関連コマンド

mesh-profile enable

目次

このセクションのページは **2-x-x** です。

19 章 コンフィグレーションプロファイルの設定 19-1
19.1 コンフィグレーションプロファイルの設定コマンド 19-1
19.1.1 acl 19-1
19.1.2 address 19-3
19.1.3 address range 19-4
19.1.4 authentication-mode 19-5
19.1.5 authorization-attribute 19-7
19.1.6 configuration profile 19-9
19.1.7 configuration-profile 19-10
19.1.8 dhcp enable 19-11
19.1.9 dhcp relay server-address 19-12
19.1.10 dhcp select 19-13
19.1.11 dhcp server ip-pool 19-14
19.1.12 dns-list 19-15
19.1.13 expired 19-16
19.1.14 forbidden-ip-range 19-17
19.1.15 gateway-list 19-18
19.1.16 interface 19-19
19.1.17 interface bridge-aggregation 19-19
19.1.18 interface vlan-interface 19-20
19.1.19 ip address 19-21
19.1.20 ip address dhcp-alloc 19-22
19.1.21 ip route-static 19-23
19.1.22 line 19-24
19.1.23 line class 19-25
19.1.24 local-user 19-26
19.1.25 nat address-group 19-28
19.1.26 nat inbound 19-29
19.1.27 nat outbound 19-32
19.1.28 network 19-35
19.1.29 packet-filter 19-36
19.1.30 password 19-37
19.1.31 port access vlan 19-39
19.1.32 port hybrid pvid 19-39
19.1.33 port hybrid vlan 19-41
19.1.34 port link-aggregation group 19-42

19.1.35 port link-type 19-43
19.1.36 port trunk permit vlan 19-44
19.1.37 port trunk pvid 19-45
19.1.38 port-isolate enable 19-46
19.1.39 qos priority 19-47
19.1.40 qos trust 19-48
19.1.41 rule (IPv4 advanced ACL view) 19-49
19.1.42 rule (IPv4 basic ACL view) 19-55
19.1.43 rule (Layer 2 ACL view) 19-57
19.1.44 rule comment 19-59
19.1.45 service-type 19-60
19.1.46 set authentication password 19-60
19.1.47 shutdown 19-62
19.1.48 step 19-63
19.1.49 telnet server enable 19-64
19.1.50 vlan 19-65

19章 コンフィグレーションプロファイルの設定

19.1 コンフィグレーションプロファイルの設定コマンド

🕮 **メモ**:

この章のコマンドは、ソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

19.1.1 acl

Syntax

acl number *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]

acl { name *acl-name* | **number** *acl-number* [**name** *acl-name*] }

acl { **advanced** | **basic** } { *acl-number* | **name** *acl-name* }

acl mac { *acl-number* | **name** *acl-name* }

undo acl { all | **name** *acl-name* | **number** *acl-number* }

undo acl { **all** | { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } }

undo acl mac { **all** | *acl-number* | **name** *acl-name* }

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

basic: 標準 ACL を指定します。

advanced: 拡張 ACL を指定します。

mac: L2 ACL を指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。

name *acl-name*: ACL を識別しやすくするため、ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。混乱を避けるため、**all** は使用できません。

all: すべての ACL を指定します。

説明

acl コマンドは ACL を作成し、ACL の view に移行します。すでに ACL が作成されている場合、その view に移行します。

undo acl コマンドは指定された、あるいはすべての ACL を削除します。

ACL のルールが一致順序を含む、あるいは以下の一致基準が有効である場合、一致するパケットはソフトウェアベースのパケット転送を行います。

- 送信元および宛先 IP アドレス
- 送信元ポート、宛先ポート
- トランスポートレイヤプロトコル
- ICMP メッセージタイプ、メッセージコード、およびメッセージ名
- VPN インスタンス
- ロギング
- タイムレンジ

ソフトウェアベースのパケット転送は、転送エントリのため、コントロールプレーンにパケットを送信します。これは装置のパケット転送に影響します。

例

コンフィグレーションプロファイル **ap1** に標準 IPv4 ACL 2000 を作成し、その view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl basic 2000

[AC-config-profile-ap1-acl-ipv4-basic-2000]

コンフィグレーションプロファイル **ap1** に ACL 名が flow の標準 IPv4 ACL を作成し、その view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl basic name flow

[AC-config-profile-ap1-acl-ipv4-basic-flow]

コンフィグレーションプロファイル **ap1** に 拡張 IPv4 ACL 3000 を作成し、その view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl advanced 3000

[AC-config-profile-ap1-acl-ipv4-adv-3000]

コンフィグレーションプロファイル **ap1** に L2 ACL 4000 を作成し、その view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl mac 4000

[AC-config-profile-ap1-acl-mac-4000]

コンフィグレーションプロファイル **ap1** に ACL 名が flow の L2 ACL を作成し、その view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl mac name flow

[AC-config-profile-ap1-acl-mac-flow]

19.1.2 address

Syntax

address *start-address end-address*

undo address *start-address end-address*

デフォルト

設定なし

View

Configuration profile-NAT address group view

定義済みユーザロール

network-admin

パラメータ

start-address end-address: アドレス範囲の開始 IP アドレスと終了 IP アドレスを指定します。終了アドレスは開始アドレスより小さくできません。同じ場合、アドレス範囲には IP アドレスが 1 つしかありません。IP アドレスの範囲は 65535 個まで指定できます。

説明

address コマンドは NAT アドレスグループにアドレス範囲を追加します。

undo address コマンドは NAT アドレスグループからアドレス範囲を削除します。

NAT アドレスグループは、アドレス範囲のセットです。外部ネットワーク宛てのパケットの送信元アドレスは、アドレス範囲の 1 つのアドレスに変換されます。

単一の NAT アドレスグループまたは複数の NAT アドレスグループのアドレス範囲が重複していないことを確認します。

例

コンフィグレーションプロファイル **ap1** に作成した NAT アドレスグループ 2 にアドレス範囲を追加します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] nat address-group 2

[AC-config-profile-address-group-2] address 10.1.1.1 10.1.1.15

[AC-config-profile-address-group-2] address 10.1.1.20 10.1.1.30

関連コマンド

nat address-group

19.1.3 address range

Syntax

address range *start-ip-address end-ip-address*

undo address range

デフォルト

設定なし

View

Configuration profile-DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

start-ip-address: 開始 IP アドレスを指定します。

end-ip-address: 終了 IP アドレスを指定します。

説明

address range コマンドはダイナミックの割り当てを行うため DHCP アドレスプールの IP アドレス範囲を設定します。

undo address range コマンドは DHCP アドレスプールの IP アドレス範囲を削除します。

IP アドレス範囲が指定されていない場合、address pool view で **network** コマンドを使用してサブネットのすべての IP アドレスを割り当てることができます。IP アドレス範囲が指定されている場合、IP アドレス範囲の IP アドレスのみを割り当てることができます。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

address range で指定されたアドレス範囲は **network** コマンドで指定されたサブネット内にある必要があります。範囲外のアドレスを割り当てることはできません。

例

コンフィグレーションプロファイル **ap1** の DHCP アドレスプール 1 に 192.168.8.1～192.168.8.150 のアドレス範囲を指定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool 1

[AC-config-profile-ap1-dhcp-pool-1] address range 192.168.8.1 192.168.8.150

関連コマンド

network

19.1.4 authentication-mode

Syntax

authentication-mode { **none** | **password** | **scheme** }

undo authentication-mode

デフォルト

VTY line の認証モードは password です。

コンソールユーザの認証モードは製品モデルにより異なります。

QX-W1000 シリーズは none です。

QX-W1100 シリーズは password です。

QX-W1200 シリーズは password です。

View

Configuration profile-user line view

Configuration profile-user line class view

定義済みユーザロール

network-admin

パラメータ

none: 認証を無効にします。

password: ローカルパスワード認証を行います。

scheme: AAA 認証を行います。AAA の詳細はオペレーションマニュアルのセクション 9 *セキュリティ　"AAA"* を参照してください。

説明

authentication-mode コマンドは user line の認証モードを設定します。

undo authentication-mode コマンドはデフォルトに戻します。

network-admin またはレベル 15 ユーザの役割を割り当てられたユーザだけがこのコマンドを実行することができます。他のユーザがこのコマンドを実行する権利を与えられても、このコマンドを実行することができません。

認証モードが **none** である場合、すべてのユーザは認証なしでログインすることができます。装置のセキュリティを改善するため、認証モードを **password** あるいは **scheme** にしてください。

VTY line view で、**authentication-mode** コマンドは **protocol inbound** コマンドと関連します。VTY line view で 2 つのコマンドのうち、1 つコマンドのみデフォルトでない認証モードである場合、もう一方のコマンドは VTY line class view の設定に関わらず、デフォルトの認証モードを使用します。

認証モードを変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

例

コンフィグレーションプロファイル **ap1** の user line VTY 0 で認証モードを none にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] line vty 0

[AC-config-profile-ap1-line-vty0] authentication-mode none

コンフィグレーションプロファイル **ap1** の user line VTY 0 で認証モードを password に設定し、パスワードを 321 に設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] line vty 0

[AC-config-profile-ap1-line-vty0] authentication-mode password

[AC-config-profile-ap1-line-vty0] set authentication password simple 321

コンフィグレーションプロファイル **ap1** の user line VTY 0 で認証モードを scheme に設定します。ローカルユーザ 123 を設定し、パスワードを 321 に設定します。Telnet サービスを割り当て、ユーザのユーザロールを network-admin に割り当てます。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] line vty 0

[AC-config-profile-ap1-line-vty0] authentication-mode scheme

[AC-config-profile-ap1-line-vty0] quit

[AC-config-profile-ap1] local-user 123

[AC-config-profile-ap1-luser-manage-123] password simple 321

[AC-config-profile-ap1-luser-manage-123] service-type telnet

[AC-config-profile-ap1-luser-manage-123] authorization-attribute user-role network-admin

関連コマンド

set authentication password

19.1.5 authorization-attribute

Syntax

authorization-attribute { **idle-cut** *minutes* | **user-role** *role-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } *

undo authorization-attribute { **idle-cut** | **session-timeout** | **user-role** *role-name* | **vlan** | **work-directory** } *

デフォルト

FTP、SFTP ユーザは作業ディレクトリとして NAS のルートディレクトリを設定します。しかし、ユーザはルートディレクトリへのアクセス許可がありません。

network-admin あるいは level-15 のユーザによって作成されたローカルユーザは network-operator のユーザロールが割り当てられています。

View

Configuration profile-Local user view

定義済みユーザロール

network-admin

パラメータ

idle-cut *minute*: アイドルタイムアウト時間を設定します。設定範囲は 1～120 分です。指定されるアイドル時間を超過したアイドル中のオンラインユーザはログアウトされます。

user-role *role-name*: 許可されたユーザロールを指定します。設定範囲は 1～63 です。大文字、小文字を区別します。ユーザに 64 のユーザロールを指定することができます。このオプションは local user view でのみ有効で、user group view では無効です。

vlan *vlan-id*: 許可 VLAN を指定します。設定範囲は 1～4094 です。認証にパスし、VLAN が許可されたのち、ローカルユーザは VLAN のリソースのみアクセスすることができます。

work-directory *directory-name*: FTP、SFTP ユーザの作業ディレクトリを指定します。設定範囲は 1～255 です。大文字、小文字を区別しません。このディレクトリは既に存在している必要があります。デフォルトで FTP、SFTP ユーザは装置のルートディレクトリにアクセスすることができます。

説明

authorization-attribute コマンドはローカルユーザまたはユーザグループの許可属性を設定します。ローカルユーザ、またはローカルユーザのユーザグループが認証を通過すると、装置はユーザにそれらの属性を割り当てます。

undo authorization-attribute コマンドはデフォルトに戻します。

アプリケーション環境と目的に従って許可属性を設定してください。ユーザのサービスタイプに依存して許可属性をサポートします。

SSH、Telnet、端末ユーザの場合、許可属性はアイドルカット、ユーザロール、作業ディレクトリが適用できます。

HTTP、HTTPS ユーザの場合、許可属性はユーザロールが適用できます。

FTP ユーザの場合、許可属性はアイドルカット、ユーザロール、作業ディレクトリが適用できます。

ローカルユーザのほかのタイプは適用されません。

ユーザが許可されたユーザロールのみ適用させるため、あらかじめ定義されたユーザロールを削除するために **undo authorization-attribute user-role** コマンドを使用してください。

例

コンフィグレーションプロファイル **ap1** に作成した装置管理ユーザ abc の許可される VLAN を VLAN 2 として設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] local-user abc class network

[AC-config-profile-ap1-luser-network-abc] authorization-attribute vlan 2

19.1.6 configuration profile

Syntax

configuration profile *profile-name* **[model** *model-name* **]**

undo configuration profile *profile-name*

デフォルト

設定無し

View

System view

定義済みユーザロール

network-admin

パラメータ

profile-name: コンフィグレーションプロファイルの名前を 1～64 文字の文字列で指定します。文字、数字、アンダースコア (_) 、ドット (。) 、左括弧 ([) 、右括弧 (]) 、スラッシュ (/) 、ハイフン (-) が使用可能です。大文字と小文字は区別されます。

model *model-name*: AP モデル名を指定します。このパラメータは、コンフィグレーションプロファイルを作成するときに必要です。

説明

configuration profile コマンドはコンフィグレーションプロファイルを作成し、その View に移行するか、既存のコンフィグレーションプロファイルの View に移行します。

undo configuration profile コマンドは、既存のコンフィグレーションプロファイルを削除します。

AC でコンフィグレーションプロファイルを作成し、プロファイルを 1 つまたは複数の AP に関連付けることができます。その後、AC はプロファイルで指定された設定を、関連付けられた AP がオンラインになったときに自動的に展開します。

コンフィグレーションプロファイルを作成するときは、AP モデル名を指定する必要があります。AC は、AP モデルに基づいてプロファイルにデフォルト設定を生成します。

AC には最大 2048 のコンフィグレーションプロファイルを作成することができます。

例

AP **ap1 model QX-W1130** のコンフィグレーションプロファイルを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1130

[AC-config-profile-ap1]

19.1.7 configuration-profile

メモ：

- **configuration-profile** と **remote-configuration** を同じ AP に対して設定しないでください。
- コンフィグレーションプロファイルで設定できないコマンドを設定したい場合に限り、**map-configuration** の併用をご検討ください。また、**configuration-profile** と **map-configuration** の両方に同じ機能を有するコマンド設定がある場合、AP へのコンフィグ適用が正常におこなわれません。

Syntax

configuration-profile *profile-name*

undo configuration-profile

デフォルト

設定無し

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

profile-name: コンフィグレーションプロファイルの名前を 1～64 文字の文字列で指定します。文字、数字、アンダースコア (_) 、ドット (。) 、左括弧 ([) 、右括弧 (]) 、スラッシュ (/) 、ハイフン (-) が使用可能です。大文字と小文字は区別されます。

説明

configuration-profile コマンドは、既存のコンフィグレーションプロファイルを AP または AP グループと関連付けます。

undo configuration-profile コマンドは、デフォルトに戻します。

既存のコンフィグレーションプロファイルを AP または AP グループに関連付けます。AP または AP グループ内の AP がオンラインになると、AC はプロファイル内の設定を AP に自動的に展開します。

コンフィグレーションプロファイルと AP または AP グループの関連付けを解除するには、undo configuration-profile コマンドを実行します。また、undo configuration-profile コ

マンドを実行すると、AP または AP グループ内の AP の設定が工場出荷時のデフォルトに復元されます。

例

AP **ap1 model QX-W1130** とコンフィグレーションプロファイル **profile1** を関連付けます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] configuration-profile profile1

AP グループ **apgroup1** の 型番 **QX-W1130** とコンフィグレーションプロファイル **profile1** を関連付けます。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1130

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130] configuration-profile profile1

19.1.8 dhcp enable

Syntax

dhcp enable

undo dhcp enable

デフォルト

無効

View

Configuration profile view

定義済みユーザロール

network-admin

説明

dhcp enable コマンドは DHCP を有効にします。

undo dhcp enable コマンドは DHCP を無効にします。

DHCP に関する設定は DHCP を有効にしたのち適用されます。

DHCP サーバあるいは DHCP リレーエージェントの設定を実行する前に、DHCP を有効にしてください。

例

コンフィグレーションプロファイル **ap1** の DHCP を有効にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp enable

19.1.9 dhcp relay server-address

Syntax

dhcp relay server-address *ip-address*

undo dhcp relay server-address [*ip-address*]

デフォルト

設定なし

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: DHCP サーバの IP アドレスを指定します。DHCP リレーエージェントは DHCP クライアントから受信した DHCP パケットを DHCP サーバに転送します。

説明

dhcp relay server-address コマンドは DHCP リレーエージェントの DHCP サーバを指定します。

undo dhcp relay server-address コマンドは DHCP サーバを削除します。

DHCP サーバを指定する IP アドレスは、DHCP リレーエージェントインタフェースの IP アドレスと同一のサブネット上に置くことはできません。その場合、DHCP クライアントは IP アドレスの取得に失敗します。

インタフェースで最大 8 つの DHCP サーバを指定することができます。DHCP リレーエージェントはクライアントからのパケットをすべての指定された DHCP サーバに転送します。

IP アドレスを指定しない場合、**undo dhcp relay server-address** コマンドはインタフェースのすべての DHCP サーバを削除します。

例

コンフィグレーションプロファイル **ap1** の VLAN インタフェース 10 で DHCP リレーエージェントの DHCP サーバアドレス 1.1.1.1 を指定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1130

[AC-config-profile-ap1] interface vlan-interface 10

[AC-config-profile-ap1-Vlan-interface10] dhcp relay server-address 1.1.1.1

19.1.10 dhcp select

Syntax

dhcp select { **relay** | **server** }

undo dhcp select { **relay** | **server** }

デフォルト

インタフェースは DHCP サーバモードで動作し、設定パラメータの DHCP 要求に応答します。

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

パラメータ

relay: インタフェースで DHCP リレーエージェントを有効にします。

server: インタフェースで DHCP サーバを有効にします。

説明

dhcp select コマンドはインタフェースで DHCP サーバあるいは DHCP リレーエージェントを有効にします。

undo dhcp select コマンドはインタフェースで DHCP サーバあるいは DHCP リレーエージェントを無効にします。無効にした場合、インタフェースは受信した DHCP パケットを廃棄します。

例

コンフィグレーションプロファイル **ap1** の VLAN インタフェース 2 で DHCP リレーエージェントを有効にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface vlan-interface 2

[AC-config-profile-ap1-Vlan-interface2] dhcp select relay

19.1.11 dhcp server ip-pool

Syntax

dhcp server ip-pool *pool-name*

undo dhcp server ip-pool *pool-name*

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

pool-name: アドレスプールを固有に識別するため DHCP アドレスプールの名前を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

説明

dhcp server ip-pool コマンドは DHCP アドレスプールを作成し、その view に移行します。

undo dhcp server ip-pool コマンドは指定した DHCP アドレスプールを削除します。

またコマンドを使用して既存の DHCP アドレスプールに移行することができます。

DHCP アドレスプールは DHCP クライアントに割り当てられる設定パラメータを記録するために使用されます。

例

コンフィグレーションプロファイル **ap1** に DHCP アドレスプール pool1 を作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool pool1

[AC-config-profile-ap1-dhcp-pool-pool1]

関連コマンド

- **dhcp server apply ip-pool**
- **display dhcp server pool**

19.1.12 dns-list

Syntax

dns-list *ip-address*&<1-8>

undo dns-list [*ip-address*&<1-8>]

デフォルト

設定なし

View

Configuration profile-DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-8>: DNS サーバを指定します。&<1-8>は DNS サーバのアドレスを半角スペースで区切り最大 8 つまで指定できることを示します。

説明

dns-list コマンドは DHCP アドレスプールの DNS サーバアドレスを指定します。

undo dns-list コマンドは DHCP アドレスプールの DNS サーバアドレスを削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

パラメータを指定しない場合、**undo dns-list** コマンドは DHCP アドレスプールのすべての DNS サーバのアドレスを削除します。

例

コンフィグレーションプロファイル **ap1** の DHCP アドレスプール 0 の DNS サーバアドレス 10.1.1.254 を指定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool 0

[AC-config-profile-ap1-dhcp-pool-0] dns-list 10.1.1.254

関連コマンド

display dhcp server pool

19.1.13 expired

Syntax

expired { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }

undo expired

デフォルト

1 日

View

Configuration profile-DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

day *day*: 日数を指定します。設定範囲は 0～365 日です。

hour *hour*: 時間を指定します。設定範囲は 0～23 時間です。デフォルトは 0 時間です。

minute *minute*: 分を指定します。設定範囲は 0～59 分です。デフォルトは 0 分です。

second *second*: 秒を指定します。設定範囲は 0～59 秒です。デフォルトは 0 秒です。

unlimited: リース期間を指定しません。正確には 136 年のリース期間です。

説明

expired コマンドは DHCP アドレスプールのリース期間を指定します。

undo expired コマンドは DHCP アドレスプールのリース期間をデフォルトに戻します。

DHCP サーバは DHCP クライアントにリース期間と共に IP アドレスを割り当てます。リース期間が終了する前に、DHCP クライアントはリース期間を延長する必要があります。

- リース期間の延長が成功した場合、DHCP クライアントは IP アドレスを使用し続けることができます。
- リース期間の延長が失敗したとき、以下のイベントの両方が発生します。
  - リース期間が終了した後 DHCP クライアントは IP アドレスを使用することができません。
  - DHCP サーバは終了したアドレスとして IP アドレスにラベルをつけます。

例

コンフィグレーションプロファイル **ap1** に作成した DHCP アドレスプール 0 のリース期間を 1 日、2 時間、3 分、4 秒に指定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool 0

[AC-config-profile-ap1-dhcp-pool-0] expired day 1 hour 2 minute 3 second 4

19.1.14 forbidden-ip-range

Syntax

forbidden-ip-range *start-ip-address* [*end-ip-address*]

undo forbidden-ip-range [*start-ip-address* [*end-ip-address*]]

デフォルト

設定なし

View

Configuration profile-DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

start-ip-address: 除外する IP アドレス範囲の開始アドレスを指定します

end-ip-address: 除外する IP アドレス範囲の終了アドレスを指定します

説明

forbidden-ip-range コマンドはアドレスプールのダイナミック割り当てから IP アドレス範囲を除外します。

undo forbidden-ip-range コマンドは設定を削除します。

例

コンフィグレーションプロファイル **ap1** に作成した DHCP アドレスプール 0 のダイナミック割り当てから 192.168.10.1 から 192.168.10.10 のアドレス範囲を除外します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool 1

[AC-config-profile-ap1-dhcp-pool-1] forbidden-ip-range 192.168.10.1 192.168.10.10

19.1.15 gateway-list

Syntax

gateway-list *ip-address*&<1-64>

undo gateway-list [*ip-address*&<1-64>]

デフォルト

設定なし

View

Configuration profile-DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-64>: ゲートウェイを指定します。&<1-64>はゲートウェイアドレスを半角スペースで区切り最大 64 つまで指定できることを示します。ゲートウェイアドレスは割り当て可能な IP アドレスと同一のサブネットに存在する必要があります。

説明

gateway-list コマンドは DHCP アドレスプールのゲートウェイアドレスを指定します。

undo gateway-list コマンドは DHCP アドレスプールからゲートウェイアドレスを削除します。

パラメータを指定しない場合、**undo gateway-list** コマンドはすべてのゲートウェイアドレスを削除します。

例

コンフィグレーションプロファイル **ap1** に作成した DHCP アドレスプール 0 のゲートウェイアドレスに 10.1.1.1 を指定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool 0

[AC-config-profile-ap1-dhcp-pool-0] gateway-list 10.1.1.1

19.1.16 interface

Syntax

interface *interface-type interface-number*

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

interface-type: インタフェースタイプを指定します。

interface-number: インタフェース番号を指定します。

説明

interface コマンドは interface view に移行します。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 の interface view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1]

19.1.17 interface bridge-aggregation

Syntax

interface bridge-aggregation *interface-number*

undo interface bridge-aggregation *interface-number*

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

interface-number: アグリゲートインタフェースの番号を指定します。（1 で固定です。）

説明

interface bridge-aggregation コマンドはアグリゲートインタフェースを作成し、aggregate interface view に移行します。すでにアグリゲートインタフェースが存在する場合、aggregate interface view に移行します。

undo interface bridge-aggregation コマンドはアグリゲートインタフェースを削除します。

アグリゲートインタフェースを作成したとき、システムは自動的に同一番号のアグリゲーショングループを作成します。デフォルトのアグリゲーショングループはスタティックのアグリゲーションモードです。

アグリゲートインタフェースを削除するとアグリゲートグループも削除されます。同時にアグリゲーショングループのメンバポートがアグリゲーショングループから除外されます。

例

コンフィグレーションプロファイル **ap1** にアグリゲートインタフェース Bridge-Aggregation 1 を作成し、aggregate interface view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface bridge-aggregation 1

[AC-config-profile-ap1-Bridge-Aggregation1]

19.1.18 interface vlan-interface

Syntax

interface vlan-interface *interface-number*

undo interface vlan-interface *interface-number*

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

interface-number: VLAN インタフェース番号を指定します。設定範囲は 1～4094 です。

説明

interface vlan-interface コマンドは VLAN インタフェースを作成し、作成された VLAN インタフェースの view に移行あるいは既存の VLAN インタフェースの view に移行します。

undo interface vlan-interface コマンドは VLAN インタフェースを削除します。

VLAN インタフェースを作成する前に、VLAN を作成してください。

例

コンフィグレーションプロファイル **ap1** に VLAN インタフェース 2 を作成し、作成された VLAN インタフェースの view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] vlan 2

[AC-config-profile-ap1-vlan2] quit

[AC-config-profile-ap1] interface vlan-interface 2

[AC-config-profile-ap1-Vlan-interface2]

19.1.19 ip address

Syntax

ip address *ip-address* { *mask-length* | *mask* } [**sub**]

undo ip address [*ip-address* { *mask-length* | *mask* } [**sub**]

デフォルト

設定なし

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: インタフェースの IP アドレスを指定します。ドットで区切り、10 進数で指定します。

mask-length: サブネットマスクの長さを指定します。設定範囲は 1～31 です。

mask: サブネットマスクを指定します。ドットで区切り、10 進数で指定します。

sub: インタフェースにセカンダリ IP アドレスを割り当てます。

説明

ip address コマンドはインタフェースに IP アドレスを割り当てます。

undo ip address コマンドはインタフェースから IP アドレスを削除します。

インタフェースのプライマリ IP アドレスあるいはセカンダリ IP アドレスを設定するために、このコマンドを使用します。

インタフェースは 1 つのプライマリ IP アドレスのみ設定することができます。新しく設定されたプライマリ IP アドレスは、古いアドレスを上書きします。インタフェースが複数のサブネットに接続されている場合、サブネットがインタフェースを通して通信できるように、プライマリ IP アドレスとサブネットを設定します。

BOOTP、DHCP、PPP を通して IP アドレスを取得するインタフェースはセカンダリ IP アドレスを設定することができません。

undo ip address コマンドはインタフェースからすべての IP アドレスを削除します。

undo ip address *ip-address* { *mask* | *mask-length* }コマンドはプライマリ IP アドレスを削除します。**undo ip address** *ip-address* { *mask* | *mask-length* } **sub** コマンドはセカンダリ IP アドレスを削除します。

インタフェースに割り当てたプライマリ IP アドレスとセカンダリ IP アドレスは同一ネットワークセグメント上に設定することができますが、装置の異なるインタフェースは異なるネットワークセグメント上に存在する必要があります。

例

コンフィグレーションプロファイル **ap1** に 作成した VLAN インタフェース 10 にプライマリ IP アドレスを 129.12.0.1、セカンダリ IP アドレスを 202.38.160.1、サブネットマスクを 255.255.255.0 に設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface vlan-interface 10

[AC-config-profile-ap1-Vlan-interface10] ip address 129.12.0.1 255.255.255.0

[AC-config-profile-ap1-Vlan-interface10] ip address 202.38.160.1 255.255.255.0 sub

19.1.20 ip address dhcp-alloc

Syntax

ip address dhcp-alloc

undo ip address dhcp-alloc

デフォルト

設定なし

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

説明

ip address dhcp-alloc コマンドは DHCP を使用して IP アドレスを取得するインタフェースを設定します。

undo ip address dhcp-alloc コマンドはインタフェースで DHCP の使用を停止します。

undo ip address dhcp-alloc コマンドを実行すると、インタフェースは DHCP を通して取得した IP アドレスをリリースするため、DHCP-RELEASE メッセージを送信します。インタフェースがダウンしている場合、メッセージを送信することができません。

例

コンフィグレーションプロファイル **ap1** の VLAN インタフェース 10 に、 DHCP を使用して IP アドレスを取得する設定をします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface vlan-interface 10

[AC-config-profile-ap1-Vlan-interface10] ip address dhcp-alloc

19.1.21 ip route-static

Syntax

ip route-static *dest-address* { *mask-length* | *mask* } *next-hop-address*

undo ip route-static *dest-address* { *mask-length* | *mask* } [*next-hop-address*]

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

dest-address: スタティックルートの宛先アドレスを指定します。ドットで区切り、10 進数で指定します。

mask-length: IP アドレスのマスク長を指定します。設定範囲は 0～32 です。

mask: IP アドレスのマスクを指定します。ドットで区切り、10 進数で指定します。

next-hop-address: ネクストホップの IP アドレスを指定します。ドットで区切り、10 進数で指定します。詳細はオペレーションマニュアルのセクション 6 *ルーティングプロトコル “スタティックルーティング”* を参照してください。

説明

ip route-static コマンドはスタティックルートを設定します。

undo ip route-static コマンドはスタティックルートを削除します。

宛先アドレスとマスクの両方が 0.0.0.0（あるいは 0）である場合、設定されたルートはデフォルトルートです。デフォルトルートはルーティングテーブルに一致するエントリがないパケットを転送するのに使用されます。

例

コンフィグレーションプロファイル **ap1** に宛先アドレスが 1.1.1.1/24、ネクストホップが 2.2.2.2、のスタティックルートを設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] ip route-static 1.1.1.1 24 2.2.2.2

19.1.22 line

Syntax

line { **console** | **vty** } *first-number* [*last-number*] }

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

console *first-number*: first console line の相対番号を指定します。

vty *first-number*: first VTY line の相対番号を指定します（0～63）。

vty *last-number*: last VTY user line の相対番号を指定します（1～63）。*first-number* よりも小さくすることはできません。

説明

line コマンドは 1 つ以上の user line view に移行します。

シングル user line に設定を行うために、このコマンドを使用して user line view に移行します。

同じ設定を複数の user line に行うために、このコマンドを使用して複数の user line view に移行します。

例

コンフィグレーションプロファイル **ap1** の user line Console 0 の view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1130

[AC-config-profile-ap1] line console 0

[AC-config-profile-ap1-line-console0]

コンフィグレーションプロファイル **ap1** の user lines VTY 0～VTY 4 の view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1130

[AC-config-profile-ap1] line vty 0 4

[AC-config-profile-ap1-line-vty0-4]

関連コマンド

line class

19.1.23 line class

Syntax

line class { **console** | **vty** }

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

console: console line class view を指定します。

vty: VTY line class view を指定します。

説明

line class コマンドは user line class view に移行します。

line class のすべての user line で設定を同一にするために、user line class view に移行します。

user line class view では以下のコマンドを実行することができます。

- **authentication-mode**
- **set authentication password**

いくつかのログインコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定は user line で適用されます。user line class view の設定は class のすべての user line で適用されます。
- user line view と user line class view のどちらかの view でデフォルトでない設定がある場合、デフォルトでない設定は、もう一方のデフォルト設定よりも優先されます。user line view のデフォルトでない設定は user line class view のデフォルトでない設定よりも優先されます。
- user line view の設定はすぐに適用され、オンラインユーザに影響します。user line class view の設定は設定が完了したのちにログインしたユーザのみ適用されます。user line class view の設定はオンラインユーザに影響しません。

例

コンフィグレーションプロファイル **ap1** の VTY line class view で認証モードを none にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] line class vty

[AC-config-profile-ap1-line-class-vty] authentication-mode none

関連コマンド

line

19.1.24 local-user

Syntax

local-user *user-name* [**class manage**]

undo local-user { *user-name* **class manage** | **all** [**service-type** { **ftp** | **http** | **https | ssh** | **telnet** | **terminal** } | **class manage**] }

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

user-name *user-name*: ローカルユーザ名を指定します。設定範囲は 1～55 です。大文字、小文字を区別します。

- ドメイン名を含めることはできません。
- スラッシュ（/），バックスラッシュ、垂直バー（|）、コロン（:）、アスタリスク（*）、クエスチョンマーク（?）、小なり記号（<）、大なり記号（>）、アットマーク（@）
- （a）、（al）、（all）は使用できません。

class: ローカルユーザタイプを指定します。指定しない場合、装置管理ユーザを指定します。

- **manage**: 装置管理ユーザを指定します。装置管理ユーザは FTP、HTTP、HTTPS、SSH、Telnet、端末サービスを使用することができます。

all: すべてのユーザを指定します。

service-type: ローカルユーザの使用するサービスタイプを指定します。

- **ftp**: FTP ユーザを指定します。
- **http**: HTTP ユーザを指定します。
- **https**: HTTPS ユーザを指定します。
- **ssh**: SSH ユーザを指定します。
- **telnet**: Telnet ユーザを指定します。
- **terminal**: コンソールポートを使用してログインする端末ユーザを指定します。

説明

local-user コマンドはローカルユーザを追加し、local user view に移行します。

undo local-user コマンドはローカルユーザを削除します。

Configuration profile view では装置管理ユーザのみ作成することができ、最大 16 の装置管理ユーザが作成することができます。

例

コンフィグレーションプロファイル **ap1** に装置管理ユーザ user1 を追加し、local user view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] local-user user1 class manage

[AC-config-profile-ap1-luser-manage-user1]

関連コマンド

service-type

19.1.25 nat address-group

Syntax

nat address-group *group-id* [**name** *group-name*]

undo nat address-group *group-id*

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

group-id : NAT アドレスグループの ID を指定します。この引数の値の範囲は 0 から 65535 です。

name *group-name*: NAT アドレスグループに名前を割り当てます。*group-name* 引数は、1~63 文字のストリングで、大文字と小文字が区別されます。

説明

nat address-group コマンドは NAT アドレスグループを作成し、そのビューを移行するか、または既存の NAT アドレスグループのビューを移行します。

undo nat address-group コマンドは NAT アドレスグループを削除します。

NAT アドレスグループは、アドレス範囲のセットです。address コマンドを使用して、NAT アドレスグループにアドレス範囲を追加します。ダイナミック NAT は、パケットの送信元 IP アドレスをアドレスグループ内の IP アドレスに変換します。

例

コンフィグレーションプロファイル **ap1** に番号が 1 で名前が abc の NAT アドレスグループを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] nat address-group 1 name abc

関連コマンド

- **address**
- **nat inbound**
- **nat outbound**

19.1.26 nat inbound

Syntax

nat inbound { *ipv4-acl-number* | **name** *ipv4-acl-name* } **address-group** { *group-id* | **name** *group-name* } [**no-pat** [**reversible**] [**add-route**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*] [**counting**]

undo nat inbound { *ipv4-acl-number* | **name** *ipv4-acl-name* }

デフォルト

設定なし

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

パラメータ

ipv4-acl-number: 2000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、すべてを指定することはできません。

address-group: アドレス変換のアドレスグループを指定します。

group-id: アドレスグループ ID を指定します。この引数の値の範囲は 0 から 65535 です。

name *group-name*: アドレスグループ名を指定します。1~63 文字で、大文字と小文字は区別されません。

no-pat: NO-PAT モードを使用します。このキーワードを指定しない場合は、PAT が使用されます。PAT では、TCP、UDP、および ICMP クエリーパケットだけがサポートされます。ICMP パケットの場合、送信元ポート番号として ICMP ID が使用されます。

reversible: 逆アドレス変換をイネーブルにします。逆アドレス変換は、既存の NO-PAT エントリを使用して、内部ネットワークからアクティブに開始された接続の宛先アドレスを外部ネットワークに変換します。

add-route: 変換後に自動的に送信元アドレスにルートを追加します。出力インタフェースは NAT インタフェースで、ネクストホップは変換前の送信元アドレスです。

rule *rule-name*: ルールの名前を指定します。大文字と小文字が区別され、1~63 文字のストリングで指定します。バックスラッシュ (¥) 、スラッシュ (/) 、コロン (:) 、アスタリスク (*) 、疑問符 (?) 、左かぎかっこ (<) 、右かぎかっこ (>) 、縦棒 (|) 、引用符 (") 、またはアット記号 (@) です。このオプションを指定しない場合、規則に名前はありません。

priority *priority*: ルールのプライオリティを 0~2147483647 の範囲で指定します。値が小さいほど、優先順位が高くなります。このオプションを指定しない場合、同じタイプの NAT 規則の中で優先順位が最も低くなります。

disable: 受信ダイナミック NAT ルールを無効にします。このキーワードを指定しない場合、ルールは有効になります。

description *text*: 受信ダイナミック NAT ルールの説明を指定します。text 引数は、大文字と小文字を区別しない 1~63 文字の文字列です。

counting: NAT カウントを有効にします。アドレスマッピングを使用するフローの数がカウントされます。

説明

nat inbound コマンドは受信ダイナミック NAT ルールを設定します。

undo nat inbound コマンドは受信ダイナミック NAT ルールを削除します。

受信ダイナミック NAT は、ACL によって許可された受信パケットの送信元 IP アドレスをアドレスグループ内の IP アドレスに変換します。

受信ダイナミック NAT は、次のモードをサポートします。

- [PAT] :IP アドレス変換とポート変換の両方を実行します。
- [NO-PAT] :IP アドレス変換だけを実行します。

NO-PAT モードでは、逆アドレス変換がサポートされます。逆アドレス変換では、ACL 逆マッチングを使用して、変換するパケットを識別します。ACL リバースマッチングは次のように機能します。

- パケットの送信元 IP アドレス/ポートと ACL 内の宛先 IP アドレス/ポートを比較します。
- 一致する NO-PAT エントリに従ってパケットの宛先 IP アドレスを変換し、変換された宛先 IP アドレス/ポートを ACL 内の送信元 IP アドレス/ポートと比較します。

受信ダイナミック NAT は通常、次のいずれかと連携して双方向 NAT を実装します。

- 送信ダイナミック NAT (nat outbound コマンド) 。
- NAT Server (nat server コマンド) 。
- 送信スタティック NAT (nat static コマンド) 。

アドレスグループは、nat inbound コマンドと nat outbound コマンドの両方で使用できません。nat inbound コマンドでは、PAT モードと NO-PAT モードの両方で使用できません。

内部ネットワークと外部ネットワークが存在するサブネットが重複している場合は、add-route キーワードを指定しないでください。その他のネットワークシナリオの場合:

- add-route キーワードを指定すると、デバイスはパケットの変換後に自動的に送信元アドレスにルートを追加します。宛先アドレスは NAT アドレスグループ内の NAT アドレス、出力インタフェースはコマンドが実行されるインタフェース、ネクストホップは変換前の送信元アドレスです。
- add-route キーワードを指定しない場合は、ルートを手動で追加する必要があります。自動ルート追加は低速であるため、手動でルートを追加することをお勧めします。

ACL は、インタフェース上の 1 つの受信ダイナミック NAT ルールだけで使用できます。

1 つのインタフェースに複数の受信ダイナミック NAT ルールを設定できます。

同じプライオリティ値で設定された受信ダイナミック NAT ルールは、その ACL を使用して照合されます。

- 名前付き ACL を持つ NAT ルールは、名前なし ACL を持つ NAT ルールよりも優先順位が高くなります。
- 名前付き ACL を持つ NAT ルールは、ACL 名のアルファベット順に照合されます。
- 名前なし ACL を持つ NAT ルールは、ACL 番号の降順で照合されます。

例

コンフィグレーションプロファイル **ap1** にサブネット 10.110.10.0/24 からのパケットだけを通過させる、ACL 2001 を設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl basic 2001

[AC-config-profile-ap1-acl-ipv4-basic-2001] rule permit source 10.110.10.0 0.0.0.255

[AC-config-profile-ap1-acl-ipv4-basic-2001] rule deny

[AC-acl-ipv4-basic-2001] quit

コンフィグレーションプロファイル **ap1** にアドレスグループ 1 を作成し、アドレス範囲 202.110.10.10~202.110.10.12 をグループに追加します。

[AC-config-profile-ap1] nat address-group 1

[AC-config-profile-ap1-address-group-1] address 202.110.10.10 202.110.10.12

[AC-config-profile-ap1-address-group-1] quit

#インバウンド NO-PAT ルールを# コンフィグレーションプロファイル **ap1** のインタフェース VLAN インタフェース 10 に設定します。NAT は、受信パケットの送信元アドレスをアドレスグループ 1 のアドレスに変換し、変換されたパケットのルートを自動的に追加します。ルール名を abc に、優先順位を 0 に設定します。

[AC-config-profile-ap1] interface vlan-interface 10

[AC-config-profile-ap1-Vlan-interface10] nat inbound 2001 address-group 1 no-pat add-route rule abc priority 0

19.1.27 nat outbound

Syntax

NO-PAT:

nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*] **address-group** { *group-id* | **name** *group-name* } **no-pat** [**reversible**] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*] [**counting**]

undo nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*]

PAT:

nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*] [**address-group** { *group-id* | **name** *group-name* }] [**port-preserved**] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** text] [**counting**]

undo nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*]

デフォルト

設定なし

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

パラメータ

ipv4-acl-number: ipv 4-acl-number:2000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、all を指定することはできません。

address-group: NAT のアドレスグループを指定します。アドレスグループを指定しない場合、インタフェースの IP アドレスが NAT アドレスとして使用されます。Easy IP が使用されている。

group-id: アドレスグループ ID を指定します。この引数の値の範囲は 0 から 65535 です。

name *group-name*: アドレスグループ名を指定します。1~63 文字で、大文字と小文字は区別されません。

no-pat: NO-PAT モードを使用します。このキーワードを指定しない場合は、PAT が使用されます。PAT では、TCP、UDP、および ICMP クエリーパケットだけがサポートされます。ICMP パケットの場合、送信元ポート番号として ICMP ID が使用されます。

reversible: 逆アドレス変換を有効にします。逆アドレス変換では、既存の NO-PAT エントリを使用して、外部ネットワークからアクティブに開始された接続の宛先アドレスを内部ネットワークに変換します。

port-preserved: PAT のポート番号を保持しようとします。このキーワードは、ダイナミック NAT ポートブロックマッピングでは有効になりません。

rule *rule-name*: ルールの名前を指定します。大文字と小文字が区別され、1~63 文字のストリングで指定します。バックスラッシュ (¥) 、スラッシュ (/) 、コロン (:) 、アスタリスク (*) 、疑問符 (?) 、左かぎかっこ (<) 、右かぎかっこ (>) 、縦棒 (|) 、引用符 (") 、またはアット記号 (@) です。このオプションを指定しない場合、規則に名前はありません。

priority *priority*: ルールのプライオリティを 0~2147483647 の範囲で指定します。値が小さいほど、優先順位が高くなります。このオプションを指定しない場合、同じタイプの NAT 規則の中で優先順位が最も低くなります。

disable: 送信ダイナミック NAT ルールを無効にします。このキーワードを指定しない場合、ルールは有効になります。

description *text*: 送信ダイナミック NAT ルールの説明を指定します。text 引数は、大文字と小文字を区別しない 1~63 文字の文字列です。

counting: NAT カウントを有効にします。アドレスマッピングを使用するフローの数がカウントされます。

説明

nat outbound コマンドは送信ダイナミック NAT 規則を設定します。

undo nat outbound コマンドは送信ダイナミック NAT 規則を削除します。

送信ダイナミック NAT は通常、外部ネットワークに接続されたインタフェースで設定されます。1 つのインタフェースに複数の送信ダイナミック NAT ルールを設定できます。

送信ダイナミック NAT は、次のモードをサポートします。

- PAT :IP アドレス変換とポート変換の両方を実行します。PAT モードでは、エンドポイントに依存しないマッピング動作が使用されている場合、外部ホストは内部ホストにアクティブにアクセスできます。
- NO-PAT :IP アドレス変換だけを実行します。reversible キーワードを指定した場合、NO-PAT モードでは、外部ホストが内部ホストにアクティブにアクセスできます。ACL が指定されている場合、リバースアドレス変換は ACL リバースマッチングで許可されたパケットだけに適用されます。ACL リバースマッチングは次のように機能します。
  - □ パケットの送信元 IP アドレス/ポートと ACL 内の宛先 IP アドレス/ポートを比較します。
  - □ 一致する NO-PAT エントリに従ってパケットの宛先 IP アドレスを変換し、変換された宛先 IP アドレス/ポートを ACL 内の送信元 IP アドレス/ポートと比較します。

ダイナミック NAT 444 は、NO-PAT モードをサポートしません。

NAT アドレスグループを指定する場合は、次の制約事項および注意事項に従ってください。

- アドレスグループは、nat inbound コマンドと nat outbound コマンドの両方で使用できません。
- nat outbound コマンドでは、PAT モードと NO-PAT モードの両方でアドレスグループを使用できません。
- NAT アドレスグループでポートブロックパラメータが指定されている場合、このコマンドはダイナミック NAT ポートブロックマッピングを設定します。ACL 許可ルールに一致するパケットは、ダイナミック NAT 444 によって処理されます。

ACL を指定する場合は、次の制約事項および注意事項に従ってください。

- ACL は、インタフェース上の 1 つの送信ダイナミック NAT ルールだけで使用できます。
- ACL を指定すると、NAT は ACL によって許可された送信パケットの送信元 IP アドレスをアドレスグループの IP アドレスに変換します。ACL を指定しない場合、NAT はすべてのパケットを変換します。
- インタフェースに ACL が設定されている送信ダイナミック NAT ルールは、ACL が設定されていないルールよりも優先されます。ACL ベースのダイナミック NAT ルールが 2 つ設定されている場合、ACL 番号が大きい方のルールのプライオリティが高くなります。

同じプライオリティ値で設定された送信ダイナミック NAT ルールと ACL は、ルール内の ACL を使用して照合されます。

- 名前付き ACL を持つ NAT ルールは、名前なし ACL を持つ NAT ルールよりも優先順位が高くなります。
- 名前付き ACL を持つ NAT ルールは、ACL 名のアルファベット順に照合されます。
- 名前なし ACL を持つ NAT ルールは、ACL 番号の降順で照合されます。

例

コンフィグレーションプロファイル **ap1** にサブネット 10.110.10.0/24 からのパケットだけを通過させる、ACL 2001 を設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl basic 2001

[AC-config-profile-ap1-acl-ipv4-basic-2001] rule permit source 10.110.10.0 0.0.0.255

[AC-config-profile-ap1-acl-ipv4-basic-2001] rule deny

[AC-config-profile-ap1-acl-ipv4-basic-2001] quit

コンフィグレーションプロファイル **ap1** にアドレスグループ 1 を作成し、アドレス範囲 202.110.10.10~202.110.10.12 をグループに追加します。

[AC-config-profile-ap1] nat address-group 1

[AC-config-profile-ap1-address-group-1] address 202.110.10.10 202.110.10.12

[AC-config-profile-ap1-address-group-1] quit

コンフィグレーションプロファイル **ap1** のインタフェース VLAN インタフェース 10 に送信ダイナミック PAT ルールを設定して、ACL 2001 で許可された送信パケットの送信元アドレスをアドレスグループ 1 のアドレスに変換します。

[AC-config-profile-ap1] interface vlan-interface 10

[AC-config-profile-ap1-Vlan-interface10] nat outbound 2001 address-group 1

[AC-config-profile-ap1-Vlan-interface10] quit

コンフィグレーションプロファイル **ap1** のインタフェース VLAN インタフェース 10 に送信 NO-PAT ルールを設定して、ACL 2001 で許可された送信パケットの送信元アドレスをアドレスグループ 1 のアドレスに変換します。

[AC-config-profile-ap1] interface vlan-interface 10

[AC-config-profile-ap1-Vlan-interface10] nat outbound 2001 address-group 1 no-pat

[AC-config-profile-ap1-Vlan-interface10] quit

#VLAN インタフェース 10 の IP アドレスを変換後のアドレスとして使用するには、Easy IP を有効にします。

[AC-config-profile-ap1] interface Vlan-interface 10

[AC-config-profile-ap1-Vlan-interface10] nat outbound 2001

[AC-config-profile-ap1-Vlan-interface10] quit

#VLAN インタフェース 10 で送信 NO-PAT ルールを設定して、ACL 2001 で許可された送信パケットの送信元アドレスをアドレスグループ 1 のアドレスに変換します。逆アドレス変換を有効にします。

[AC-config-profile-ap1] interface Vlan-interface 10

[AC-config-profile-ap1-Vlan-interface10] nat outbound 2001 address-group 1 no-pat reversible

19.1.28 network

Syntax

network *network-address* [*mask-length* | **mask** *mask*]

undo network *network-address* [*mask-length* | **mask** *mask*]

デフォルト

設定なし

View

Configuration profile-DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

network-address: ダイナミック割り当てのサブネットを指定します。マスク長やマスクが指定されない場合、ナチュラルマスクが使用されます。

mask-length: マスク長を指定します。設定範囲は 1～30 です。

mask *mask*: ドットで区切られた形式でマスクを指定します。

説明

network コマンドは DHCP アドレスプールのダイナミック割り当てのサブネットを指定します。

undo network コマンドは指定されたサブネットを削除します。

DHCP アドレスプールで 1 つのプライマリサブネットのみを指定することができます。コマンドを複数回設定した場合、最後に行った設定が適用されます。

ネットワークの設定の変更あるいは削除を行うと現在のアドレスプールから割り当てられたアドレスを削除します。

例

コンフィグレーションプロファイル **ap1** に作成した DHCP アドレスプール 0 のサブネットとして 192.168.8.0/24 を指定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool 0

[AC-config-profile-ap1-dhcp-pool-0] network 192.168.8.0 mask 255.255.255.0

関連コマンド

gateway-list

19.1.29 packet-filter

Syntax

packet-filter [mac] { *acl-number* **| name** *acl-name* **} { inbound | outbound }**

undo packet-filter [mac] { *acl-number* **| name** *acl-name* **} { inbound | outbound }**

デフォルト

設定なし

View

Configuration profile- interface view

定義済みユーザロール

network-admin

パラメータ

mac: L2 ACL を指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。

name *acl-name*: ACL を識別しやすくするため、ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。混乱を避けるため、**all** は使用できません。

inbound: インタフェースで受信されるパケットをフィルタリングします。

outbound: インタフェースで送信されるパケットをフィルタリングします。

説明

packet-filter コマンドはパケットをフィルタするため、インタフェースに ACL を適用します。

undo packet-filter コマンドはインタフェースから ACL を削除します。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 に受信トラフィックをフィルタするため、標準 IPv4 ACL 2001 を適用します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] packet-filter 2001 inbound

19.1.30 password

Syntax

password [{ **hash** | **simple** } *string*]

undo password

デフォルト

ローカルユーザのパスワードは設定されていません。正しいユーザ名を入力し、属性の確認を行った後、認証にパスできます。

View

Configuration profile-Local user view

定義済みユーザロール

network-admin

パラメータ

cipher: 暗号テキストのパスワードを設定します。

hash: ハッシュパスワードを設定します。

simple: プレーンテキストのパスワードを設定します。セキュリティのため、プレーンテキストで設定されたパスワードを含めたすべてのパスワードは、暗号化されて保存されます。

string: パスワードを指定します。大文字、小文字を区別します。

- ハッシュテキストのパスワードは 1～110 文字です。
- プレーンテキストのパスワードは 1～63 文字です。

🕮 **メモ：**

string は以下の要件を満たす文字列にしてください。

- 10 文字以上。
- アルファベット、数字、記号のうち 2 種類以上を含む。
- ユーザ名またはユーザ名の逆の文字を含まない。

説明

password コマンドはローカルユーザのパスワードを設定します。

undo password コマンドはローカルユーザのパスワードを削除します。

プレーンテキストパスワードとハッシュパスワードをサポートします。

例

コンフィグレーションプロファイル **ap1** に 装置管理ユーザ user1 のパスワード 123456TESTplat&!をプレーンテキストで設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] local-user user1 class manage

[AC-config-profile-ap1-luser-manage-user1] password simple 123456TESTplat&!

19.1.31 port access vlan

Syntax

port access vlan *vlan-id*

undo port access vlan

デフォルト

すべてのアクセスポートは VLAN1 に所属しています。

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を指定します。設定範囲は 1～4094 です。

説明

port access vlan コマンドはアクセスポートを指定した VLAN に割り当てます。

undo port access vlan コマンドはデフォルトに戻します。

アクセスポートを VLAN に割り当てる前に、VLAN が作成されていることを確認してください。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 に VLAN 3 を割り当てます。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] vlan 3

[AC-config-profile-ap1-vlan3] quit

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port access vlan 3

19.1.32 port hybrid pvid

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

デフォルト

リンクタイプがアクセスであるとき、ハイブリッドポートの PVID はポートが所属している VLAN の ID です。

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を指定します。設定範囲は 1～4094 です。

説明

port hybrid pvid コマンドはハイブリッドポートの PVID を設定します。

undo port hybrid pvid コマンドはハイブリッドポートの PVID を 1 に設定します。

ハイブリッドポートの PVID として存在しない VLAN を使用することができます。**undo vlan** コマンドでハイブリッドポートの PVID を削除する場合、ポートの PVID の設定は適用されません。

ローカルとリモートのハイブリッドポートに同じ PVID を設定することを推奨します。

PVID からのパケットの転送を許可するためにハイブリッドポートの設定に **port hybrid pvid** コマンドを使用してください。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 をハイブリッドポートに設定します。PVID を VLAN 100 に設定し、GigabitEthernet 1/0/1 に VLAN 100 をタグ無しメンバとして割り当てます。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] vlan 100

[AC-config-profile-ap1-vlan100] quit

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port link-type hybrid

[AC-config-profile-ap1-GigabitEthernet1/0/1] port hybrid pvid vlan 100

[AC-config-profile-ap1-GigabitEthernet1/0/1] port hybrid vlan 100 untagged

関連コマンド

- **port hybrid vlan**
- **port link-type**

19.1.33 port hybrid vlan

Syntax

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

デフォルト

リンクタイプがアクセスであるとき、ハイブリッドポートはポートが所属している VLAN のタグなしメンバです。

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN ID の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* **to** *vlan-id2* です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

tagged: ポートは VLAN タグを削除しないで指定した VLAN のパケットを送信するように設定します。

untagged: ポートは VLAN タグを削除したのち、指定した VLAN のパケットを送信するように設定します。

説明

port hybrid vlan コマンドは指定した VLAN にハイブリッドポートを割り当てます。

undo port hybrid vlan コマンドは指定した VLAN からハイブリッドポートを削除します。

ハイブリッドポートは、複数の VLAN が通過できます。**port hybrid vlan** コマンドを繰り返し実行すると、ハイブリッドポートを通過する VLAN は、各実行の *vlan-id-list* により指定された VLAN に設定されます。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 をハイブリッドポートに設定します。VLAN 2、VLAN 4 および VLAN 50～VLAN 100 に割り当て、これらの VLAN のパケットにタグを付けて送信するよう GigabitEthernet 1/0/1 に設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port link-type hybrid

[AC-config-profile-ap1-GigabitEthernet1/0/1] port hybrid vlan 2 4 50 to 100 tagged

関連コマンド

port link-type

19.1.34 port link-aggregation group

Syntax

port link-aggregation group *number*

undo port link-aggregation group

デフォルト

設定なし

View

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

number: アグリゲーショングループに対応するアグリゲートインタフェースの数を指定します。（1 で固定です。）

説明

port link-aggregation group コマンドは指定したアグリゲーショングループにインタフェースを割り当てます。

undo port link-aggregation group コマンドは所属しているアグリゲーショングループからインタフェースを削除します。

インタフェースは 1 つのアグリゲーショングループのみ所属することができます。

例

コンフィグレーションプロファイル **ap1** の アグリゲーショングループ 1 に GigabitEthernet 1/0/1 を割り当てます。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port link-aggregation group 1

19.1.35 port link-type

Syntax

port link-type { **access** | **hybrid** | **trunk** }

undo port link-type

デフォルト

access

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

access: ポートのリンクタイプをアクセスとして指定します。

hybrid: ポートのリンクタイプをハイブリッドとして指定します。

trunk: ポートのリンクタイプをトランクとして指定します。

説明

port link-type コマンドはポートのリンクタイプを設定します。

undo port link-type コマンドはデフォルトに戻します。

トランクポートからハイブリッドポート（またはその逆）のリンクタイプを変更するには、まずリンクタイプをアクセスに設定する必要があります。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 のリンクタイプをトランクポートに設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port link-type trunk

19.1.36 port trunk permit vlan

Syntax

port trunk permit vlan { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

デフォルト

トランクポートは VLAN 1 からのパケットのみ通過できるように許可します。

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: インタフェースを指定します。半角スペースで区切り 10 まで設定するか、VLAN ID の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* **to** *vlan-id2* です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: すべての VLAN を通過できるように許可します。許可されていない VLAN ユーザがポートを通して制限されたリソースにアクセスすることを防ぐため､注意して **port trunk permit vlan all** コマンドを使用してください。

説明

port trunk permit vlan コマンドはトランクポートを指定した VLAN に割り当てます。

undo port trunk permit vlan コマンドはトランクポートを指定した VLAN から削除します。

トランクポートは複数の VLAN を通過できます。**port trunk permit vlan** コマンドを繰り返し実行すると、トランクポートを通過する VLAN は、各 *vlan-id-list* により指定された VLAN に設定されます。

トランクポート上では、PVID のトラフィックのみタグなしで通過することができます。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 をトランクポートに設定します。VLAN 2、VLAN 4 および VLAN 50～VLAN 100 に割り当てます。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port link-type trunk

[AC-config-profile-ap1-GigabitEthernet1/0/1] port trunk permit vlan 2 4 50 to 100

関連コマンド

port link-type

19.1.37 port trunk pvid

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

デフォルト

VLAN 1

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を指定します。設定範囲は 1～4094 です。

説明

port trunk pvid コマンドはトランクポートの PVID を設定します。

undo port trunk pvid コマンドはデフォルトに戻します。

トランクポートの PVID として存在しない VLAN を使用することができます。**undo vlan** コマンドを使用してトランクポートの PVID を削除しても、ポートの PVID の設定には影響しません。

ローカルおよびリモートのトランクポートは、PVID のトラフィックが正常に送信されるために同じ PVID を使用する必要があります。

PVID からのパケットの転送を許可するためにトランクポートの設定に **port trunk permit vlan** コマンドを使用してください。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 をトランクポートに設定します。PVID を VLAN 100 に設定し、GigabitEthernet 1/0/1 に VLAN 100 を割り当てます。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port link-type trunk

[AC-config-profile-ap1-GigabitEthernet1/0/1] port trunk pvid vlan 100

[AC-config-profile-ap1-GigabitEthernet1/0/1] port trunk permit vlan 100

関連コマンド

- **port link-type**
- **port trunk permit vlan**

19.1.38 port-isolate enable

Syntax

port-isolate enable

undo port-isolate enable

デフォルト

Layer2 Ethernet interface view では、ポートアイソレーションは有効です。

Layer2 Aggregate interface view では、ポートアイソレーションは無効です。

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

port-isolate enable コマンドはポートアイソレーションを有効にします。

undo port-isolate コマンドはポートアイソレーションを無効にします。

Ethernet interface view での設定は、そのインタフェースにのみ適用されます。

aggregate interface view での設定は、アグリゲートインタフェースとアグリゲーションメンバポートに適用されます。装置がアグリゲートインタフェースへの設定の適用に失敗した場合、装置はどのアグリゲーションメンバポートもアイソレーショングループに割り当てません。設定の適用失敗がアグリゲーションメンバポートで起きた場合、装置は失敗が起きたポートをスキップし、別のアグリゲーションメンバポートをアイソレーショングループに割り当てます。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 でポートアイソレーションを有効にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port-isolation enable

コンフィグレーションプロファイル **ap1** のアグリゲートインタフェース Bridge-Aggregation 1 でポートアイソレーションを有効にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface Bridge-Aggregation 1

[AC-config-profile-ap1-Bridge-Aggregation-1] port-isolate enable

19.1.39 qos priority

Syntax

qos priority *priority-value*

undo qos priority

デフォルト

0

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

パラメータ

priority-value: ポートプライオリティの値を指定します。設定範囲は 0～7 です。

説明

qos priority コマンドはインタフェースのポートプライオリティを変更します。

undo qos priority コマンドはデフォルトに戻します。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 のポートプライオリティを 2 に設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface gigabitethernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] qos priority 2

19.1.40 qos trust

Syntax

qos trust { **dot1p** | **dscp** }

undo qos trust

デフォルト

インタフェースはパケットのプライオリティを信用しません。802.1p プライオリティとしてポートプライオリティを使用します。

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

パラメータ

dot1p: プライオリティマッピングの受信パケットの 802.1p プライオリティを使用します。

dscp: プライオリティマッピングの受信パケットの DSCP を使用します。

説明

qos trust コマンドはインタフェースのプライオリティトラステッドモードを設定します。

undo qos trust コマンドはデフォルトのプライオリティのトラステッドモードに戻します。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 のプライオリティトラステッドモードを 802.1p プライオリティに設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface gigabitethernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] qos trust dot1p

19.1.41 rule (IPv4 advanced ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **destination** | **destination-port** | { **dscp** | { **precedence** | **tos** } * } | **fragment** | **icmp-type** | **source** | **source-port** | **time-range**] *

undo rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **source** { *source-address source-wildcard* | **any** } | **source-port** | **time-range** *time-range-name*] *

デフォルト

設定なし

View

Configuration profile-IPv4 advanced ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当て

ます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

protocol: プロトコル番号あるいはプロトコル名を指定します。

- プロトコル番号の設定範囲は 0～255 です。
- プロトコル名は **gre** (47)、**icmp** (1)、**igmp** (2)、**ip**、**ipinip** (4)、**ospf** (89)、**tcp** (6)、**udp** (17)を指定できます。**ip** はすべてのプロトコルを指定します。表 19-1 にプロトコルの値に関わらず指定できるパラメータを示します。

表 19-1 拡張 IPv4 ACL ルールの一致基準と他のルールの情報

パラメータ	機能	説明
source { *source-address source-wildcard* | **any** }	送信元アドレスを定義します。	*source-address*と*source-wildcard*はドットで区切られた10進数表記の送信元IPアドレスとワイルドカードマスクを示します。すべてが0のワイルドカードはホストアドレスを示します。 **any**は、任意の送信元IPアドレスを示します。
destination { *dest-address dest-wildcard* | **any** }	宛先アドレスを定義します。	*dest-address*と*dest-wildcard*はドットで区切られた10進数表記の宛先IPアドレスとワイルドカードマスクを示します。すべてが0のワイルドカードはホストアドレスを示します。 **any**は、任意の宛先IPアドレスを示します。
precedence *precedence*	IPプレシーデンスの値を指定します。	プレシーデンスの値あるいはプレシーデンスの名前を指定します。番号の設定範囲は0～7です。名前は**routine** (0)、**priority** (1)、**immediate** (2)、**flash** (3)、**flash-override** (4)、**critical** (5)、**internet** (6)、**network** (7)が指定できます。
tos *tos*	ToSプレシーデンスを指定します。	プレシーデンスの値あるいはプレシーデンスの名前を指定します。番号の設定範囲は0～15です。名前は**max-reliability** (2)、**max-throughput** (4)、**min-delay** (8)、**min-monetary-cost** (1)、**normal** (0)が指定できます。

パラメータ	機能	説明
dscp *dscp*	DSCPプライオリティを指定します。	*dscp*プライオリティの値あるいはプライオリティの名前を指定します。番号の設定範囲は0～63です。名前は**af11** (10)、**af12** (12)、**af13** (14)、**af21** (18)、**af22** (20)、**af23** (22)、**af31** (26)、**af32** (28)、**af33** (30)、**af41** (34)、**af42** (36)、**af43** (38)、**cs1** (8)、**cs2** (16)、**cs3** (24)、**cs4** (32)、**cs5** (40)、**cs6** (48)、**cs7** (56)、**default** (0)、**ef** (46)が指定できます。
fragment	最初のフラグメントではないフラグメントを指定します。	指定しない場合、ルールはすべてのフラグメントと非フラグメントを適用します。
time-range *time-range-name*	ルールのタイムレンジを指定します。	*time-range-name*の設定範囲は1～32文字です。大文字、小文字を区別しません。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション8 *ACL and QoS* *“タイムレンジ”*を参照してください。

protocol が **tcp** (6)あるいは **udp** (17)である場合、設定するパラメータを表 19-2 に示します。

表 19-2 拡張 IPv4 ACL ルールの TCP/UDP 指定パラメータ

パラメータ	機能	説明
source-port *operator port1* [*port2*]	1つまたは複数のTCP/UDPの送信元ポート番号を指定します。	*operator*は**lt** (lower than)、**gt** (greater than)、**eq** (equal to)、**neq** (not equal to)、**range** (inclusive range)が指定できます。*port1*、*port2*はTCPあるいはUDPポート番号です。設定範囲は0～65535です。*port2*は*operator*が範囲であるときのみ必要です。 TCPポート番号は以下の名前で指定できます。**chargen** (19)、**bgp** (179)、**cmd** (514)、**daytime** (13)、**discard** (9)、**domain** (53)、**echo** (7)、**exec** (512)、**finger** (79)、**ftp** (21)、**ftp-data** (20)、**gopher** (70)、**hostname** (101)、**irc** (194)、**klogin** (543)、**kshell** (544)、**login** (513)、**lpd** (515)、**nntp** (119)、**pop2** (109)、**pop3** (110)、**smtp** (25)、**sunrpc** (111)、**tacacs** (49)、**talk** (517)、
destination-port *operator port1* [*port2*]	1つまたは複数のTCP/UDPの宛先ポート番号を指定します。	

パラメータ	機能	説明
		telnet (23)、**time** (37)、**uucp** (540)、**whois** (43)、**www** (80) UDPポート番号は以下の名前で指定できます **biff** (512)、**bootpc** (68)、**bootps** (67)、**discard** (9)、**dns** (53)、**dnsix** (90)、**echo** (7)、**mobilip-ag** (434)、**mobilip-mn** (435)、**nameserver** (42)、**netbios-dgm** (138)、**netbios-ns** (137)、**netbios-ssn** (139)、**ntp** (123)、**rip** (520)、**snmp** (161)、**snmptrap** (162)、**sunrpc** (111)、**syslog** (514)、**tacacs-ds** (65)、**talk** (517)、**tftp** (69)、**time** (37)、**who** (513)、**xdmcp** (177)
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	ACK、FIN、PSH、RST、SYN、URGを含む1つまたは複数のTCPフラグを指定します。	TCP用のパラメータです。各値は0(フラグビットがセットされていません)または1(フラグビットがセットされています)が指定できます。ルールのTCPフラグはANDの関係です。たとえば、ack 0 psh 1が設定されたルールは、ACKフラグが設定されていないパケット、およびPSHフラグが設定されているパケットに一致します。
established	TCP接続の確立状態を示すフラグを指定します。	TCP用のパラメータです。ルールはACKあるいはRSTフラグがセットされているTCP接続パケットに一致します。

protocol が **icmp** (1)である場合、設定するパラメータを表 19-3 に示します。

表 19-3 拡張 IPv4 ACL ルールの ICMP 指定パラメータ

パラメータ	機能	説明
icmp-type { **icmp-type** *icmp-code* | *icmp-message* }	ICMPメッセージタイプとコードを指定します。	*icmp-type*の設定範囲は0～255です。*icmp-code*の設定範囲は0～255です。*icmp-message*はメッセージの名前を指定します。サポートされるICMPメッセージ名と対応するタイプとコードの値を表 19-4に示します。

表 19-4 拡張 IPv4 ACL ルールでサポートされる ICMP メッセージ名

ICMP メッセージ名	ICMP メッセージタイプ	ICMP メッセージコード
echo	8	0
echo-reply	0	0

ICMP メッセージ名	ICMP メッセージタイプ	ICMP メッセージコード
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

説明

rule コマンドは拡張 IPv4 ACL のルールを作成あるいは修正します。

undo rule コマンドは拡張 IPv4 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

- すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。
- パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

例

コンフィグレーションプロファイル **ap1** にアドレス 129.9.0.0/16 から 202.38.160.0/24 の宛先ポート 80 の TCP パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl advanced 3000

[AC-config-profile-ap1-acl-ipv4-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0 0.0.0.255 destination-port eq 80

コンフィグレーションプロファイル **ap1** に 192.168.1.0/24 宛の ICMP パケットを除くすべての IP パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl advanced 3001

[AC-config-profile-ap1-acl-ipv4-adv-3001] rule deny icmp destination 192.168.1.0 0.0.0.255

[AC-config-profile-ap1-acl-ipv4-adv-3001] rule permit ip

コンフィグレーションプロファイル **ap1** に FTP の送受信パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl advanced 3002

[AC-config-profile-ap1-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp

[AC-config-profile-ap1-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp-data

[AC-config-profile-ap1-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp

[AC-config-profile-ap1-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp-data

コンフィグレーションプロファイル **ap1** に SNMP と SNMP trap の送受信パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl advanced 3003

[AC-config-profile-ap1-acl-ipv4-adv-3003] rule permit udp source-port eq snmp

[AC-config-profile-ap1-acl-ipv4-adv-3003] rule permit udp source-port eq snmptrap

[AC-config-profile-ap1-acl-ipv4-adv-3003] rule permit udp destination-port eq snmp

[AC-config-profile-ap1-acl-ipv4-adv-3003] rule permit udp destination-port eq snmptrap

関連コマンド

- **acl**
- **step**
- **time-range**

19.1.42 rule (IPv4 basic ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**fragment** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *

undo rule *rule-id* [**fragment** | **source** | **time-range**] *

undo rule [*rule-id*] { **deny** | **permit** } [**fragment** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *

デフォルト

設定なし

View

Configuration profile-IPv4 basic ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

fragment: 最初のフラグメントではないフラグメントを指定します。指定しない場合、ルールはすべてのフラグメントと非フラグメントを適用します。

source { *source-address source-wildcard* | **any** }: 送信元アドレスを定義します。*source-address* と *source-wildcard* はドットで区切られた 10 進数表記の送信元 IP アドレスとワイルドカードマスクを示します。すべてが 0 のワイルドカードはホストアドレスを示します。**any** は、任意の送信元 IP アドレスを示します。

time-range *time-range-name*: ルールのタイムレンジを指定します。*time-range-name* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS* *"タイムレンジ"* を参照してください。

説明

rule コマンドは標準 IPv4 ACL のルールを作成あるいは修正します。

undo rule コマンドは標準 IPv4 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

- すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。
- パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

例

コンフィグレーションプロファイル **ap1** に アドレス 10.0.0.0/8、172.17.0.0/16、192.168.1.0/24 を除く送信元 IP セグメントからのパケットを拒否する標準 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl basic 2000

[AC-config-profile-ap1-acl-ipv4-basic-2000] rule permit source 10.0.0.0 0.255.255.255

[AC-config-profile-ap1-acl-ipv4-basic-2000] rule permit source 172.17.0.0 0.0.255.255

[AC-config-profile-ap1-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255

[AC-config-profile-ap1-acl-ipv4-basic-2000] rule deny source any

関連コマンド

- **acl**
- **step**
- **time-range**

19.1.43 rule (Layer 2 ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

undo rule *rule-id* [**time-range**]

undo rule [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

デフォルト

設定なし

View

Configuration profile-Layer 2 ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

cos *vlan-pri*: 802.1p プライオリティを定義します。

- プライオリティの設定範囲は 0～7 です。
- **best-effort** (0)、**background** (1)、**spare** (2)、**excellent-effort** (3)、**controlled-load** (4)、**video** (5)、**voice** (6)、**network-management** (7)の用語で定義することができます。

dest-mac *dest-address dest-mask*: 宛先 MAC アドレス範囲を定義します。*dest-address* と *dest-mask* は宛先 MAC アドレスとマスクを示します。マスクの形式は H-H-H です。

lsap *lsap-type lsap-type-mask*: LLC カプセル化の DSAP と SSAP フィールドを定義します。*lsap-type* は 16 進数表記でカプセル化フォーマットを示します。*lsap-type-mask* は 16 進数表記で LSAP マスクを示します。

type *protocol-type protocol-type-mask*: L2 の 1 つ以上のプロトコルを定義します。*protocol-type* は 16 進数表記で Ethernet_II と Ethernet_SNAP のプロトコルタイプを示します。*protocol-type-mask* は 16 進数表記でプロトコルタイプのマスクを示します。

source-mac *source-address source-mask*: 送信元 MAC アドレス範囲を定義します。*source-address* は送信元 MAC アドレスを示します。*sour-mask* はマスクを示します。マスクの形式は H-H-H です。

time-range *time-range-name*: ルールのタイムレンジを指定します。*time-range-name* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。最初の文字は英字を使用する必要があります。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS* *"タイムレンジ"* を参照してください。

説明

rule コマンドは L2 ACL のルールを作成あるいは修正します。

undo rule コマンドは L2 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

- すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。
- パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

L2 ACL のルールとルールの ID を表示する場合、**display acl all** コマンドを使用します。

例

L2 ACL 4000 のルールを作成します。ARP パケットを許可し、RARP パケットを拒否します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] rule permit type 0806 ffff

[AC-config-profile-ap1-acl-mac-4000] rule deny type 8035 ffff

関連コマンド

- **acl**
- **step**

19.1.44 rule comment

Syntax

rule *rule-id* **comment** *text*

undo rule *rule-id* **comment**

デフォルト

設定なし

View

Configuration profile-IPv4 basic/advanced ACL view

Configuration profile-Layer 2 ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ACL のルール ID を指定します。設定範囲は 0～65534 です。ACL のルールはすでに作成されている必要があります。

text: ACL のルールの説明を指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

rule comment コマンドは ACL のルールの説明を設定します。

undo rule comment コマンドは ACL のルールの説明を削除します。

例

標準 IPv4 ACL 2000 を作成し、ルールの説明を追加します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl basic 2000

[AC-config-profile-ap1-acl-ipv4-basic-2000] rule 0 deny source 1.1.1.1 0

[AC-config-profile-ap1-acl-ipv4-basic-2000] rule 0 comment This rule is used on Gigabitethernet 1/0/1.

19.1.45 service-type

Syntax

service-type { **ftp** | { **telnet** | **terminal** } * }

undo service-type { **ftp** | { **telnet** | **terminal** } * }

デフォルト

ローカルユーザは許可されておらず、サービスを使用することができません。

View

Configuration profile-Local user view

定義済みユーザロール

network-admin

パラメータ

ftp: ユーザが FTP サービスを使用することを許可します。許可されたディレクトリは **authorization-attribute work-directory** コマンドで変更することができます。

telnet: ユーザが Telnet サービスを使用することを許可します。

terminal: ユーザが端末サービスを使用し、コンソールポートからログインすることを許可します。

説明

service-type コマンドはローカルユーザが使用するサービスタイプを指定します。

undo service-type コマンドはローカルユーザが使用するサービスタイプを削除します。

複数のサービスタイプをユーザに割り当てることができます。

例

コンフィグレーションプロファイル **ap1** に作成した 装置管理ユーザ user1 が Telnet、FTP サービスを使用することを許可します。

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] local-user user1 class manage

[AC-config-profile-ap1-luser-manage-user1] service-type telnet

[AC-config-profile-ap1-luser-manage-user1] service-type ftp

19.1.46 set authentication password

Syntax

set authentication password { **hash** | **simple** } *password*

undo set authentication password

デフォルト

コンソールユーザのパスワード設定は AP モデルにより異なります。

QX-W1000 シリーズは設定なしです。

QX-W1100 シリーズは qx_admin です。

QX-W1200 シリーズは qx_admin です。

line class vty のパスワード設定は AP モデルにより異なります。

QX-W1000 シリーズは設定なしです。

QX-W1100 シリーズは qx_admin です。

QX-W1200 シリーズは qx_admin です。

View

Configuration profile-user line view

Configuration profile-user line class view

定義済みユーザロール

network-admin

パラメータ

hash: 暗号テキストのパスワードを設定します。

Simple: プレーンテキストのパスワードを設定します。

Password: 大文字、小文字が区別されたパスワードを指定します。**Simple** が指定された場合、設定範囲は 1～16 文字です。**Hash** が指定された場合、設定範囲は 1～110 文字です。

説明

set authentication password コマンドはパスワード認証のパスワードを設定します。

Undo set authentication password コマンドはパスワードを削除します。

セキュリティのため、保存されたパスワードは設定に関わらず常に暗号テキストで表示されます。

このコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定がデフォルトでないとき、user line view の設定が適用されます。
- user line view の設定がデフォルトで user line class view の設定がデフォルトでないとき、user line class view の設定が適用されます。

例

コンフィグレーションプロファイル **ap1** の user line Console 0 でパスワード認証のパスワード hello を設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] line console 0

[AC-line-console0] authentication-mode password

[AC-line-console0] set authentication password simple hello

関連コマンド

authentication-mode

19.1.47 shutdown

Syntax

shutdown

undo shutdown

デフォルト

インタフェースはアップ状態です。

View

Configuration profile-interface view

定義済みユーザロール

network-admin

説明

shutdown コマンドはインタフェースをシャットダウンします。

Undo shutdown コマンドはインタフェースをアップします。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 をシャットダウンし、それからアップします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] shutdown

[AC-config-profile-ap1-GigabitEthernet1/0/1] undo shutdown

コンフィグレーションプロファイル **ap1** の アグリゲートインタフェース Bridge-Aggregation 1 を up にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface bridge-aggregation 1

[AC-config-profile-ap1-Bridge-Aggregation1] undo shutdown

コンフィグレーションプロファイル **ap1** の VLAN インタフェース 2 をシャットダウンし、up にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface vlan-interface 2

[AC-config-profile-ap1-Vlan-interface2] shutdown

[AC-config-profile-ap1-Vlan-interface2] undo shutdown

19.1.48 step

Syntax

step *step-value*

undo step

デフォルト

ACL のルール番号付けステップは 5 で、開始ルール ID は 0 です。

View

Configuration profile-Ipv4 basic/advanced ACL view

Configuration profile-Layer 2 ACL view

定義済みユーザロール

network-admin

パラメータ

step-value: ACL ルールのステップ数を指定します。設定範囲は 1～20 です。

説明

step コマンドは ACL ルールに自動的に番号を割り振るためのステップ数を設定します。

Undo step コマンドはデフォルトに戻します。

ルールの番号づけステップはシステムが自動的にルール番号の増分を設定します。たとえば、デフォルトの ACL の番号づけステップは 5 です。ルールを作成するとき、ID を割り当てない場合、ルールの番号は 0、5、10、15、…と番号づけられます。番号づけのステップを広くする場合、2 つのルールの間に多くのルールを挿入することができます。ステップを変更したときはいつでも、ルールは 0 から再ナンバリングが行われます。たとえば、5 つのルールの番号 5、10、13、15、20 がつけられている場合、ステップを 5 から 2 に変更すると、ルールの番号は 0、2、4、6、8 に再ナンバリングされます。

例

コンフィグレーションプロファイル **ap1** に作成した 標準 IPv4 ACL 2000 のステップ数を 2 に設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl basic 2000

[AC-config-profile-ap1-acl-ipv4-basic-2000] step 2

19.1.49 telnet server enable

Syntax

telnet server enable

undo telnet server enable

デフォルト

デフォルトは AP モデルにより異なります。

QX-W1000 シリーズでは無効です。

QX-W1100 シリーズでは有効です。

QX-W1200 シリーズでは有効です。

View

Configuration profile view

定義済みユーザロール

network-admin

説明

telnet server enable コマンドは Telnet サーバ機能を有効にします。

undo telnet server enable コマンドは Telnet サーバ機能を無効にします。

管理者は Telnet サーバ機能が有効であるときのみ装置に Telnet を行うことができます。

例

Telnet サーバ機能を有効にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] telnet server enable

19.1.50 vlan

Syntax

vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

undo vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

デフォルト

VLAN 1（システムデフォルト VLAN）

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

vlan-id1, vlan-id2: VLAN ID を指定します。設定範囲は 1～4094 です。

vlan-id1 **to** *vlan-id2*: VLAN の範囲を指定します。*vlan-id1* と *vlan-id2* は VLAN ID を指定します。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: VLAN 1～4094 を指定します。

説明

vlan *vlan-id* コマンドは VLAN を作成し、その view あるいは既存の VLAN の view に移行します。

vlan *vlan-id1* **to** *vlan-id2* コマンドは *vlan-id1* から *vlan-id2* の VLAN を作成します。

vlan all コマンドは VLAN 1～VLAN 4094 を作成します。

undo vlan コマンドは指定された VLAN を削除します。

システムデフォルト VLAN（VLAN 1）を作成あるいは削除することはできません。

例

コンフィグレーションプロファイル **ap1** に VLAN 2 を作成し、その view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] vlan 2

[AC-config-profile-ap1-vlan2]

コンフィグレーションプロファイル **ap1** に VLAN 4～VLAN 100 を作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] vlan 4 to 100

目次

このセクションのページは **2-x-x** です。

20 章 IoT 機能の設定 20-1
20.1 BLE 機能の設定コマンド 20-1
20.1.1 description 20-1
20.1.2 display wlan module-information 20-2
20.1.3 display iot ble neighbor-information 20-3
20.1.4 iot auto-module 20-5
20.1.5 iot auto-module persistent 20-6
20.1.6 iot auto-module persistent all 20-7
20.1.7 module 20-8
20.1.8 module enable 20-9
20.1.9 module firmware-upgrade 20-10
20.1.10 rfid-tracking ble advertisement 20-11
20.1.11 rfid-tracking ble advertisement { disable | enable } 20-13
20.1.12 rfid-tracking ble advertisement interval 20-15
20.1.13 rfid-tracking ble advertisement mode 20-16
20.1.14 rfid-tracking ble aging-time 20-18
20.1.15 tx-power 20-20
20.1.16 type ble 20-21
20.1.17 wlan execute module reset 20-22
20.2 サーバへの IoT データのレポート設定コマンド 20-23
20.2.1 azure-dps group-symmetric-key 20-23
20.2.2 azure-dps id-scope 20-24
20.2.3 display iot transport-profile 20-25
20.2.4 display iot transport-profile in-use 20-26
20.2.5 filter rssi threshold 20-28
20.2.6 filter rssi-fluctuation threshold 20-29
20.2.7 filter recent-packet duration 20-30
20.2.8 filter highest-rssi 20-32
20.2.9 iot transport-profile 20-33
20.2.10 iot-transport-profile 20-34
20.2.11 keepalive interval 20-35
20.2.12 report interval 20-35
20.2.13 server-url 20-36
20.2.14 transport-profile enable 20-37
20.3 AeroScout ロケーションの設定コマンド 20-38
20.3.1 rfid-tracking aeroscout 20-38

20.3.2 rfid-tracking aeroscout aggregate-report interval 20-39
20.3.3 rfid-tracking aeroscout engine-address 20-41
20.3.4 rfid-tracking aeroscout engine-detection 20-42
20.3.5 rfid-tracking aeroscout report-mode 20-44
20.3.6 rfid-tracking aeroscout tag-multicast-address 20-45
20.3.7 rfid-tracking aeroscout timestamp 20-47
20.3.8 rfid-tracking aeroscout vendor-port 20-48
20.3.9 rfid-tracking mode 20-49
20.3.10 rfid-tracking radio 20-50
20.4 ワイヤレスロケーション共通パラメータの設定コマンド 20-52
20.4.1 display wlan rfid-tracking radio 20-52
20.4.2 rfid-tracking client rate-limit 20-53
20.4.3 rfid-tracking client rate-limit cir 20-54
20.4.4 rfid-tracking dilution 20-55
20.4.5 rfid-tracking dilution factor 20-57
20.4.6 rfid-tracking ignore ap-frame 20-58
20.4.7 rfid-tracking ignore beacon 20-59
20.4.8 rfid-tracking keepalive 20-60
20.4.9 rfid-tracking rate-limit 20-62
20.4.10 rfid-tracking rate-limit cir 20-63
20.4.11 rfid-tracking rssi 20-64
20.4.12 rfid-tracking rssi threshold 20-65

20章 IoT 機能の設定

20.1 BLE機能の設定コマンド

🕮 **メモ：**

この章のコマンドは、ソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

20.1.1 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

Module view

定義済みユーザロール

network-admin

パラメータ

text: モジュールの説明を指定します。text 引数は大文字と小文字を区別する 1～64 文字の文字列です。

説明

description コマンドはモジュールの説明を指定します。

undo description コマンドはモジュールの説明を削除します。

description コマンドでモジュールの説明を設定することが出来ます。

IoT AP にインストールまたは接続されているモジュールを効率的に管理するには、型番、場所、および機能に基づいたモジュールの説明を設定します。

例

#モジュール 1 の説明を L3-office に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] description L3-office

20.1.2 display wlan module-information

Syntax

display wlan module-information { all | ap *ap-name* **{ module all | module** *module-id* **} } [online]**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

module all: すべてのモジュールを指定します。

module *module-id*: モジュール ID を指定します。*module-id* 引数の値の範囲は、AP モデルによって異なります。

online: オンライン状態のモジュールを指定します。

説明

display wlan module-information コマンドは AP のモジュール情報を表示します。

例

#AP ap1 のモジュール 1 に関する情報を表示します。

<AC> display wlan module-information ap ap1 module 1

```
AP name             :1110
Maximum modules      :1
  Module 1:
  Module administrative type    : BLE
  Module physical type         : NEC
  Model                       : T103-MP
  HW version                   : Ver.A
```

```
SW version                : A1253 V200R001B01D029SP53
Serial ID                 : 219801A1LHA10A100626
Module MAC                : 0023-89e2-ed76
Module physical status      : Normal
Module administrative status  : Disabled
Description               : Not configured
```

表 20-1

フィールド	説明
Module administrative type	設定されているモジュールタイプ
Module physical type	モジュールの物理タイプ
Model	モジュールの型番。使用可能なモジュールがない場合、このフィールドにはN/Aと表示されます。
HW version	モジュールのハードウェアバージョン
SW version	モジュールのソフトウェアバージョン
Serial ID	モジュールのシリアルID
Module MAC	モジュールのMACアドレス。（H-H-H形式）
Module physical status	物理モジュールの状態： • Unavailable • Normal • Absent
Module administrative status	モジュールの設定状態： • Enable • Disable
Description	モジュールの説明

20.1.3 display iot ble neighbor-information

Syntax

display iot ble neighbor-information ap *ap-name* **{ module all | module** *module-id* **| mac** *mac-addr* **}**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

module all: すべてのモジュールを指定します。

module *module-id*: モジュール ID を指定します。*module-id* 引数の値の範囲は、AP モデルによって異なります。

mac *mac-addr*: MAC アドレスを指定します。MAC アドレスは、大文字と小文字を区別しない XXXX-XXXX-XXXX 形式の 14 文字の文字列です。各 X は、0~9 の数字または a~f の小文字を表します。

説明

display iot ble neighbor-information コマンドは、AP 周辺の BLE デバイス情報を表示します。

例

#AP ap1 周辺の BLE デバイス情報を表示します。

<AC> display iot ble neighbor-information ap ap1 module 1

```
--------------------------------------------------------------------------------
--------
Module ID  MAC address     Address type         RSSI      Last update time
--------------------------------------------------------------------------------
--------
1          1111-2222-AAAA   Public               -5        Mon Nov  2 13:54:23
2021
1          ABAB-CCCC-FFFF   PrivateResolvable     6        Mon Nov  2 13:54:23
2021
```

表 20-2

フィールド	説明
MAC address	BLEデバイスのMACアドレス

フィールド	説明
Address type	アドレスの種類： • Public • Static • PrivateResolvable • PrivateNonResolvable

20.1.4 iot auto-module

Syntax

iot auto-module { disable | enable }

undo iot auto-module

デフォルト

AP view: AP group view の設定を使用します。

AP group view: 無効

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

enable: 自動モジュール機能を有効にします。

disable: 自動モジュール機能を無効にします。

説明

iot auto-module enable コマンドは自動モジュール機能を有効にします。

iot auto-module disable コマンドは自動モジュール機能を無効にします。

undo iot auto-module コマンドはデフォルトに戻します。

自動モジュール機能を有効にすると、手動モジュールを設定しなくてもモジュールを AP に関連付けることができます。

AP view の設定は、AP group view の設定より優先されます。

例

#AP ap1 の自動モジュール機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] iot auto-module enable

#AP group 10 の自動モジュール機能を有効にします。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] iot auto-module enable

20.1.5 iot auto-module persistent

Syntax

iot auto-module persistent { disable | enable }

undo iot auto-module persistent

デフォルト

AP view: AP group view の設定を使用します。

AP group view: 無効

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

enable: 自動モジュール変換機能を有効にします。

disable: 自動モジュール変換機能を無効にします。

説明

iot auto-module persistent enable コマンドは自動モジュール変換機能を有効にします。

iot auto-module persistent disable コマンドは自動モジュール変換機能を無効にします。

undo iot auto-module persistent コマンドはデフォルトに戻します。

自動モジュール変換機能を有効にすると、モジュールがオンラインになった後、自動的に自動モジュールを手動モジュールに変換します。手動モジュールに自動的に変換されるのは、自動モジュール変換機能を有効にした後でオンラインになったモジュールのみで

す。オンライン状態の自動モジュールを手動モジュールに変換する場合は、**iot auto-module persistent all** コマンドを使用します。

Module view の設定は、AP group module view の設定より優先されます。

例

#AP ap1 の自動モジュール変換機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] iot auto-module persistent enable

#AP group 10 の自動モジュール変換機能を有効にします。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] iot auto-module persistent enable

20.1.6 iot auto-module persistent all

Syntax

iot auto-module persistent all

View

AP view

AP group view

定義済みユーザロール

network-admin

説明

iot auto-module persistent all コマンドは、すべてのオンライン状態の自動モジュールを手動モジュールに変換し、変換された各モジュールにシリアル番号を自動的に割り当てます。

例

#AP ap1 のすべてのオンライン状態の自動モジュールを、手動モジュールに変換します。

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] iot auto-module persistent all

#AP group 10 のすべてのオンライン状態の自動モジュールを、手動モジュールに変換します。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] iot auto-module persistent all

20.1.7 module

Syntax

module *module-id*

View

AP view

AP group's AP model view

定義済みユーザロール

network-admin

パラメータ

module-id: モジュール ID を指定します。値の範囲は AP モデルによって異なります。

説明

module コマンドは module view に入ります。

例

#AP ap1 の module view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1]

#AP group apgroup10 の AP モデル QX-W1110 で、module view に移行します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-apgroup1] ap-model QX-W1110

[AC-wlan-ap-apgroup1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1]

20.1.8 module enable

Syntax

module { disable | enable }

undo module

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: 無効

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

enable: モジュールを有効にします。

disable: モジュールを無効にします。

説明

module enable コマンドはモジュールを有効にします。

module disable コマンドはモジュールを無効にします。

undo module コマンドはデフォルトに戻します。

Module view の設定は、AP group module view の設定より優先されます。

例

#AP ap1 のモジュールを有効にします。

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] module enable

#AP group 1 の AP モデル QX-W1110 のモジュールを有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] module enable

20.1.9 module firmware-upgrade

Syntax

module firmware-upgrade { disable | enable }

undo module firmware-upgrade

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: 有効

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

enable: モジュールの自動ファームウェアアップグレードを有効にします。

disable: モジュールの自動ファームウェアアップグレードを無効にします。

説明

module firmware-upgrade enable コマンドはモジュールの自動ファームウェアアップグレードを有効にします。

module firmware-upgrade disable コマンドはモジュールの自動ファームウェアアップグレードを無効にします。

undo module firmware-upgrade コマンドはデフォルトに戻します。

この機能により、ファームウェアバージョンが AP のイメージファイルに保存されているバージョンと異なる場合に、モジュールのファームウェアを自動でアップグレードできます。

モジュールに対してこの機能を有効にすると、モジュールがインストールされている IoT AP が再起動されるたびにこの機能が有効になります。

モジュールファームウェアのアップグレードプロセス中に、shutdown コマンドを使用して、ファームウェアアップグレード中の IoT AP と接続するインターフェイスをシャットダウンしないでください。Module view の設定は、AP group module view の設定より優先されます。

例

#AP ap1 で module1 の、自動ファームウェアアップグレードを有効にします。

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] module firmware-upgrade enable

#AP group 10 の AP モデル QX-W1110 で、module1 の自動ファームウェアアップグレードを有効にします。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] ap-model QX-W1110

[AClan-ap-group-10-ap-model-QX-W1110] module 1

[AClan-ap-group-10-ap-model-QX-W1110-module-1] module firmware-upgrade enable

20.1.10 rfid-tracking ble advertisement

Syntax

rfid-tracking ble advertisement [*ad-number* **] { major-id** *major-id* **| measured-power** *measured-power* **| minor-id** *minor-id* **| uuid** *uuid* **}**

undo rfid-tracking ble advertisement [*ad-number* **] { major-id | measured-power | minor-id | uuid }**

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: BLE モジュールの ad1 および ad2 のアドバタイズメント情報は、mjor-id は 1、minor-id は 1、measured-power は-58、uuid は E1CC5B618C06428E8720FE619DB80193 です。

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

ad-number: アドバタイズメントタイプを指定します。この引数を指定しない場合、ad 1 アドバタイズメントが設定されます。

major-id *major-id*: BLE モジュールのアドバタイズメント情報の Major-ID を指定します。major-id 引数の値の範囲は 0 から 65535 です。

measured-power *measured-power*: BLE モジュールのアドバタイズメント情報の measured-power を指定します。*measured-power* 引数の値の範囲は 0~127 で、0〜-127 dBm の信号強度を表します。measured-power 引数の値が大きいほど信号強度が弱くなります。measured-power は、iBeacon を送信したデバイスから 1 m (3.28 フィート) 離して配置した、受信デバイスで検出される信号強度です。measured-power は、アドバタイズを受信したデバイスと iBeacon 送信デバイス間の距離の計算に使用できます。

minor-id *minor-id*: BLE モジュールのアドバタイズメント情報の Minor-ID を指定します。*minor-id* 引数の値の範囲は 0 から 65535 です。

uuid *uuid*: BLE モジュールのアドバタイズメント情報の uuid を指定します。*uuid* 引数の値の範囲は、大文字と小文字を区別しない 0~f の 32 桁の 16 進数文字列です。

説明

rfid-tracking ble advertisement コマンドは BLE モジュールのアドバタイズメント情報を設定します。

undo rfid-tracking ble advertisement コマンドはデフォルトに戻します。

BLE モジュールは、Major-ID、Minor-ID、Measured-power、UUID を含む iBeacon アドバタイズメントを近くのアプリケーションソフトウェアにブロードキャストします。アドバタイズメントを受信したアプリケーションソフトウェアは、アドバタイズメント情報に応じて特定の動作を行い、ソフトウェア機能を実現します。

Module view の設定は、AP group module view の設定より優先されます。

例

AP ap1 で、BLE module 1 の ad1 アドバタイズメント情報を設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement major-id 4

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement minor-id 4

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement uuid 34ae56115098ca67321a11256bca3007

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement measured-power 30

AP グループ 1 の AP モデル QX-W 1110 で、BLE module 1 の ad 1 アドバタイズメント情報を設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement major-id 4

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement minor-id 4

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement uuid 34ae56115098ca67321a11256bca3007

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement measured-power 30

#AP ap 1 上で、BLE モジュール 1 の ad 2 アドバタイズメント情報を設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement ad2 major-id 5

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement ad2 minor-id 5

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement ad2 uuid 44ae56115098ca67321a11256bca3008

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement ad2 measured-power 30

#AP グループ 1 の AP モデル QX-W 1110 で、BLE モジュール 1 の ad 2 アドバタイズメント情報を設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement ad2 major-id 5

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement ad2 minor-id 5

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement ad2 uuid 44ae56115098ca67321a11256bca3008

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement ad2 measured-power 30

20.1.11 rfid-tracking ble advertisement { disable | enable }

Syntax

rfid-tracking ble advertisement { disable | enable }

undo rfid-tracking ble advertisement

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: 無効

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

enable: BLE モジュールの iBeacon 送信機能を有効にします。

disable: BLE モジュールの iBeacon 送信機能を無効にします。

説明

rfid-tracking ble advertisement enable コマンドは BLE モジュールの iBeacon 送信機能を有効にします。

rfid-tracking ble advertisement disable コマンドは BLE モジュールの iBeacon 送信機能を無効にします。

undo rfid-tracking ble advertisement コマンドはデフォルトに戻します。

BLE モジュールが iBeacon ad1 および ad2 アドバタイズメントを定期的にブロードキャストできるようにします。iBeacon アドバタイズメントには、UUID、Major-ID、Minor-ID が含まれます。ad1 または ad2 アドバタイズメントのパラメータを設定するには、rfid-tracking ble advertisement コマンドを使用します。

Module view の設定は、AP group module view の設定より優先されます。

例

#AP ap 1 上の BLE モジュール 1 の iBeacon 送信機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement enable

#AP グループ 1 の AP モデル QX-W 1110 で、BLE module 1 の iBeacon 送信機能を有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement enable

20.1.12 rfid-tracking ble advertisement interval

Syntax

rfid-tracking ble advertisement [*ad-number* **] interval** *interval*

undo rfid-tracking ble advertisement [*ad-number* **] interval**

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: BLE モジュールの iBeacon ad1 および ad2 アドバタイズメントをブロードキャストする間隔は 100 センチ秒です。

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

ad-number: アドバタイズメントタイプを指定します。この引数を指定しない場合、コマンドは ad1 アドバタイズメントをブロードキャストする間隔を設定します。

interval: BLE モジュールが iBeacon アドバタイズメントをブロードキャストする間隔を 10 の倍数値で指定します。値の範囲は 50~1000 で、単位はセンチ秒です。

説明

rfid-tracking ble advertisement interval コマンドは BLE モジュールが iBeacon をブロードキャストする間隔を設定します。

undo rfid-tracking ble advertisement interval コマンドはデフォルトに戻します。

Module view の設定は、AP group module view の設定より優先されます。

例

AP ap1 で、BLE module 1 の ad1 アドバタイズメントを 200 センチ秒ごとにブロードキャストするように設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement interval 200

AP グループ 1 の AP モデル QX-W 1110 で、BLE module 1 の ad 1 アドバタイズメント情報を 200 センチ秒ごとにブロードキャストするように設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement interval 200

#AP ap 1 上で、BLE モジュール 1 の ad 2 アドバタイズメント情報を 200 センチ秒ごとにブロードキャストするように設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement ad2 interval 200

#AP グループ 1 の AP モデル QX-W 1110 で、BLE モジュール 1 の ad 2 アドバタイズメント情報を 200 センチ秒ごとにブロードキャストするように設定します

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement ad2 interval 200

20.1.13 rfid-tracking ble advertisement mode

Syntax

rfid-tracking ble advertisement mode { continuous *ad-number* **| periodic {** *ad-number period* **}&<2> }**

undo rfid-tracking ble advertisement mode

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: BLE モジュールの iBeacon ad1 のアドバタイズメントを連続モードで送信します。

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

continuous: 連続モードを指定します。

ad-number: アドバタイズメントタイプを指定します。

periodic: *periodic モードを指定します。*

{ ad-number period }&<2>: アドバタイズメントタイプとアドバタイズメント期間を 10 の倍数値で指定します。アドバタイズメント期間の範囲は 50～6000 で、単位はセンチ秒です。&<2>は、2 つのアドバタイズメントタイプと 2 つのアドバタイズメント期間を指定する必要があることを示します。

説明

rfid-tracking ble advertisement mode コマンドは BLE アドバタイズメントモードを設定します。

undo rfid-tracking ble advertisement mode コマンドはデフォルトに戻します。

BLE モジュールは、次のモードでアドバタイズメントを送信できます。

- 連続モード: 指定された間隔で 1 種類のアドバタイズメント (ad 1 または ad 2) だけを送信します。
- Periodic モード: 指定した間隔で ad 1 アドバタイズメントと ad 2 アドバタイズメントを交互に送信します。

たとえば、ad1 アドバタイズメント期間が 210 センチ秒、ad2 アドバタイズメント期間が 310 センチ秒、アドバタイズメント間隔がそれぞれ 100 センチ秒の場合、BLE モジュールは、最初に 210 センチ秒の間に 3 つの ad 1 アドバタイズメントを送信し、次に 310 センチ秒の間に 4 つの ad2 アドバタイズメントを送信します。このパターンでは、BLE モジュールは ad1 および ad2 アドバタイズメントを交互に送信します。

アドバタイズメント間隔は、rfid-tracking ble advertisement interval コマンドを使用して設定します。

Module view の設定は、AP group module view の設定より優先されます。

例

AP ap1 で、BLE module 1 の ad1 アドバタイズメントを連続モードで送信するように設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement mode continuous ad1

AP グループ 1 の AP モデル QX-W 1110 で、BLE module 1 の ad 1 アドバタイズメント情報を連続モードで送信するように設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement mode continuous ad1

#AP ap 1 上で、BLE モジュール 1 の ad1 および ad2 のアドバタイズメント情報を Periodic モードで送信するように設定します。ad1 のアドバタイズメント期間を 200 センチ秒、ad2 のアドバタイズメント期間を 100 センチ秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement mode periodic ad1 200 ad2 100

#AP グループ 1 の AP モデル QX-W 1110 で、BLE モジュール 1 の ad1 および ad2 のアドバタイズメント情報を Periodic モードで送信するように設定します。ad1 のアドバタイズメント期間を 200 センチ秒、ad2 のアドバタイズメント期間を 100 センチ秒に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement mode periodic ad1 200 ad2 100

20.1.14 rfid-tracking ble aging-time

Syntax

rfid-tracking ble aging-time *aging-time*

undo rfid-tracking ble aging-time

デフォルト

AP view: AP group view の設定を使用します。AP group view に設定がない場合、global configuration view の設定を使用します。

AP group view: global configuration view の設定を使用します。

global configuration view: 180 秒

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

aging-time: エージングタイムを 60~3600 秒の範囲で指定します

説明

rfid-tracking ble aging-time コマンドは BLE デバイスのエージングタイムを設定します。

undo rfid-tracking ble aging-time コマンドはデフォルトに戻します。

rfid-tracking ble aging-time コマンドは、BLE デバイスのエージングタイムを設定します。AP view の設定は、AP group view の設定よりも優先されます。AP group view の設定は、グローバル設定 view の設定よりも優先されます

例

#AP ap 1 の BLE デバイスのエージングタイムを 60 秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking ble aging-time 60

#AP group 10 の BLE デバイスのエージングタイムを 60 秒に設定します。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] rfid-tracking ble aging-time 60

#BLE デバイスのエージングタイムをグローバルで 60 秒に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] rfid-tracking ble aging-time 60

20.1.15 tx-power

Syntax

tx-power { *power-level* **| value** *power-value* **}**

undo tx-power

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: 送信電力レベル 1 です。これは送信電力 4dBm を示します。

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

power-level:送信電力レベルを指定します。値は 1、2、3、4 のいずれかで、それぞれ 4 dBm、-1 dBm、-5 dBm、-9 dBm の送信電力を示します。

value *power-value*: 送信電力を指定します。値の範囲は-40 dBm~+8 dBm です。

説明

tx-power コマンドはモジュールの送信電力を設定します。

undo tx-power コマンドはデフォルトに戻します。

Module view の設定は、AP group module view の設定より優先されます。

例

#AP ap1 のモジュール 1 の送信電力レベルを 4 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] tx-power 4

#AP group 1 の AP モデル QX-W1110 で、モジュール 1 の送信電力レベルを 4 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] tx-power 4

20.1.16 type ble

Syntax

type ble

undo type

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: 設定なし

View

Module view

AP group module view

定義済みユーザロール

network-admin

説明

type ble コマンドは、サポート対象モジュールタイプとして BLE を指定します。

undo type コマンドはデフォルトに戻します。

AP 上のモジュールが正しく動作するには、指定するサポート対象モジュールタイプが物理モジュールタイプと一致している必要があります。

Module view の設定は、AP group module view の設定より優先されます。

例

#AP ap1 のモジュール 1 でサポート対象モジュールタイプとして BLE を指定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] type ble

#AP group 1 の AP モデル QX-W1110 で、モジュール 1 のサポート対象モジュールとして BLE を指定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] type ble

20.1.17 wlan execute module reset

Syntax

wlan execute module reset ap *ap-name* **module** *module-id*

View

System view

定義済みユーザロール

network-admin

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

module *module-id*: モジュール ID を指定します。module-id 引数の値の範囲は、AP モデルによって異なります。

説明

wlan execute module reset コマンドは AP のモジュールを再起動します。

例

#AP ap1 のモジュール 1 を再起動します。

<AC> system-view

[AC] wlan execute module reset ap ap1 module 1

20.2 サーバへのIoTデータのレポート設定コマンド

🕮 **メモ：**

この章のコマンドは、ソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

20.2.1 azure-dps group-symmetric-key

Syntax

azure-dps group-symmetric-key { cipher | simple } *string*

undo azure-dps group-symmetric-key

デフォルト

設定なし

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

cipher: 暗号テキストで鍵を設定します。

simple: プレーンテキストで鍵を設定します。セキュリティ上の理由から、平文形式で指定された鍵は暗号化された形式で保存されます。

string: 鍵の文字列を指定します。暗号テキストの鍵は大文字と小文字を区別する 33～201 の文字列です。プレーンテキストの鍵は大文字と小文字を区別する 1～128 文字の文字列です。

説明

azure-dps group-symmetric-key コマンドは Microsoft Azure IoT Hub DPS のグループ対称キーを設定します。

undo azure-dps group-symmetric-key コマンドはデフォルトに戻します。

IoT データレポート用のサーバが Microsoft Azure IoT hub DPS の場合、IoT トランスポートプロファイルを有効にする前に、このコマンドを実行する必要があります。グループ対称キーを編集する場合、事前に IoT トランスポートプロファイルを無効にする必要があります。

例

#Microsoft Azure IoT hub DPS のグループ対称キーを、暗号テキストで設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub] azure-dps group-symmetric-key cipher OpsBHTTubGabpHTmYbc3w7dKqG9XC6e8OS2apbHRMtVunBkYTY9B/ScyjLeRpf7cjJxXPIsIqna8WV1DePS8uA==

関連コマンド

iot transport-profile

20.2.2 azure-dps id-scope

Syntax

azure-dps id-scope *id-scope*

undo azure-dps *id-scope*

デフォルト

設定なし

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

id-scope: Microsoft Azure IoT Hub DPS の ID スコープの文字列を指定します。ID スコープは 1～63 文字の文字列です。

説明

azure-dps id-scope コマンドは Microsoft Azure IoT Hub DPS の ID スコープを設定します。

undo azure-dps id-scope コマンドはデフォルトに戻します。

IoT データレポート用のサーバが Microsoft Azure IoT hub DPS の場合、IoT トランスポートプロファイルを有効にする前に、このコマンドを実行する必要があります。ID スコープを編集する場合、事前に IoT トランスポートプロファイルを無効にする必要があります。

例

#Microsoft Azure IoT hub DPS の ID スコープを 1234567890a として設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub] azure-dps id-scope 1234567890a

関連コマンド

iot transport-profile

20.2.3 display iot transport-profile

Syntax

display iot transport-profile

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display iot transport-profile コマンドは、IoT トランスポートプロファイルに関する情報を表示します。

IoT トランスポートプロファイルに関する情報を表示するには、まず System view で IoT トランスポートプロファイルを作成する必要があります。

例

#作成されたすべての IoT トランスポートプロファイルに関する情報を表示します。

<AC> display iot transport-profile

```
Profile name                Server type          Status
Azureiot1                   Azure                Enabled
Azureiot2                   Azure                Disabled
```

表 20-3

フィールド	説明
Server type	サーバタイプ。サポートされているのはAzureのみ。
Status	IoTトランスポートプロファイルの状態: • Enabled • Disabled

関連コマンド

iot-transport-profile

20.2.4 display iot transport-profile in-use

Syntax

display iot transport-profile in-use

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display iot transport-profile in-use コマンドは、使用中の IoT トランスポートプロファイルに関する情報を表示します。

例

#使用中の IoT トランスポートプロファイルに関する情報を表示します。

<AC> display iot transport-profile in-use

```
Connect status: connected
Connected for: 0d 19h 20m 15s
Profile name: aaa
Server URL: global.azure-devices-provisioning.net
Server type: azure iot
Azure DPS information:
  ID scope: 0cn0002B978
  Key type: symmetric
  Group                                                    key(cipher):
$c$3$hQpNztebohdFlXL5p0aVIsA4Hn2QYH5PIWSJDTtZr0mwKW942Erghtscx0aZ3
osazfgmTSZ0PKjz5DavZFpYk6y/ijJqAHC5U+6jIltCjhh2vrRCsh2gNiCnHGpOEr8YH0HJhHOzxE
acd6Q=
  Register ID: sn-210235A3KYC187000028
Report interval: 60 seconds
Keepalive interval: 60 seconds
Total sent messages: 0
Sent BLE data messages: 0
Sent keepalive messages: 0
Total received messages: 0
```

表 20-4

フィールド	説明
Connect status	デバイスとサーバ間の接続の状態: ● connecting－接続試行中 ● connected －接続 ● disconnected－切断
Connected for	サーバとの接続時間
Profile name	IoTトランスポートプロファイル名
Server URL	サーバのURL
Server type	サービスタイプ。現在のソフトウェアではMicrosoft Azure IoT Hub DPSのみをサポートしています。
Azure DPS information	Azure DPSの情報
ID scope	Azure DPSのIDスコープ。
Key type	Azure DPSキーの種類。現在のソフトウェアでは対称キーのみをサポートしています。
Group key(cipher)	Azure DPS登録グループの対称キー。キーは暗号テキストで表示されます。
Register ID	Azure DPSのデバイス登録ID
Report interval	APがIoTデータをサーバにレポートする間隔。単位は秒です。
Keepalive interval	サーバにキープアライブパケットを送信する間隔。単位は秒です。
Total sent messages	送信したメッセージの合計数
Sent BLE data messages	送信したBLEデータメッセージの合計数
Sent keepalive messages	送信したキープアライブメッセージの合計数
Total received messages	受信したメッセージの合計数

20.2.5 filter rssi threshold

🕮 メモ：

この章のコマンドは、ソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

filter rssi threshold *rssi-threshold*

undo filter rssi threshold

デフォルト

設定なし

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

rssi-threshold: ロケーションパケットをフィルタリングするための RSSI しきい値を-127~+20 dBm の範囲で指定します。

説明

filter rssi threshold コマンドはロケーションパケットをフィルタリングするための RSSI しきい値を設定します。

undo filter rssi threshold コマンドはデフォルトに戻します。

IoT ロケーションシナリオで無効なロケーションパケットを処理することによる IoT AP および IoT サーバの負荷を軽減するには、次のフィルタを使用してロケーションパケットをフィルタリングします。

- RSSI しきい値。
- RSSI 変動しきい値。RSSI 変動は、同じ IoT エンドポイントによって送信されるロケーションパケットの RSSI が変動した場合に発生します。
- 各ロケーションパケットレポート間隔の最新のサブ間隔。
- レポート間隔中の RSSI 値。

指定された RSSI しきい値を超える RSSI を持つロケーションパケットのみが IoT AP によって受け入れられ、IoT サーバに報告されます。

適切な RSSI しきい値を設定します。値が大きすぎると、大量のロケーションパケットが破棄される可能性があります。値が小さすぎると、最適なパケットフィルタリングパフォーマンスを実現できません。

例

#ロケーションパケットをフィルタリングするための RSSI しきい値を-70 dBm に設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-transport-profile-azureiothub] filter rssi threshold -70

20.2.6 filter rssi-fluctuation threshold

🕮 **メモ：**

この章のコマンドは、ソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

filter rssi-fluctuation threshold *rssi-threshold*

undo filter rssi-fluctuation threshold

デフォルト

設定なし

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

rssi-threshold: ロケーションパケットをフィルタリングするための RSSI 変動しきい値を 1～127 dBm の範囲で指定します。

説明

filter rssi-fluctuation threshold コマンドはロケーションパケットをフィルタリングするための RSSI 変動しきい値を設定します。

undo filter rssi-fluctuation threshold コマンドはデフォルトに戻します。

IoT ロケーションシナリオで無効なロケーションパケットを処理することによる IoT AP および IoT サーバの負荷を軽減するには、次のフィルタを使用してロケーションパケットをフィルタリングします。

- RSSI しきい値。

- RSSI 変動しきい値。RSSI 変動は、同じ IoT エンドポイントによって送信されるロケーションパケットの RSSI が変動した場合に発生します。
- 各ロケーションパケットのレポート間隔の最新のサブ間隔。
- レポート間隔中の RSSI 値。

指定された RSSI 変動しきい値以上の RSSI 変動値を持つロケーションパケットのみが IoT AP によって受け入れられ、IoT サーバに報告されます。

適切な RSSI 変動しきい値を設定します。値が大きすぎると、大量のロケーションパケットが破棄される可能性があります。値が小さすぎると、最高のパケットフィルタリングパフォーマンスを実現できません。

例

#ロケーションパケットをフィルタリングするための RSSI 変動しきい値を 20 dBm に設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC -iot-transport-profile-azureiothub] filter rssi-fluctuation threshold 20

関連コマンド

iot-transport-profile

20.2.7 filter recent-packet duration

🕮 **メモ**：

この章のコマンドは、ソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

filter recent-packet duration *duration*

undo filter recent-packet duration

デフォルト

設定なし

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

duration: 各レポート間隔の対象となる最新のサブ間隔を指定します。これにより、このサブ間隔よりも前に受信されたロケーションパケットを、詳細なパケットフィルタリングで抑制できます。

説明

filter recent-packet duration コマンドは IoT AP が各レポート間隔の指定された最新のサブ間隔で受信したロケーションパケットのみをレポートできるようにします。

undo filter recent-packet duration コマンドは IoT トランスポートプロファイルを削除します。

IoT ロケーションシナリオで無効なロケーションパケットを処理することによる IoT AP および IoT サーバの負荷を軽減するには、次のフィルタを使用してロケーションパケットをフィルタリングします。

- RSSI しきい値。
- RSSI 変動しきい値。RSSI 変動は、同じ IoT エンドポイントによって送信されるロケーションパケットの RSSI が変動した場合に発生します。
- 各ロケーションパケットのレポート間隔の最新のサブ間隔。
- レポート間隔中の RSSI 値。

このコマンドを設定すると、IoT AP は、各レポート間隔の指定された最新のサブ間隔で受信したロケーションパケットのみをレポートします。

各レポート間隔の最新のサブ間隔は、**report interval** コマンドで指定したレポート間隔よりも小さい必要があります。

値が大きすぎると、大量のロケーションパケットが破棄される可能性があります。値が小さすぎると、最適なパケットフィルタリングパフォーマンスを実現できません。

例

#各 IoT AP がレポート間隔の最新の 50 秒間に受信したロケーションパケットのみをレポートするように設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-transport-profile-azureiothub] filter recent-packet duration 50

関連コマンド

- **iot transport-profile**
- **report interval**

20.2.8 filter highest-rssi

🕮 **メモ：**

この章のコマンドは、ソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

filter highest-rssi

undo filter highest-rssi

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

説明

filter highest-rssi コマンドはレポート間隔中に各 IoT エンドポイントからの RSSI が最も高いロケーションパケットのみを IoT サーバにレポートするように装置を設定します。

undo filter highest-rssi コマンドはデフォルトに戻します。

IoT ロケーションシナリオで無効なロケーションパケットを処理することによる IoT AP および IoT サーバの負荷を軽減するには、次のフィルタを使用してロケーションパケットをフィルタリングします。

- RSSI しきい値。
- RSSI 変動しきい値。RSSI 変動は、同じ IoT エンドポイントによって送信されるロケーションパケットの RSSI が変動した場合に発生します。
- 各ロケーションパケットのレポート間隔の最新のサブ間隔。
- レポート間隔中の RSSI 値。

このコマンドを設定すると、IoT AP はレポート間隔中に、各 IoT エンドポイントからの RSSI が最も高いロケーションパケットのみを IoT サーバにレポートします。レポート間隔を設定するには、**report interval** コマンドを使用します。

例

#レポート間隔中に、各 IoT エンドポイントからの RSSI が最も高いロケーションパケットのみを IoT サーバにレポートするように IoT AP を設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-transport-profile-azureiothub] filter highest-rssi

関連コマンド

- **iot transport-profile**
- **report interval**

20.2.9 iot transport-profile

Syntax

iot transport-profile *transport-profile-name*

undo iot transport-profile *transport-profile-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

transport-profile-name: IoT トランスポートプロファイル名を指定します。IoT トランスポートプロファイル名は、大文字、小文字を区別しない 1～63 文字の文字列です。

説明

iot transport-profile コマンドは IoT トランスポートプロファイルを作成し、その View に入るか、既存の IoT トランスポートプロファイル View に入ります。

undo iot transport-profile コマンドは IoT トランスポートプロファイルを削除します。

IoT トランスポートプロファイルには、IoT データを送信する宛先のサーバアドレスや、レポート間隔などを設定します。

IoT トランスポートプロファイルは最大 8 個まで作成できます。

IoT トランスポートプロファイルを削除する場合、事前に IoT トランスポートプロファイルのバインド設定を解除する必要があります。

例

#IoT トランスポートプロファイル azureiothub を作成し、その view に移行します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub]

関連コマンド

iot-transport-profile

20.2.10 iot-transport-profile

Syntax

iot-transport-profile *transport-profile-name*

undo iot-transport-profile *transport-profile-name*

デフォルト

設定なし

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

transport-profile-name: IoT トランスポートプロファイル名を指定します。IoT トランスポートプロファイル名は、大文字と小文字は区別しない 1～63 文字の文字列です。

説明

iot-transport-profile コマンドは IoT トランスポートプロファイルをバインドします。

undo iot-transport-profile コマンドはデフォルトに戻します。

オンライン AP は、グローバルコンフィグレーション view で IoT トランスポートプロファイルをバインドした後にのみ、IoT データをサーバにレポートします。

既存の IoT トランスポートプロファイル名のみを指定できます。

このコマンドを複数回実行した場合、最新の設定が有効になります。

例

#グローバルコンフィグレーション View で、IoT トランスポートプロファイル azureiothub をバインドします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] iot-transport-profile azureiothub

関連コマンド

iot transport-profile

20.2.11 keepalive interval

Syntax

keepalive interval *interval*

undo keepalive interval

デフォルト

60 秒

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

interval: キープアライブパケットを送信する間隔を 1~600 秒の範囲で指定します。

説明

keepalive interval コマンドは装置がサーバにキープアライブパケットを送信する間隔を設定します。

undo keepalive interval コマンドはデフォルトに戻します。

例

#キープアライブパケットを 50 秒毎にサーバに送信するように設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub] keepalive interval 50

関連コマンド

iot transport-profile

20.2.12 report interval

Syntax

report interval *interval*

undo report interval

デフォルト

60 秒

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

interval: IoT データをサーバにレポートする間隔を 1~600 秒の範囲で指定します。

説明

report interval コマンドは IoT データをサーバにレポートする間隔を設定します。

undo report interval コマンドはデフォルトに戻します。

レポートする間隔が長すぎるとサービスに影響しますが、間隔を短くすると AC の負荷が増加するため、適切な値を設定する必要があります。

例

#50 秒毎に IoT データをサーバにレポートするように設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub] report interval 50

関連コマンド

iot transport-profile

20.2.13 server-url

Syntax

server-url *server-url-string*

undo server-url

デフォルト

設定なし

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

server-url-string: サーバの URL を指定します。サーバの URL は、大文字と小文字を区別する 1～127 文字の文字列です。

説明

server-url コマンドは IoT データレポート用のサーバの URL を設定します。

undo server-url コマンドはデフォルトに戻します。

IoT トランスポートプロファイルを有効にする前に、このコマンドを設定する必要があります。

サーバの URL を編集する場合、事前に IoT トランスポートプロファイルを無効にする必要があります。

このコマンドを複数回実行した場合は、最新の設定が有効になります。

例

#IoT データレポート用のサーバの URL を global.azure-devices-provisioning.net として設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub] server-url global.azure-devices-provisioning.net

関連コマンド

iot transport-profile

20.2.14 transport-profile enable

Syntax

transport-profile enable

undo transport-profile enable

デフォルト

無効

View

IoT transport profile view

定義済みユーザロール

network-admin

説明

transport-profile enable コマンドは IoT トランスポートプロファイルを有効にします。

undo transport-profile enable コマンドはデフォルトに戻します。

例

#IoT トランスポートプロファイル azureiothub を有効にします。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub] transport-profile enable

関連コマンド

iot transport-profile

20.3 AeroScoutロケーションの設定コマンド

🕮 **メモ：**

この章のコマンドは、ソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

20.3.1 rfid-tracking aeroscout

Syntax

rfid-tracking aeroscout { disable | enable }

undo rfid-tracking aeroscout

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 無効

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

説明

rfid-tracking aeroscout enable コマンドは AeroScout ロケーションを有効にします。

rfid-tracking aeroscout disable コマンドは AeroScout ロケーションを無効にします。

undo rfid-tracking aeroscout コマンドはデフォルトに戻します。

この機能により、AP はサポートされているすべてのチャネルをスキャンします。すべてのチャネルにデバイスを配置しない場合は、チャネルスキャンホワイトリストまたはブラックリストを設定します。チャネルスキャンホワイトリストおよびブラックリストの詳細は、オペレーションマニュアルのセクション 2 *WLAN "チャネルスキャンの設定"*を参照してください。

AP がロケーションパケットをロケーションサーバに送信するには、AeroScout ロケーションと無線ベースロケーションの両方を有効にする必要があります。

例

AP ap1 で、AeroScout ロケーションを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking aeroscout enable

AP グループ 1 の AP で、AeroScout ロケーションを有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking aeroscout enable

#グローバルで、AeroScout ロケーションを有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking aeroscout enable

関連コマンド

rfid-tracking radio

20.3.2 rfid-tracking aeroscout aggregate-report interval

Syntax

rfid-tracking aeroscout aggregate-report interval *interval*

undo rfid-tracking aeroscout aggregate-report interval

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: MU ロケーションパケットを集約せずに送信します

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

interval:集約した MU ロケーションパケットのレポート間隔を 100~600000 ミリ秒の範囲で指定します。

説明

rfid-tracking aeroscout aggregate-report interval コマンドは、MU ロケーションパケットの集約を有効にし、集約した MU ロケーションパケットをレポートする間隔を設定します。

undo rfid-tracking aeroscout aggregate-report interval コマンドはデフォルトに戻します。

デフォルトでは、AP は MU ロケーションパケットを受信するとすぐに、そのパケットをロケーションサーバに報告します。これは多くのネットワークリソースを消費します。

この機能を使用すると、AP は受信した MU ロケーションパケットを 1 つのロケーションパケットに集約し、集約したパケットを指定した間隔でロケーションサーバに報告します。集約パケットのサイズが 1400 バイトに達すると、AP はロケーションパケットを直ちにロケーションサーバに報告します。

この機能は、AeroScout ロケーションモードがスタティックモードの場合にだけ有効です。

例

AP ap1 で、MU ロケーションパケットの集約を有効にし、レポート間隔を 100 ミリ秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking aeroscout aggregate-report interval 100

AP グループ 1 の AP で、MU ロケーションパケットの集約を有効にし、レポート間隔を 100 ミリ秒に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking aeroscout aggregate-report interval 100

#グローバルで、MU ロケーションパケットの集約を有効にし、レポート間隔を 100 ミリ秒に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking aeroscout aggregate-report interval 100

関連コマンド

rfid-tracking aeroscout

20.3.3 rfid-tracking aeroscout engine-address

Syntax

rfid-tracking aeroscout engine-address *engine-address* **engine-port** *engine-port*

undo rfid-tracking aeroscout engine-address

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 設定なし

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

engine-address : AeroScout ロケーションサーバの IPv4 アドレスを指定します。

engine-port : AeroScout ロケーションサーバのポート番号を 1~65535 の範囲で指定します。

説明

rfid-tracking aeroscout engine-address コマンドは、AeroScout ロケーションサーバの IPv4 アドレスとポート番号を設定します。

undo rfid-tracking aeroscout engine-address コマンドはデフォルトに戻します。

AP がロケーションサーバと通信するために、ロケーションサーバの IPv4 アドレスとポート番号を指定します。スタティック AeroScout ロケーションが使用されている場合、この機能を設定する必要があります。ダイナミック AeroScout ロケーションが使用されている場合、この機能は有効になりません。

例

AP ap1 で、ロケーションサーバの IPv4 アドレスを 192.168.10.10、ポート番号を 3000 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking aeroscout engine-address 192.168.10.10 engine-port 3000

AP グループ 1 の AP で、ロケーションサーバの IPv4 アドレスを 192.168.10.10、ポート番号を 3000 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking aeroscout engine-address 192.168.10.10 engine-port 3000

#グローバルで、ロケーションサーバの IPv4 アドレスを 192.168.10.10、ポート番号を 3000 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking aeroscout engine-address 192.168.10.10 engine-port 3000

関連コマンド

rfid-tracking aeroscout engine-detection

20.3.4 rfid-tracking aeroscout engine-detection

Syntax

rfid-tracking aeroscout engine-detection { dynamic | static }

undo rfid-tracking aeroscout engine-detection

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: ダイナミックロケーション

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

dynamic：ダイナミックロケーションを指定します。

static：スタティックロケーションを指定します。

説明

rfid-tracking aeroscout engine-detection コマンドは、AeroScout ロケーションモードを指定します。

undo rfid-tracking aeroscout engine-detection コマンドはデフォルトに戻します。

AeroScout ロケーションには、次のロケーションモードがあります。

- ダイナミックロケーション：AP はロケーションサーバとネゴシエーションを行い、タグのマルチキャスト MAC アドレス、パケット間引きの設定、およびロケーションサーバの IP アドレスとポート番号を取得します。ロケーションサーバは、AP の AeroScout バージョン、MAC アドレス、無線モード、およびチャネル情報を取得します。次に、ロケーションサーバは AP にロケーションパケットを送信するように通知します。
- スタティックロケーション：AP は AC から定義済みのロケーション属性を取得し、ロケーションサーバへのロケーションパケットの送信を開始します。ロケーションサーバが AP によるダイナミックネゴシエーションをサポートしていない場合は、スタティック AeroScout ロケーションを使用します。

例

AP ap1 で、AeroScout ロケーションモードをダイナミックロケーションに設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking aeroscout engine-detection dynamic

AP グループ 1 の AP で、AeroScout ロケーションモードをダイナミックロケーションに設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking aeroscout engine-detection dynamic

#グローバルで、AeroScout ロケーションモードをダイナミックロケーションに設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking aeroscout engine-detection dynamic

20.3.5 rfid-tracking aeroscout report-mode

Syntax

rfid-tracking aeroscout report-mode { central | local }

undo rfid-tracking aeroscout report-mode

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view：AP(ローカルレポートモード)

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

central : AC(集中レポートモード)を指定します。

local : AP(ローカルレポートモード)を指定します。

説明

rfid-tracking aeroscout report-mode コマンドは、AeroScout ロケーションパケットのレポートモードを指定します。

undo rfid-tracking aeroscout report-mode コマンドはデフォルトに戻します。

ロケーションサーバにロケーションパケットをレポートするモードには、AC (集中レポートモード) と AP (ローカルレポートモード) があります。AC(集中レポートモード)では、AP は最初にロケーションパケットを AC に送信する必要があります。

例

AP ap1 で、AeroScout ロケーションパケットのレポートモードを AC(集中レポートモード)に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking aeroscout report-mode central

AP グループ 1 の AP で、AeroScout ロケーションパケットのレポートモードを AC(集中レポートモード)に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking aeroscout report-mode central

#グローバルで、AeroScout ロケーションパケットのレポートモードを AC(集中レポートモード)に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking aeroscout report-mode central

20.3.6 rfid-tracking aeroscout tag-multicast-address

Syntax

rfid-tracking aeroscout tag-multicast-address *mac-address*

undo rfid-tracking aeroscout tag-multicast-address

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view：設定なし

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

engine-address : タグのマルチキャスト MAC アドレスを H-H-H の形式で指定します。

説明

rfid-tracking aeroscout tag-multicast-address コマンドは、タグのマルチキャスト MAC アドレスを指定します。

undo rfid-tracking aeroscout tag-multicast-address コマンドはデフォルトに戻します。

AP は、受信したワイヤレスパケットの宛先 MAC アドレスによってタグを識別します。タグのマルチキャスト MAC アドレスを指定しない場合、AP は受信した 802.11 パケットがすべて MU からのものであると判断します。

スタティック AeroScout ロケーションが設定されている場合、タグのマルチキャスト MAC アドレスの指定が必要です。ダイナミック AeroScout ロケーションが使用されている場合、この機能は有効になりません。

例

AP ap1 で、タグのマルチキャスト MAC アドレスとして 0134-1122-3344 を設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking aeroscout tag-multicast-address 0134-1122-3344

#AP グループ 1 の AP で、タグのマルチキャスト MAC アドレスとして 0134-1122-3344 を設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking aeroscout tag-multicast-address 0134-1122-3344

#グローバルで、タグのマルチキャスト MAC アドレスとして 0134-1122-3344 を設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking aeroscout tag-multicast-address 0134-1122-3344

関連コマンド

rfid-tracking aeroscout engine-detection

20.3.7 rfid-tracking aeroscout timestamp

Syntax

rfid-tracking aeroscout timestamp { absolute | relative }

undo rfid-tracking aeroscout timestamp

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view：相対タイムスタンプ

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

absolute：絶対タイムスタンプを指定します。絶対タイムスタンプは、1970 年からの経過時間をミリ秒単位で表します。

relative：相対タイムスタンプを指定します。相対タイムスタンプは、AP が起動してからの経過時間をミリ秒単位で表します。

説明

rfid-tracking aeroscout timestamp コマンドは、MU パケットをカプセル化するタイムスタンプの形式を指定します。

undo rfid-tracking aeroscout timestamp コマンドはデフォルトに戻します。

タグパケットは、相対時間だけでカプセル化できます。MU パケットが相対タイムスタンプと絶対タイムスタンプのどちらでカプセル化されるかは、ロケーションサーバの設定によって異なります。一部のベンダのロケーションサーバは、絶対タイムスタンプでカプセル化された MU パケットだけをサポートしています。

例

AP ap1 で、タイムスタンプの形式を絶対タイムスタンプに設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking aeroscout timestamp absolute

AP グループ 1 の AP で、タイムスタンプの形式を絶対タイムスタンプに設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking aeroscout timestamp absolute

#グローバルで、タイムスタンプの形式を絶対タイムスタンプに設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking aeroscout timestamp absolute

関連コマンド

rfid-tracking aeroscout

20.3.8 rfid-tracking aeroscout vendor-port

Syntax

rfid-tracking aeroscout vendor-port *vendor-port-number*

undo rfid-tracking aeroscout vendor-port

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view：1144 ポート

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

vendor-port-number :ポート番号を 1~65535 の範囲で指定します。

説明

rfid-tracking aeroscout vendor-port コマンドは、AP がロケーションサーバからのメッセージを受信するポートを指定します。

undo rfid-tracking aeroscout vendor-port コマンドはデフォルトに戻します。

AP がロケーションサーバからのメッセージを受信するポートを指定するには、このコマンドを実行します。スタティック AeroScout ロケーションが設定されている場合、AP は指定されたポートから受信したパケットに応答しません。

例

AP ap1 で、AP がロケーションサーバからのメッセージを受信するポートを 3000 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking aeroscout vendor-port 3000

AP グループ 1 の AP で、AP がロケーションサーバからのメッセージを受信するポートを 3000 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking aeroscout vendor-port 3000

#グローバルで､AP がロケーションサーバからのメッセージを受信するポートを 3000 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking aeroscout vendor-port 3000

関連コマンド

- **rfid-tracking aeroscout**
- **rfid-tracking aeroscout engine-detection**

20.3.9 rfid-tracking mode

Syntax

rfid-tracking mode { mu | tag }

undo rfid-tracking mode { mu | tag }

デフォルト

Radio view: AP group radio view の設定を使用します。

AP group radio view: 設定なし

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

mu :MU を指定します。

tag :タグを指定します。

説明

rfid-tracking mode コマンドは、検索するデバイスのタイプを指定します。

undo rfid-tracking mode コマンドは、指定されたデバイスのタイプを削除します。

rfid-tracking mode コマンドを実行すると、AP は指定されたタイプのデバイスに関するロケーション情報だけをロケーションサーバに送信します。

検出するデバイスのタイプとして、**mu** と **tag** の最低限どちらか一方の設定が必要です。

このコマンドを複数回実行して、MU とタグの両方を検索するように AP を設定できます。

例

AP ap1 で、検索するデバイスのタイプを MU に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rfid-tracking mode mu

AP グループ 1 の型番 QX-W1110 の AP で、検索するデバイスのタイプを MU に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-radio-1] rfid-tracking mode mu

関連コマンド

rfid-tracking aeroscout

20.3.10 rfid-tracking radio

Syntax

rfid-tracking radio { disable | enable }

undo rfid-tracking radio

デフォルト

Radio view: AP group radio view の設定を使用します。

AP group radio view: 無効

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

説明

rfid-tracking radio enable コマンドは、無線ベースのロケーションを有効にします。

rfid-tracking radio disable コマンドは、無線ベースのロケーションを無効にします。

undo rfid-tracking radio コマンドは、デフォルトに戻します。

AP がロケーションパケットをロケーションサーバに送信するには、AeroScout ロケーションと無線ベースのロケーションを両方有効にする必要があります。

例

AP ap1 で、無線ベースのロケーションを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rfid-tracking radio enable

AP グループ 1 の型番 QX-W1110 の AP で、無線ベースのロケーションを有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-radio-1] rfid-tracking radio enable

関連コマンド

rfid-tracking aeroscout

20.4 ワイヤレスロケーション共通パラメータの設定コマンド

🕮 **メモ：**

この章のコマンドは、ソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

20.4.1 display wlan rfid-tracking radio

Syntax

display wlan rfid-tracking radio [ap *ap-name* **]**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan rfid-tracking radio コマンドは、ワイヤレスロケーションの無線情報を表示します。

例

#ワイヤレスロケーションの無線情報を表示します。

<AC> display wlan rfid-tracking radio

```
                    Wireless Locating
--------------------------------------------------------------------------
 AP name                       Radio ID   Type
--------------------------------------------------------------------------
 ap1                           1          MU/Tag
 ap2                           1          MU
 ap3                           2          Tag
 ap4                           1          N/A
--------------------------------------------------------------------------
```

表 20-5 コマンド出力

フィールド	説明
Type	検索するデバイスのタイプ : • MU/Tag : MUデバイスとTagデバイスの両方 • MU : MUデバイス • Tag : Tagデバイス • N/A : 検索するデバイスのタイプが指定されていません

20.4.2 rfid-tracking client rate-limit

Syntax

rfid-tracking client rate-limit { disable | enable }

undo rfid-tracking client rate-limit

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 無効

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

説明

rfid-tracking client rate-limit enable コマンドは AP のワイヤレスパケットの受信レート制限を有効にします。

rfid-tracking client rate-limit disable コマンドは AP のワイヤレスパケットの受信レート制限を無効にします。

undo rfid-tracking client rate-limit コマンドはデフォルトに戻します。

この機能を使用すると、AP は CIR と CBS の両方を超過した場合に、過剰なクライアントパケットからのロケーション情報を報告できなくなります。各クライアントのロケーション情報をロケーションサーバに送信できるようになり、クライアントパケットが AP にフラッディングするのを防ぐことができます。

パケットの間引きが有効になっている場合、この機能は間引きされたパケットのレートを制限します。

例

AP ap1 で、ワイヤレスパケットの受信レート制限を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking client rate-limit enable

AP グループ 1 の AP で、ワイヤレスパケットの受信レート制限を有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking client rate-limit enable

#グローバルで、ワイヤレスパケットの受信レート制限を有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking client rate-limit enable

関連コマンド

rfid-tracking client rate-limit cir

20.4.3 rfid-tracking client rate-limit cir

Syntax

rfid-tracking client rate-limit cir *cir* **[cbs** *cbs* **]**

undo rfid-tracking client rate-limit cir

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: CIR は 0、CBS は 0

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

cir *cir*: 受信ワイヤレスパケットの CIR を 1 から 1300000 kbps の範囲で指定します。

cbs *cbs*: 受信ワイヤレスパケットの CBS を 80 から 130000000 バイトの範囲で指定します。デフォルトの CBS は CIR×700 バイトです。

説明

rfid-tracking client rate-limit cir コマンドはワイヤレスパケットの受信レートの制限値を設定します。

undo rfid-tracking client rate-limit cir コマンドはデフォルトに戻します。

CIR および CBS の設定は、ワイヤレスパケットの受信レート制限を有効にした場合にのみ有効になります。

例

AP ap1 で、受信ワイヤレスパケットの CIR と CBS をそれぞれ 200000 kbps と 50000 バイトに設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking client rate-limit cir 200000 cbs 50000

AP グループ 1 の AP で、受信ワイヤレスパケットの CIR と CBS をそれぞれ 200000 kbps と 50000 バイトに設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking client rate-limit cir 200000 cbs 50000

#グローバルで、受信ワイヤレスパケットの CIR と CBS をそれぞれ 200000 kbps と 50000 バイトに設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking client rate-limit cir 200000 cbs 50000

関連コマンド

rfid-tracking client rate-limit

20.4.4 rfid-tracking dilution

Syntax

rfid-tracking dilution { disable | enable }

undo rfid-tracking dilution

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 無効

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

説明

rfid-tracking dilution enable コマンドは AP のパケットの間引きを有効にします。

rfid-tracking dilution disable コマンドは AP のパケットの間引きを無効にします。

undo rfid-tracking dilution コマンドはデフォルトに戻します。

この機能を使用すると、AP は特定の数のワイヤレスパケットを受信したとき、または特定の間隔でロケーションパケットを送信します。これにより、ロケーションサーバと AP の負荷を軽減することができます。

例

AP ap1 で、パケットの間引きを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking dilution enable

AP グループ 1 の AP で、パケットの間引きを有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking dilution enable

#グローバルで、パケットの間引き有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking dilution enable

関連コマンド

rfid-tracking dilution factor

20.4.5 rfid-tracking dilution factor

Syntax

rfid-tracking dilution factor *factor* **timeout** *timeout*

undo rfid-tracking dilution factor

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 設定なし

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

factor *factor*: パケットの間引き係数を 1～10000 の範囲で指定します。

timeout *timeout*:パケットの間引きタイムアウトタイマを 1~60 秒の範囲で指定します。

説明

rfid-tracking dilution factor コマンドはパケットの間引き係数を設定します。

undo rfid-tracking dilution factor コマンドはデフォルトに戻します。

パケットの間引き係数を 10、タイムアウトタイマを 5 秒に設定した場合、パケットの間引きは次のように動作します。

- AeroScout ロケーションまたは RF フィンガープリントが有効の場合、AP は MU クライアントから、10 個のワイヤレスパケット(管理パケット、ブロードキャストパケットを除く)を受信するたびにロケーションパケットを送信します。タイムアウトのタイマ時間が経過する前に AP が MU クライアントから 10 個のワイヤレスパケットを受信できなかった場合、AP は最新のワイヤレスパケットをロケーションサーバに送信します。
- CUPID ロケーションが有効の場合、AP は関連付けられていないクライアントから 10 個のプローブ要求を受信するたびにロケーション測定を実行します。タイムアウトのタイマが経過する前に AP がアソシエートされていないクライアントから 10 個のプローブ要求を受信できなかった場合、タイマが時間切れになると AP はロケーション測定を実行します。

例

AP ap1 で、パケットの間引き係数を 10、パケットの間引きタイムアウトタイマを 10 秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking dilution factor 10 timeout 10

#AP グループ 1 の AP で、パケットの間引き係数を 10、パケットの間引きタイムアウトタイマを 10 秒に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking dilution factor 10 timeout 10

#グローバルで、パケットの間引き係数を 10、パケットの間引きタイムアウトタイマを 10 秒に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking dilution factor 10 timeout 10

関連コマンド

rfid-tracking dilution

20.4.6 rfid-tracking ignore ap-frame

Syntax

rfid-tracking ignore ap-frame { disable | enable }

undo rfid-tracking ignore ap-frame

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 無効

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

説明

rfid-tracking ignore ap-frame enable コマンドは AP フレームの無視を有効にします。

rfid-tracking ignore ap-frame disable コマンドは AP フレームの無視を無効にします。

undo rfid-tracking ignore ap-frame コマンドはデフォルトに戻します。

AP フレームを無視すると、AP は受信した AP フレーム内の情報をロケーションサーバに送信できなくなります。AP フレームは、AP が他の AP から受信したフレームです。この機能は、AP を検索または監視する必要がない場合に設定します。

例

AP ap1 で、AP フレームの無視を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking ignore ap-frame enable

AP グループ 1 の AP で、AP フレームの無視を有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking ignore ap-frame enable

#グローバルで、AP フレームの無視を有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking ignore ap-frame enable

20.4.7 rfid-tracking ignore beacon

Syntax

rfid-tracking ignore beacon { disable | enable }

undo rfid-tracking ignore beacon

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 無効

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

説明

rfid-tracking ignore beacon enable コマンドはビーコンフレームの無視を有効にします。

rfid-tracking ignore beacon disable コマンドはビーコンフレームの無視を無効にします。

undo rfid-tracking ignore beacon コマンドはデフォルトに戻します。

ビーコンフレームを無視すると、AP は受信したビーコンフレームをロケーションサーバに送信できなくなります。

ビーコンフレームを無視することで、トラフィックフラッディングを防止します。

例

AP ap1 で、ビーコンフレームの無視を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking ignore beacon enable

AP グループ 1 の AP で、ビーコンフレームの無視を有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking ignore beacon enable

#グローバルで、ビーコンフレームの無視を有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking ignore beacon enable

20.4.8 rfid-tracking keepalive

Syntax

rfid-tracking keepalive { disable | enable }

undo rfid-tracking keepalive

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 無効

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

説明

rfid-tracking keepalive enable コマンドはワイヤレスロケーションのキープアライブを有効にします。

rfid-tracking keepalive disable コマンドはワイヤレスロケーションのキープアライブを無効にします。

undo rfid-tracking keepalive コマンドはデフォルトに戻します。

この機能を有効にすると、AP は 15 秒間隔で Hello パケットをロケーションサーバに送信します。ロケーションサーバが 30 秒以内に AP からパケットを受信しない場合、ロケーションサーバは AP がオフラインであると判断します。

例

AP ap1 で、ワイヤレスロケーションのキープアライブを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking keepalive enable

AP グループ 1 の AP で、ワイヤレスロケーションのキープアライブを有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking keepalive enable

#グローバルで、ワイヤレスロケーションのキープアライブを有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking keepalive enable

20.4.9 rfid-tracking rate-limit

Syntax

rfid-tracking rate-limit { disable | enable }

undo rfid-tracking rate-limit

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 無効

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

説明

rfid-tracking rate-limit enable コマンドは AP のロケーションパケットレート制限を有効にします。

rfid-tracking rate-limit disable コマンドは AP のロケーションパケットレート制限を無効にします。

undo rfid-tracking rate-limit コマンドはデフォルトに戻します。

この機能を使用すると、CIR と CBS の両方が超過した場合に、AP が過剰なロケーションパケットを破棄します。これにより、ロケーションパケットがロケーションサーバにフラッディングするのを防ぐことができます。

この機能は、AeroScout ロケーションまたは RF フィンガープリントが設定されている場合にだけ有効です。

例

AP ap1 で、ロケーションパケットレート制限を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking rate-limit enable

AP グループ 1 の AP で、ロケーションパケットレート制限を有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking rate-limit enable

#グローバルで、ロケーションパケットレート制限を有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking rate-limit enable

関連コマンド

rfid-tracking client rate-limit cir

20.4.10 rfid-tracking rate-limit cir

Syntax

rfid-tracking rate-limit cir *cir* **[cbs** *cbs* **]**

undo rfid-tracking rate-limit cir

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: CIR は 0、CBS は 0

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

cir *cir*: 受信ワイヤレスパケットの CIR を 8 から 1300000 kbps の範囲で指定します。

cbs *cbs*: 受信ワイヤレスパケットの CBS を 500 から 130000000 バイトの範囲で指定します。デフォルトの CBS は CIR×700 バイトです。

説明

rfid-tracking rate-limit cir コマンドはロケーションパケットの送信レートの制限値を設定します。

undo rfid-tracking rate-limit cir コマンドはデフォルトに戻します。

CIR および CBS の設定は、ロケーションパケットレート制限を有効にした場合にのみ有効になります。

例

AP ap1 で、送信ロケーションパケットの CIR と CBS をそれぞれ 800000 kbps と 50000 バイトに設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking rate-limit cir 800000 cbs 50000

AP グループ 1 の AP で、送信ロケーションパケットの CIR と CBS をそれぞれ 800000 kbps と 50000 バイトに設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking rate-limit cir 800000 cbs 50000

#グローバルで、送信ロケーションパケットの CIR と CBS をそれぞれ 800000 kbps と 50000 バイトに設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking rate-limit cir 800000 cbs 50000

関連コマンド

rfid-tracking client rate-limit

20.4.11 rfid-tracking rssi

Syntax

rfid-tracking rssi { disable | enable }

undo rfid-tracking rssi

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 無効

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

説明

rfid-tracking rssi enable コマンドは RSSI ベースのパケットフィルタリングを有効にします。

rfid-tracking rssi disable コマンドは RSSI ベースのパケットフィルタリングを無効にします。

undo rfid-tracking rssi コマンドはデフォルトに戻します。

RSSI ベースのパケットフィルタリングが有効の場合、AP は RSSI しきい値よりも低い RSSI を持つパケットのロケーション情報を報告しません。この機能により、AP は AP から遠く離れたクライアントを見つけることができなくなります。

例

AP ap1 で、RSSI ベースのパケットフィルタリングを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking rssi enable

AP グループ 1 の AP で、RSSI ベースのパケットフィルタリングを有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking rssi enable

#グローバルで、RSSI ベースのパケットフィルタリングを有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking rssi enable

関連コマンド

rfid-tracking rssi threshold

20.4.12 rfid-tracking rssi threshold

Syntax

rfid-tracking rssi threshold *rssi-threshold*

undo rfid-tracking rssi threshold

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 5 (–123 dBm)

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

threshold *rssi-threshold*: パケットフィルタリングの RSSI しきい値を 5(-123dBm)から 100(-28 dBm) の範囲で指定します。

説明

rfid-tracking rssi threshold コマンドは RSSI ベースのパケットフィルタリングの RSSI しきい値を設定します。

undo rfid-tracking rssi threshold コマンドはデフォルトに戻します。

AP は、指定された RSSI しきい値よりも RSSI が低いパケットの位置情報を報告しません。このコマンドは、RSSI ベースのパケットフィルタリングが有効の場合にのみ有効です。

例

AP ap1 で、RSSI ベースのパケットフィルタリングの RSSI しきい値を 50 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking rssi threshold 50

AP グループ 1 の AP で、RSSI ベースのパケットフィルタリングの RSSI しきい値を 50 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking rssi threshold 50

#グローバルで、RSSI ベースのパケットフィルタリングの RSSI しきい値を 50 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking rssi threshold 50

関連コマンド

rfid-tracking rssi

目次

このセクションのページは **2-x-x** です。

21 章 Web リダイレクトの設定 21-1
21.1 Web リダイレクトの設定コマンド 21-1
21.1.1 web-redirect url 21-1

21章 Web リダイレクトの設定

21.1 Webリダイレクトの設定コマンド

21.1.1 web-redirect url

🕮 **メモ：**

このコマンドは、ソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

web-redirect url *url-string* **[interval** *interval* **]**

undo web-redirect

デフォルト

無効

Viwe

service-template view

定義済みのユーザーロール

network-admin

パラメータ

url *url-string*：ユーザのリダイレクト先の URL を 1 文字から 256 文字の文字列で指定します。URL は存在する URL を指定してください。形式は、http://または https://で始まる完全な URL であることを確認してください。

interval *interval*：指定した URL にユーザがリダイレクトされる時間間隔を指定します。60 秒から 86400 秒の範囲で指定します。デフォルトの間隔は 86400 秒です。

説明

web-redirect url コマンドは Web リダイレクト機能を有効にします。

undo web-redirect url コマンドは Web リダイレクト機能を無効にします。

この機能は、Web ブラウザを介して外部ネットワークにアクセスする前に、ユーザを指定された URL にリダイレクトします。指定された間隔が経過してから、HTTP のサイト

へ移動しようとすると、ユーザは訪問中の Web サイトから指定された URL に再度リダイレクトされます。

Web リダイレクト機能は、デフォルトのポート番号 80 を使用する HTTP パケットに対してのみ有効です。

url *url-string* オプションを使用することで、 異なるユーザに異なる広告ページを発信することができます。

設定パラメータは以下の通りです。

・userip=%c:ユーザの IP アドレスです。

・usermac=%m:ユーザの MAC アドレスです。

・nasid=%n:デバイスの NAS 識別子です。

・ssid=%E:ユーザが関連付ける SSID です。

・originalurl=%o:ユーザがブラウザに入力する元の URL です

パラメータ形式は以下の形式に準拠していることを確認してください。

http://XXXX/index.html?userip=%c&usermac=%m&nasid=%n&ssid=%E&originalurl=%o

例

#サービステンプレート service 1 で Web リダイレクトを設定します。リダイレクト URL を **http://192.0.0.1/index.html?userip=%c&usermac=%m&nasid=%n&ssid=%E&originall=%o** に設定します。間隔は 3600 秒に設定します。

<AC> system-view

[AC] wlan service-template service-template1

[AC-wlan-st-service-template1] web-redirect url http://192.0.0.1/index.html?userip=%c&usermac=%m&nasid=%n&ssid=%E&originalurl=%o interval 3600

目次

このセクションのページは **2-x-x** です。

22 章 Hotspot 2.0 の設定 22-1
22.1 Hotspot 2.0 の設定コマンド 22-1
22.1.1 3gpp-info 22-1
22.1.2 authentication-type 22-2
22.1.3 comeback-delay 22-3
22.1.4 description 22-3
22.1.5 dgaf enable 22-4
22.1.6 display wlan hotspot uploaded-osu-icon 22-5
22.1.7 domain-name 22-6
22.1.8 friendly-name 22-7
22.1.9 gas-limit 22-8
22.1.10 hessid 22-8
22.1.11 hotspot-policy 22-9
22.1.12 icon-file 22-10
22.1.13 ip-protocol 22-12
22.1.14 ip-type 22-13
22.1.15 method 22-14
22.1.16 nai 22-15
22.1.17 nai-realm 22-16
22.1.18 network-type 22-19
22.1.19 operator-name 22-20
22.1.20 osu-provider 22-21
22.1.21 osu-ssid 22-22
22.1.22 policy-name 22-23
22.1.23 roam-oi 22-23
22.1.24 uri 22-24
22.1.25 venue group 22-25
22.1.26 venue name 22-28
22.1.27 wan-metrics 22-29
22.1.28 wlan hotspot-policy 22-30
22.1.29 wlan hotspot osu-icon unload 22-31
22.1.30 wlan hotspot osu-icon upload 22-32
22.1.31 wlan osu-provider 22-33
22.1.32 wlan venue url-unescape-chars 22-33

22章 Hotspot 2.0 の設定

🕮 **メモ：**

Hotspot 2.0 の設定は、ソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

22.1 Hotspot 2.0の設定コマンド

22.1.1 3gpp-info

Syntax

3gpp-info country-code *mobile-country-code* **network-code** *mobile-network-code*

undo 3gpp-info country-code *mobile-country-code* **network-code**

mobile-network-code

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

mobile-country-code: モバイル国コード(MCC)を指定します。MCC は、クライアントが属する国を一意に識別する 3 桁の数値コードです。

mobile-network-code: モバイルネットワークコード(MNC)を指定します。モバイルネットワークコードは、クライアントが属するモバイルネットワークを一意に識別する 2 桁または 3 桁の数値コードです。

説明

3gpp-info コマンドは 3GPP 情報を設定します。

undo 3gpp-info コマンドは 3GPP 情報を削除します。

Hotspot 2.0 ポリシーでは、最大 32 個の国コードとモバイルネットワークコードの組み合わせを指定できます。

一つの国コードを複数のモバイルネットワークコードと組み合わせることができます。

例

3GPP 情報を設定するため、国コードを 460 に、ネットワークコードを 01 に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] 3gpp-info country-code 460 network-code 01

22.1.2 authentication-type

Syntax

authentication-type { **0** [**redirect-url** *url*] | **1** | **2 redirect-url** *url* | **3** }

undo authentication-type { **0** | **1** | **2** | **3** }

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

0: 使用条件への同意を指定します。

1: オンライン登録を指定します。

2: HTTP/HTTPS リダイレクトを指定します。

3: DNS リダイレクトを指定します。

redirect-url *url*: リダイレクトされた URL アドレスを指定します。

説明

authentication-type コマンドはネットワーク認証の種類を指定します。

undo authentication-type コマンドはネットワーク認証の種類を削除します。

Hotspot 2.0 ポリシーには、最大 4 つのネットワーク認証タイプを指定できます。

例

ネットワーク認証タイプを指定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] authentication-type 1

22.1.3 comeback-delay

Syntax

comeback-delay *value*

undo comeback-delay

デフォルト

1 TU

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

value: カムバック遅延を 1 から 1024 TU の範囲で指定します。1TU は 1024 μs に相当します。

説明

comeback-delay コマンドはクライアントが GAS カムバック要求を送信するためのカムバック遅延を設定します。

undo comeback-delay コマンドはデフォルトを復元します。

クライアントが多くの GAS カムバック要求を送信するのを防ぐことができます。

例

カムバック遅延を 10 TU に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] comeback-delay 10

22.1.4 description

Syntax

description *description* **lang-code** *lang-code*

undo description *description* **lang-code** *lang-code*

デフォルト

設定なし

View

OSU server view

定義済みユーザロール

network-admin

パラメータ

description: 説明を指定します。1 から 252 文字の文字列で、大文字と小文字が区別されます。

lang-code: 言語コードを指定します。デバイスは、一般的な国際標準をサポートします。

説明

description コマンドは OSU サーバの説明を設定します。

undo description コマンドは OSU サーバの説明を削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

OSU サーバには、最大 32 個の説明を設定できます。クライアントには、クライアントシステムと同じ言語の説明が 1 つ表示されます。

例

OSU サーバ 1 の説明を設定します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1] description "Free service for test purpose" lang-code eng

22.1.5 dgaf enable

Syntax

dgaf enable

undo dgaf enable

デフォルト

有効

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

説明

dgaf enable コマンドは Downstream Group-Addressed Forwarding(DGAF)を有効にします。

undo dgaf enable コマンドは DGAF を無効にします。

DGAF を使用すると、AP はすべてのダウンストリームワイヤレスブロードキャスト ARP パケットおよびワイヤレスマルチキャストパケットを転送できます。ダウンストリームマルチキャストを使用したスプーフィング攻撃を防止するには、AP の DGAF を無効にします。

DGAF を無効にする前に、Hotspot 2.0 ポリシーにバインドされているすべてのサービステンプレートが無効になっていることを確認します。

パケット損失を回避するには、DGAF を無効にする前にプロキシ ARP とマルチキャスト最適化を有効にします。プロキシ ARP の詳細については、オペレーションマニュアルのセクション 5 *IP サービス*“*Proxy ARP*”を参照してください。

例

DGAF を無効にします。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] undo dgaf enable

22.1.6 display wlan hotspot uploaded-osu-icon

Syntax

display wlan hotspot uploaded-osu-icon

View

Any view

定義済みユーザロール

network-admin

network-operator

説明

display wlan hotspot uploaded-osu-icon コマンドはアップロードされた OSU サーバアイコンのリストを表示します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

例

アップロードされた OSU サーバアイコンのリストを表示します。

<AC> display wlan hotspot uploaded-osu-icon

```
Total uploaded osu icon count: 1
Icon name                       Icon type
--------------------------------------------------------------------------------
college.png                     png
```

関連コマンド

- **icon-file**
- **wlan hotspot osu-icon upload**

22.1.7 domain-name

Syntax

domain-name *domain-name*

undo domain-name *domain-name*

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

domain-name: ドメイン名を指定します。大文字と小文字が区別される 1 から 255 文字の文字列です。

説明

domain-name コマンドはドメイン名を設定します。

undo domain-name コマンドはドメイン名を削除します。

1 つの Hotspot 2.0 ポリシーでは、最大 32 個のドメイン名を設定できます。

例

Hotspot 2.0 ポリシー1 でドメイン名を college に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] domain-name college

22.1.8 friendly-name

Syntax

friendly-name *friendly-name* **lang-code** *lang-code*

undo friendly-name *friendly-name* **lang-code** *lang-code*

デフォルト

設定なし

View

OSU server view

定義済みユーザロール

network-admin

パラメータ

description: 説明を指定します。1 から 252 文字の文字列で、大文字と小文字が区別されます。

lang-code: 言語コードを指定します。デバイスは、一般的な国際標準をサポートします。

説明

friendly-name コマンドは OSU サーバの名前を設定します。

undo friendly-name コマンドは指定した OSU サーバ名を削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。OSU サーバには最大 32 個の名前を設定できます。クライアントには、クライアントシステムと同じ言語の名前が表示されます。

OSU サーバがすでに Hotspot 2.0 ポリシーにバインドされている場合、サーバに指定された最新の名前を削除することはできません。

例

OSU サーバ 1 の名前を設定します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1] friendly-name osu1 lang-code en

22.1.9 gas-limit

Syntax

gas-limit number *number* **interval** *interval*

undo gas-limit

デフォルト

AC が受信できる GAS 初期要求の数に制限はありません。

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

number *number*: AC が受信できる GAS 初期要求の最大数を 10 から 60 の範囲で指定します。

Interval *interval*: AC が GAS 初期要求を受信する間隔を 10 から 60 秒の範囲で指定します。

説明

gas-limit コマンドは AC が指定された間隔内に受信できる GAS 初期要求の最大数を設定します。

undo gas-limit コマンドはデフォルトを復元します。

AC が受信した GAS 初期要求の数が制限を超えた場合、超過したフレームは廃棄されます。

例

AC が 15 秒以内に受信できる GAS 初期要求の最大数を 50 に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] gas-limit number 50 interval 15

22.1.10 hessid

Syntax

hessid *hessid*

undo hessid

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

hessid: 同一 ESS を一意に識別する HESSID を H-H-H 形式で指定します。値をすべてゼロにすることはできません。

説明

hessid コマンドは同一 ESS 識別子(HESSID)を設定します。

undo hessid コマンドはデフォルトを復元します。

HESSID を設定する前に、Hotspot 2.0 ポリシーにバインドされているすべてのサービステンプレートが無効になっていることを確認してください。

例

Hotspot 2.0 ポリシー1 で HESSID を 0000-5e00-5310 に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] hessid 0000-5e00-5310

22.1.11 hotspot-policy

Syntax

hotspot-policy *policy-number*

undo hotspot-policy

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

policy-number: Hotspot 2.0 ポリシーの番号を 1 から 32 の範囲で指定します。

説明

hotspot-policy コマンドは Hotspot 2.0 ポリシーをサービステンプレートにバインドします。

undo hotspot-policy コマンドはデフォルトに戻します。

Hotspot 2.0 ポリシーをサービステンプレートにバインドする場合は、次のガイドラインに従ってください。

- Hotspot 2.0 ポリシーが存在し、サービステンプレートが無効になっていることを確認してください。
- サービステンプレートが次のように設定されていることを確認してください。
  - 802.1X 認証および鍵管理モード
  - RSN IE
  - AES-CCMP 暗号スイート

例

Hotspot 2.0 ポリシー1 をサービステンプレート 1 にバインドします。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] hotspot-policy 1

22.1.12 icon-file

Syntax

icon-file *filename* **lang-code** *lang-code* **icon-type** *icon-type*

undo icon-file *filename*

デフォルト

設定なし

View

OSU server view

定義済みユーザロール

network-admin

パラメータ

filename: アイコンファイルを名前で指定します。1 から 63 文字の文字列で、大文字と小文字が区別されます。

lang-code *lang-code*: 言語コードを指定します。デバイスは、一般的な国際標準をサポートしています。

icon-type *icon-type*: アイコンファイルの種類を指定します。1 から 15 文字の文字列で、大文字と小文字が区別されます。

説明

icon-file コマンドは OSU サーバのアイコンを指定します。

undo icon-file コマンドは OSU サーバの指定したアイコンを削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

コマンドが実行されると、デバイスは指定されたアイコンを読み込みます。OSU サーバには最大 6 つのアイコンを指定できます。クライアントには、クライアントシステムと同じ言語のアイコンが表示されます。

OSU サーバのアイコンを指定する場合は、次の制限とガイドラインに従ってください。

- バージョンファイルが保存されているルートディレクトリに icon という名前のディレクトリを作成し、FTP または TFTP を使用してアイコンファイルをフォルダにダウンロードしてからコマンドを実行します。
- 指定したアイコンファイルがアイコンディレクトリにない場合、アイコンファイルを読み込めません。アイコンファイルを読み込むには、アイコンディレクトリにアイコンファイルを保存してから、**wlan hotspot osu-icon upload** コマンドを実行してください。
- ファイルサイズは 64 KB を超えることはできません。
- コマンドで指定されたファイルの種類が実際のファイルの種類と同じであることを確認してください。
- OSU サーバがすでに Hotspot 2.0 ポリシーにバインドされている場合、最後に指定した OSU サーバのアイコンを削除することはできません。

例

OSU サーバ 1 のアイコンを指定します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1] icon-file test_icon lang-code eng icon-type png

22.1.13 ip-protocol

Syntax

ip-protocol { **esp** | **icmp** | **tcp** | **udp** } **port-number** *port-number* { **closed** | **open** | **unknown** }

undo ip-protocol { **esp** | **icmp** | **tcp** | **udp** } **port-number** *port-number*

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

esp: ESP プロトコルを指定します。

icmp: ICMP プロトコルを指定します。

tcp: TCP プロトコルを指定します。

udp: UDP プロトコルを指定します。

port-number: ポート番号を指定します。

表 22-1 ポート番号とプロトコル種別

プロトコル種別	ポート番号	説明
ICMP	0	診断で使用されます。
TCP	20	FTPで使用されます。
TCP	22	SSHで使用されます。
TCP	80	HTTPで使用されます。
TCP	443	TLS VPNで使用されます。
TCP	1723	Point to Point Tunneling Protocol VPNで使用されます。
TCP	5060	VoIPで使用されます。
UDP	500	IKEv2(IPSec VPN)で使用されます。
UDP	5060	VoIPで使用されます。
UDP	4500	IKEv2(IPSec VPN)で使用されます。
ESP	0	IPSec VPNで使用されます。

closed: ポートステータスをクローズとして指定します。

open: ポートステータスをオープンとして指定します。

unknown: ポートステータスを不明として指定します。

説明

ip-protocol コマンドは IP プロトコルのポートステータスを設定します。

undo ip-protocol コマンドは設定を削除します。

例

ポート番号を 20 に設定し、TCP のポートステータスをオープンに設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] ip-protocol tcp port-number 20 open

22.1.14 ip-type

🕮 **メモ**:

IPv6 は未サポートです。

Syntax

ip-type ipv4 *ipv4-type* **ipv6** *ipv6-type*

undo ip-type

デフォルト

可用性は、IPv4 アドレスの場合は 1、IPv6 アドレスの場合は 2 です。

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

ipv4-type: IPv4 アドレスの可用性を 0～7 の範囲で指定します。

表 22-2 IPv4 アドレスの可用性

アドレス値	説明
0	アドレスの種類は使用できません。
1	使用可能なパブリックIPv4アドレスです。

アドレス値	説明
2	使用可能なポート制限IPv4アドレスです。
3	使用可能な単一NATプライベートIPv4アドレスです。
4	使用可能なダブルNATプライベートIPv4アドレスです。
5	使用可能なポート制限付きIPv4アドレスおよび単一NAT IPv4アドレスです。
6	使用可能なポート制限付きIPv4アドレスおよびダブルNAT IPv4アドレスです。
7	アドレスタイプの可用性が不明です。

ipv6-type: IPv6 アドレスの可用性を 0～2 の範囲で指定します。

表 22-3 IPv6 アドレスの可用性

アドレス値	説明
0	アドレスの種類は使用できません。
1	使用可能なアドレスタイプです。
2	アドレスタイプの可用性が不明です。

説明

ip-type コマンドは IP アドレスの可用性を設定します。

undo ip-type コマンドはデフォルトに戻します。

例

可用性を IPv4 アドレスの場合は 2、IPv6 アドレスの場合は 1 に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] ip-type ipv4 2 ipv6 1

22.1.15 method

Syntax

method *method-id*

undo method *method-id*

デフォルト

設定なし

View

OSU server view

定義済みユーザロール

network-admin

パラメータ

method-id: プロトコル ID を指定します。

- 0: OMA-DM を指定します。
- 1: SOAP-XML SPP を指定します。

説明

method コマンドはクライアントが OSU サーバと通信するためのプロトコルを指定します。

undo method コマンドはクライアントが OSU サーバと通信するための指定されたプロトコルを削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

両方のプロトコルを指定できます。クライアントは、OSU サーバと通信するためのプロトコルを選択します。

OSU サーバが既に Hotspot 2.0 ポリシーにバインドされている場合は、クライアントが OSU サーバと通信するために指定された最新のプロトコルを削除することはできません。

例

クライアントが OSU サーバと通信するためのプロトコルを指定します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1] method 0

22.1.16 nai

Syntax

nai *nai*

undo nai

デフォルト

設定なし

View

OSU server view

定義済みユーザロール

network-admin

パラメータ

nai: NAI を指定します。1 から 252 文字の文字列で、大文字と小文字が区別されます。

説明

nai コマンドは OSU サーバのネットワークアクセス識別子(NAI)を設定します。

undo nai コマンドは OSU サーバに設定した NAI を削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

OSU サーバに対して NAI が設定されている場合、クライアントは OSEN OSU を介して OSU AP に接続します。OSU サーバに対して NAI が設定されていない場合、クライアントは Open OSU を介して OSU AP に接続します。

例

OSU サーバ 1 の NAI を設定します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1] nai abc@example.com

22.1.17 nai-realm

Syntax

nai-realm name *realm-name* **eap-method** *eap-method-id* **auth-method**

auth-method-id **authentication** *authentication*

undo nai-realm name *realm-name* [**eap-method** *eap-method-id* [**auth-method**

auth-method-id [**authentication** *authentication*]]]

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

name *realm-name*: NAI レルム名を指定します。1 から 255 文字の文字列で、大文字と小文字が区別されます。

eap-method *eap-method-id*: EAP 認証方式を ID で指定します。

表 22-4 EAP 認証方式

eap-method-id	説明
1	EAP-Transport Layer Security (EAP-TLS)
2	Lightweight Extensible Authentication Protocol (LEAP)
3	EAP for GSM Subscriber Identity Module (EAP-SIM)
4	EAP-Tunneled Transport Layer Security (EAP-TTLS)
5	EAP-Authentication and Key Agreement (EAP-AKA)
6	Protected EAP (PEAP)

auth-method *auth-method-id*: 認証方式を ID で指定します。

authentication *authentication*: 認証パラメータを ID で指定します。

表 22-5 認証方式および認証パラメータ

auth-method-id	auth-method-type	authentication
2	Non-EAP Inner Authentication Type	• 1: PAP • 2: CHAP • 3: MSCHAP • 4: MSCHAPV2
5	Credential Type	• 1: SIM • 2: USIM • 3: NFC Secure Element • 4: Hardware Token • 5: Soft Token • 6: Certificate • 7: username/password • 8: none

auth-method-id	auth-method-type	authentication
6	Tunneled EAP Method Credential Type	• 1: SIM • 2: USIM • 3: NFC Secure Element • 4: Hardware Token • 5: Soft Token • 6: Certificate • 7: username/password • 8: Reserved • 9: Anonymous

説明

nai-realm コマンドは NAI レルムを作成し、NAI レルムの認証タイプを指定します。

undo nai-realm コマンドは NAI レルムを削除します。

undo nai-realm コマンドを使用する場合は、次のガイドラインに従ってください。

- **undo nai-realm name** *realm-name* コマンドは、同じ名前を使用するすべての NAI レルムを削除します。
- **undo nai-realm name** *realm-name* **eap-method** *eap-method-id* コマンドは、同じ名前と EAP 認証方式を使用するすべての NAI レルムを削除します。
- **undo nai-realm name** *realm-name* **eap-method** *eap-method-id* **auth-method** *auth-method-id* コマンドは、同じ名前、EAP 認証方式、および認証方式を使用するすべての NAI レルムを削除します。
- **undo nai-realm name** *realm-name* **eap-method** *eap-method-id* **auth-method** *auth-method-id* **authentication** *authentication* コマンドは、同じ名前、EAP 認証方式、認証方式、および認証パラメータを使用するすべての NAI レルムを削除します。

Hotspot 2.0 ポリシーには、最大 32 の NAI レルム名を設定できます。

例

Hotspot 2.0 ポリシー1 で NAI レルム test の認証タイプを指定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] nai-realm name test eap-method 2 auth-method 5 authentication 1

22.1.18 network-type

Syntax

network-type *network-type* [**access-internet**]

undo network-type

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

network-type: ネットワークタイプを 0 から 5、14、および 15 の範囲で指定します。

表 22-6 アクセスネットワークタイプ

値	説明
0	プライベートネットワーク
1	ゲストアクセスのプライベートネットワーク
2	有料のパブリックネットワーク
3	無料のパブリックネットワーク
4	パーソナルデバイスネットワーク
5	緊急サービス専用ネットワーク
14	テストまたは実験用
15	ワイルドカード

access-internet: インターネットへのアクセスを有効にします。このキーワードを指定しない場合、インターネットにはアクセスできません。

説明

network-type コマンドはアクセスネットワークタイプを設定します。

undo network-type コマンドはデフォルトに戻します。

アクセスネットワークの種類を設定する前に、Hotspot 2.0 ポリシーにバインドされているすべてのサービステンプレートが無効になっていることを確認してください。

例

アクセスネットワークの種類を 1 に設定し、インターネットへのアクセスを有効にします。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] network-type 1 access-internet

22.1.19 operator-name

Syntax

operator-name *operator-name* **lang-code** *lang-code*

undo operator-name *operator-name* **lang-code** *lang-code*

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

operator-name: サービスプロバイダ名を指定します。1 から 252 文字の文字列で、大文字と小文字が区別されます。

lang-code: 言語コードを指定します。デバイスは、ISO 639-1 と ISO 639-2 の両方の規格をサポートしています。

説明

operator-name コマンドはサービスプロバイダ情報を設定します。

undo operator-name コマンドはサービスプロバイダ情報を削除します。

Hotspot 2.0 ポリシーでは、最大 32 個のサービスプロバイダと言語コードの組み合わせを構成できます。

例

サービスプロバイダ example の言語コードを en に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] operator-name example lang-code en

22.1.20 osu-provider

Syntax

osu-provider *osu-provider-number*

undo osu-provider *osu-provider-number*

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

osu-provider-number: OSU サーバを 1 から 32 の範囲の番号で指定します。指定された OSU サーバが存在している必要があります。

説明

osu-provider コマンドは OSU サーバを Hotspot 2.0 ポリシーにバインドします。

undo osu-provider コマンドは OSU サーバを Hotspot 2.0 ポリシーからバインド解除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

最大 32 台の OSU サーバを Hotspot 2.0 ポリシーにバインドできます。

OSU サーバを Hotspot 2.0 ポリシーにバインドする前に、次の設定が完了していることを確認してください。

- OSU サーバの名前を設定します。
- OSU サーバの URI を指定します。
- クライアントが OSU サーバと通信するためのプロトコルを指定します。
- OSU サーバのアイコンを指定します。

例

OSU サーバ 1 を Hotspot 2.0 ポリシー1 にバインドします。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] osu-provider 1

関連コマンド

- **friendly-name**
- **icon-file**
- **method**
- **uri**
- **wlan osu-provider**

22.1.21 osu-ssid

Syntax

osu-ssid *ssid-name*

undo osu-ssid

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

ssid-name: SSID 名を指定します。1 から 32 文字の文字列で、大文字と小文字が区別されます。

説明

osu-ssid コマンドはオンラインサインアップサービスの SSID を設定します。

undo osu-ssid コマンドはオンラインサインアップサービス用に設定した SSID を削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

オンラインサインアップサービス用に構成された SSID が、オンラインサインアップサービステンプレートの SSID と同じであることを確認します。

例

オンラインサインアップサービスの SSID を osu に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] osu-ssid osu

22.1.22 policy-name

Syntax

policy-name *name*

undo policy-name

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

name: Hotspot 2.0 ポリシー名を 1 から 32 文字の大文字と小文字を区別しない文字列で指定します。

説明

policy-name コマンドは Hotspot 2.0 ポリシーの名前を設定します。

undo policy-name コマンドはデフォルトを復元します。

例

Hotspot 2.0 ポリシー1 の名前を market に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] policy-name market

22.1.23 roam-oi

Syntax

roam-oi *oi* [**in-beacon**]

undo roam-oi *oi*

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

oi: ローミングコンソーシアムを一意に識別できる OI を、6 桁または 10 桁の 16 進数で指定します。

in-beacon: ビーコンに OI を追加します。ベストプラクティスとして、クライアントが OI を取得するには、このキーワードを指定します。

説明

roam-oi コマンドは組織識別子(OI)を設定します。

undo roam-oi コマンドは OI を削除します。

OI を設定する前に、Hotspot 2.0 ポリシーにバインドされているすべてのサービステンプレートが無効になっていることを確認します。Hotspot 2.0 ポリシーでは最大 32 の OI を構成でき、ビーコンには最大 3 つの OI を追加できます。

例

OI を 004096 に設定し、ビーコンに OI を追加します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] roam-oi 004096 in-beacon

22.1.24 uri

Syntax

uri *uri*

undo uri

デフォルト

設定なし

View

OSU server view

定義済みユーザロール

network-admin

パラメータ

uri: OSU サーバの URI を指定します。1 から 255 文字の文字列で、大文字と小文字が区別されます。

説明

uri コマンドは OSU サーバの URI を指定します。

undo uri コマンドは OSU サーバの構成済み URI を削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。クライアントは、構成された URI を使用して OSU サーバにアクセスし、オンラインサインアップを実行します。

OSU サーバがすでに Hotspot 2.0 ポリシーにバインドされている場合、サーバの構成された URI を削除することはできません。

例

OSU サーバ 1 の URI を指定します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1] uri https://osu-server.example.org/

22.1.25 venue group

Syntax

venue group *venue-group-number* **type** *venue-type-number*

undo venue group

デフォルト

設定なし

View

AP view

定義済みユーザロール

network-admin

パラメータ

venue-group-number: 場所グループを番号で指定します。範囲は 1 から 11 です。

表 22-7 場所グループの番号と説明

番号	説明
1	アセンブリ
2	ビジネス
3	教育
4	工場
5	施設
6	商業施設
7	住宅
8	倉庫
9	公共施設
10	車両
11	屋外

venue-type-number: 番号で場所タイプを指定します。値は場所グループ番号によって異なります。詳細については、表 22-8 を参照してください。

表 22-8 場所タイプ番号と説明

場所グループ番号	場所タイプ番号	場所説明
1	0	未指定
1	1	アリーナ
1	2	スタジアム
1	3	旅客ターミナル
1	4	円形劇場
1	5	遊園地
1	6	礼拝所
1	7	会議場
1	8	図書館
1	9	博物館
1	10	レストラン
1	11	劇場
1	12	バー
1	13	喫茶店
1	14	動物園または水族館
1	15	緊急対応センター
2	0	未指定

場所グループ番号	場所タイプ番号	場所説明
2	1	医師又は歯科医師の診療所
2	2	銀行
2	3	消防署
2	4	警察署
2	6	郵便局
2	7	専門オフィス
2	8	研究開発施設
2	9	弁護士事務所
3	0	未指定
3	1	小学校
3	2	中学校
3	3	大学
4	0	未指定
4	1	工場
5	0	未指定
5	1	病院
5	2	介護老人保健施設
5	3	アルコール・薬物リハビリテーションセンター
5	4	グループホーム
5	5	刑務所または拘置所
6	0	未指定
6	1	小売店
6	2	食料品市場
6	3	自動車サービスステーション
6	4	ショッピングモール
6	5	ガソリンスタンド
7	0	未指定
7	1	個人住宅
7	2	ホテルまたはモーテル
7	3	宿舎
7	4	下宿
8	0	未指定
9	0	未指定
10	0	未指定
10	1	自動車またはトラック

場所グループ番号	場所タイプ番号	場所説明
10	2	飛行機
10	3	バス
10	4	フェリー
10	5	船またはボート
10	6	電車
10	7	モーターバイク
11	0	未指定
11	1	自治体メッシュネットワーク
11	2	市立公園
11	3	休憩施設
11	4	交通管制施設
11	5	バス停
11	6	売店

説明

venue group コマンドは AP の場所グループ情報を設定します。

undo venue group コマンドはデフォルトに戻します。

例

AP ap3 の場所グループ 1 および場所タイプ 2 を指定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1120

[AC-wlan-ap-ap3] venue group 1 type 2

22.1.26 venue name

Syntax

venue name *venue-name* **lang-code** *lang-code* [**url** *url*]

undo venue name *venue-name* **lang-code** *lang-code* [**url** *url*]

デフォルト

設定なし

View

AP view

定義済みユーザロール

network-admin

パラメータ

venue-name: 場所名を指定します。1 から 252 文字の文字列で、大文字と小文字が区別されます。

lang-code: 場所の言語コードを指定します。デバイスは、ISO 639-1 と ISO 639-2 の両方の標準をサポートしています。

url: AP が属する場所の URL を指定します。1 から 63 文字の文字列で、大文字と小文字は区別されません。URL アドレスには疑問符 (?) を含めることができます。

説明

venue name コマンドは AP の場所名を設定します。

undo venue name コマンドは場所名を削除します。

一つの場所に複数の言語コードを設定できます。

AP には、最大 32 個の場所名と言語コードの組み合わせを設定できます。

このコマンドで指定する URL は、標準の HTTP または HTTPS プロトコルを介してアクセスでき、http://または https://で始まる必要があります。

例

AP ap3 の場所名を office に、言語コードを en に設定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1120

[AC-wlan-ap-ap3] venue name office lang-code en

AP ap1 の場所名を v1 に、言語コードを en に、場所 URL を http://www.example.com に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1120

[AC-wlan-ap-ap1] venue name v1 lang-code en url http://www.example.com

22.1.27 wan-metrics

Syntax

wan-metrics { **link-down** | **link-test** | **link-up** } [**asymmetric downlink-speed**

downlink-speed **uplink-speed** *uplink-speed* | **symmetric link-speed**

link-speed]

undo wan-metrics

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

link-down: WAN のリンクステータスを down に設定します。

link-test: WAN のリンクステータスを testing に設定します。

link-up: WAN のリンクステータスを up に設定します。

asymmetric: 非対称リンクを指定します。

downlink-speed *downlink-speed*: ダウンリンクの速度を 1 から 4194304 Kbps の範囲で指定します。

uplink-speed *uplink-speed*: アップリンクの速度を 1 から 4194304 Kbps の範囲で指定します。

symmetric: 対称リンクを指定します。

link-speed *link-speed*: 対称リンクの速度を 1 から 4194304 Kbps の範囲で指定します。

説明

wan-metrics コマンドは WAN リンクステータスパラメータを設定します。

undo wan-metrics コマンドはデフォルトに戻します。

例

WAN のリンクステータスをアップに、対称リンクレートを 67 Kbps に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] wan-metrics link-up symmetric link-speed 67

22.1.28 wlan hotspot-policy

Syntax

wlan hotspot-policy *policy-number*

undo wlan hotspot-policy *policy-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-number: Hotspot 2.0 ポリシーの番号を 1 から 32 の範囲で指定します。

説明

wlan hotspot-policy コマンドは Hotspot 2.0 ポリシーを作成してそのビューを開始するか、既存の Hotspot 2.0 ポリシーのビューを開始します。

undo wlan hotspot-policy コマンドは Hotspot 2.0 ポリシーを削除します。

サービステンプレートにバインドされている Hotspot 2.0 ポリシーは削除できません。

例

Hotspot 2.0 ポリシー1 を作成し、そのビューに入ります。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1]

22.1.29 wlan hotspot osu-icon unload

Syntax

wlan hotspot osu-icon unload

View

System view

定義済みユーザロール

network-admin

説明

wlan hotspot osu-icon unload コマンドはすべての OSU サーバアイコンファイルをアンロードします。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

このコマンドは、OSU サーバアイコンファイルをアンロードするだけで、アイコンファイルは削除されません。

例

すべての OSU サーバアイコンファイルをアンロードします。

<AC> system-view

[AC] wlan hotspot osu-icon unload

関連コマンド

- **icon-file**
- **wlan hotspot osu-icon upload**

22.1.30 wlan hotspot osu-icon upload

Syntax

wlan hotspot osu-icon upload

View

System view

定義済みユーザロール

network-admin

説明

wlan hotspot osu-icon upload コマンドは指定したすべての OSU サーバアイコンファイルをロードします。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

このコマンドを使用して、OSU サーバに指定されたすべてのアイコンファイルを読み込み、アイコンファイルの変更が発生したときに変更を検証します。

例

指定した OSU サーバのアイコンファイルをすべて読み込みます。

<AC> system-view

[AC] wlan hotspot osu-icon upload

関連コマンド

- **icon-file**
- **wlan hotspot osu-icon unload**

22.1.31 wlan osu-provider

Syntax

wlan osu-provider *osu-provider-number*

undo wlan osu-provider *osu-provider-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

osu-provider-number: OSU サーバを 1 から 32 の範囲の番号で指定します。

説明

wlan osu-provider コマンドは OSU サーバを作成してそのビューを開始するか、既存の OSU サーバのビューを開始します。

undo wlan osu-provider コマンドは指定した OSU サーバを削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

Hotspot 2.0 ポリシーにバインドされている OSU サーバを削除することはできません。

例

OSU サーバ 1 を作成し、そのビューを入力します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1]

22.1.32 wlan venue url-unescape-chars

Syntax

wlan venue url-unescape-chars { **composition1** | **composition2** | **custom** *character-string* }

undo wlan venue url-unescape-chars [**custom** *character-string*]

デフォルト

composition1

View

System view

定義済みユーザロール

network-admin

説明

wlan venue url-unescape-chars コマンドは場所 URL のエスケープから特定の特殊文字を除外できます。

undo wlan venue url-unescape-chars コマンドは場所 URL のエスケープから除外された特殊文字を削除できます。

クライアントが特殊文字を構文またはコマンドとして解釈し、意図した意味を変更しないようにするには、これらの文字を安全な形式 (エスケープ文字) に変換する必要があります。

実際には、サーバによっては、URL 内の特定の特殊文字のエスケープ文字が認識されず、エラーが発生することがあります。このような場合は、このタスクを実行して、特定の特殊文字をエスケープから除外できます。

場所 URL では、大文字と小文字および数字以外の文字はエスケープする必要がなく、このコマンドを使用して残りの特殊文字を構成できます。

デフォルトでは、デバイスは composition1 の特殊文字をエスケープしません。

サーバによっては、URL 内の特定の特殊文字のエスケープ文字が認識されず、例外が発生する場合があります。これに対処するには、これらの特定の文字がエスケープされないように機能を構成します。

例

場所 URL でのエスケープから composition2 の特殊文字を除外します。

<AC> system-view

[AC] wlan venue url-unescape-chars composition2

特殊文字を除く;() が場所 URL でエスケープされないようにします。

<AC> system-view

[AC] wlan venue url-unescape-chars custom ;()

QX-W2230AC アクセスコントローラ

コマンドマニュアル

3. インタフェース

本マニュアルは以下に示す章で構成されています。

01-Ethernet インタフェース

02-ループバックインタフェースと Null インタフェース

03-Interface range

目次

このセクションのページは **3-x-x** です。

1 章 Ethernet インタフェース 1-1
1.1 共通 Ethernet インタフェース設定コマンド 1-1
1.1.1 description 1-1
1.1.2 display counters 1-1
1.1.3 display counters rate 1-3
1.1.4 display interface 1-5
1.1.5 duplex 1-19
1.1.6 flow-interval 1-20
1.1.7 interface 1-21
1.1.8 jumboframe enable 1-21
1.1.9 loopback 1-22
1.1.10 reset counters interface 1-23
1.1.11 shutdown 1-24
1.1.12 speed 1-25

1章 Ethernet インタフェース

1.1 共通Ethernetインタフェース設定コマンド

1.1.1 description

Syntax

description *text*

undo description

デフォルト

インタフェース名＋Interface です。（たとえば GigabitEthernet1/0/1 Interface です）

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

text: インタフェースの説明を指定します。設定範囲は 1～255 文字です。大文字、小文字を区別します。

説明

description コマンドはインタフェースの説明を変更します。

undo description コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 の説明を lan-interface に変更します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] description lan-interface

1.1.2 display counters

Syntax

display counters { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

inbound: 受信トラフィックの統計情報を表示します。

outbound: 送信トラフィックの統計情報を表示します。

interface-type: インタフェースのタイプを指定します。

interface-number: インタフェースの番号を指定します。

説明

display counters コマンドはインタフェースのトラフィックの統計情報を表示します。

本コマンドは **flow-interval** コマンドで指定されたポートの統計情報を収集する間隔内のトラフィックの統計情報を表示します。

Ethernet インタフェースのトラフィックの統計情報を削除する場合、**reset counters interface** コマンドを使用します。

インタフェースタイプを指定しない場合、すべてのインタフェースのトラフィックの統計情報を表示します。

インタフェースタイプを指定し、番号を指定しない場合、指定したインタフェースタイプのすべてのインタフェースのトラフィックの統計情報を表示します。

インタフェースタイプと番号を指定した場合、指定したインタフェースのすべてのトラフィックの統計情報を表示します。

例

すべての GigabitEthernet インタフェースの入力方向トラフィックの統計情報を表示します。

<AC> display counters inbound interface gigabitethernet

Interface	Total (pkts)	Broadcast (pkts)	Multicast (pkts)	Err (pkts)
GE1/0/1	100	100	0	0
GE1/0/2	0	0	0	0
GE1/0/3	0	0	0	0
GE1/0/4	0	0	0	0

```
Overflow: More than 14 digits (7 digits for column "Err").
     --: Not supported.
```

表 1-1 コマンド出力

フィールド	説明
Interface	インタフェース名の省略名
Total (pkts)	インタフェースを通して送受信したパケットの総数
Broadcast (pkts)	インタフェースを通して送受信したブロードキャストパケットの総数
Multicast (pkts)	インタフェースを通して送受信したマルチキャストパケットの総数
Err (pkts)	インタフェースを通して送受信したエラーパケットの総数
Overflow: More than 14 digits (7 digits for column "Err")	以下のときに**Overflow**と表示 • エラーフィールド値のデータ長が10進数で7桁を超えました。 • 非エラーフィールド値のデータ長が10進数で14桁を超えました。
--: Not supported	統計情報を未サポート

関連コマンド

- **flow-interval**
- **reset counters interface**

1.1.3 display counters rate

Syntax

display counters rate { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

inbound: 受信トラフィックレートの統計情報を表示します。

outbound: 送信トラフィックレートの統計情報を表示します。

interface-type: インタフェースのタイプを指定します。

interface-number: インタフェースの番号を指定します。

説明

display counters rate コマンドは最後のサンプリング間隔からの up 状態のインタフェースのトラフィックレートの統計情報を表示します。

インタフェースタイプを指定しない場合、すべてのインタフェースのトラフィックレートの統計情報を表示します。

インタフェースタイプを指定し、インタフェースの番号を指定しない場合、指定されたタイプのすべての up 状態のインタフェースのトラフィックレートの統計情報を表示します。

インタフェースタイプ、インタフェースの番号を指定した場合、指定したインタフェースのトラフィックレートの統計情報を表示します。

down 状態のインタフェースが指定されている場合、システムはコマンドをサポートしていないと表示されます。

最後のサンプリングの間隔を設定する場合、**flow-interval** コマンドを使用することができます。

例

すべての GigabitEthernet インタフェースの受信トラフィックレートの統計情報を表示します。

<AC> display counters rate inbound interface gigabitethernet

```
Usage: Bandwidth utilization in percentage
Interface          Usage (%)   Total (pps)   Broadcast (pps)   Multicast (pps)
GE1/0/1                  3         200            100             100
GE1/0/2                  5         300            200             100
GE1/0/3                  5         300            200             100

 Overflow: More than 14 digits.
      --: Not supported.
```

表 1-2 コマンド出力

フィールド	説明
Interface	インタフェース名の省略名です。
Usage (%)	最後のサンプリング間隔中にインタフェースで送受信したパケットの平均レートです。単位は%です。
Total (pkts/sec)	最後のサンプリング間隔中に送受信したユニキャストパケットの平均レートです。単位はppsです。
Broadcast (pkts/sec)	最後のサンプリング間隔中に送受信したブロードキャストパケットの平均レートです。単位はppsです。

フィールド	説明
Multicast (pkts/sec)	最後のサンプリング間隔中に送受信したマルチキャストパケットの平均レートです。単位はppsです。
Overflow: more than 14 decimal digits	データ長が10進数で14桁を超えたときに、**Overflow**と表示します。
--: not supported	統計情報をサポートしていません。

関連コマンド

- **flow-interval**
- **reset counters interface**

1.1.4 display interface

Syntax

display interface [*interface-type* [*interface-number*]] [**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type: インタフェースタイプを指定します。

interface-number: インタフェース番号を指定します。

brief: 概要情報を表示します。指定しない場合、コマンドは詳細なインタフェース情報を表示します。

description: インタフェースの説明をすべて表示します。指定しない場合、インタフェースの説明の最初の 27 文字のみ表示します。

down: down 状態のインタフェースの情報と原因を表示します。指定しない場合、すべての状態のインタフェース情報を表示します。

説明

display interface コマンドは Ethernet インタフェースの情報を表示します。

インタフェースタイプを指定しない場合、すべてのインタフェースの情報を表示します。

インタフェースタイプを指定し、番号を指定しない場合、指定したタイプのすべてのインタフェースの情報を表示します。

インタフェースタイプと番号を指定した場合、指定したインタフェースの情報を表示します。

例

GigabitEthernet 1/0/1 レイヤ 3 インタフェースの情報を表示します。

<AC> display interface gigabitethernet1/0/1

```
GigabitEthernet1/0/1
Current state: Administratively DOWN
Line protocol state: DOWN
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 1000000kbps
Maximum transmission unit: 1500
Internet protocol processing: Disabled
IP packet frame type: Ethernet II, hardware address: 3822-d666-bd0c
IPv6 packet frame type: Ethernet II, hardware address: 3822-d666-bd0c
Loopback is not set
Media type is twisted pair, promiscuous mode set
Port priority: 2
Unknown-speed mode, unknown-duplex mode
Last link flapping: 6 hours 39 minutes 28 seconds
Last clearing of counters: Never
 Peak input rate: 0 bytes/sec, at 00-00-00 00:00:00
 Peak output rate: 0 bytes/sec, at 00-00-00 00:00:00
 Last 300 second input:  0 packets/sec 0 bytes/sec  0%
 Last 300 second output: 0 packets/sec 0 bytes/sec  0%
 Input  (total): 0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, - pauses
 Input  (normal): 0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input: 0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, 0 overruns, - aborts
         - ignored, - parity errors
 Output  (total): 0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, - pauses
 Output  (normal): 0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         - lost carrier, - no carrier
 Peak input rate: 0 bytes/sec, at 2013-07-07 16:07:11
```

```
 Peak output rate: 0 bytes/sec, at 2013-07-07 16:07:11
```

GigabitEthernet 1/0/1 レイヤ 2 インタフェースの情報を表示します。

<AC> display interface gigabitethernet 1/0/1

```
GigabitEthernet1/0/1
Current state: DOWN
Line protocol state: DOWN
IP packet frame type: Ethernet II, hardware address: 000c-2963-b767
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 100000kbps
Loopback is not set
Media type is twisted pair, promiscuous mode set
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length: 4000
Allow jumbo frame to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
PVID: 1
MDI type: Automdix
Port link-type: Access
 Tagged VLANs:   None
 UnTagged VLANs: 1
Port priority: 2
Last clearing of counters:  14:34:09 Tue 11/01/2011
 Peak input rate: 0 bytes/sec, at 2013-07-17 22:06:19
 Peak output rate: 0 bytes/sec, at 2013-07-17 22:06:19
 Last 300 second input:  0 packets/sec 0 bytes/sec -%
 Last 300 second output:  0 packets/sec 0 bytes/sec -%
 Input (total):  0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input (normal):  0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, 0 overruns, 0 aborts
         0 ignored, 0 parity errors
 Output (total): 0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output (normal): 0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, 0 underruns, 0 buffer failures
```

```
0 aborts, 0 deferred, 0 collisions, 0 late collisions
0 lost carrier, 0 no carrier
```

表 1-3 コマンド出力

フィールド	説明
Current state	Ethernetインタフェースの状態 • **Administratively DOWN**—**shutdown**コマンドでインタフェースがシャットダウンしています。インタフェースは運用上においてダウンしています。 • **DOWN**—**shutdown**コマンドでシャットダウンしていませんが、物理的にダウンしています（イーサネットケーブルが物理的に接続されていない、あるいはリンクに失敗している可能性があります）。 • **DOWN (Link-Aggregation interface down)**— **shutdown**コマンドでアグリゲートインタフェースがシャットダウンしています。 • **DOWN (Tunnel-Bundle administratively down)**— **shutdown**コマンドでインタフェースが所属するトンネルバンドルインタフェースがダウンしています。装置は現在のソフトウェアバージョンでは、本フィールドをサポートしません。 • **ETH-rddc Shutdown**—インタフェースはRethモジュールによりダウンしています。装置は現在のソフトウェアバージョンでは、本フィールドをサポートしません。 • **mac-address moving down**—MACアドレスの移動の抑制機能によりインタフェースがシャットダウンしています。 • **Storm-Constrain**—ストーム抑止機能が不明なユニキャストトラフィック、マルチキャストトラフィック、ブロードキャストトラフィックの上限に到達したことを検出したため、インタフェースがシャットダウンしています。 • **STP DOWN**—BPDUガード機能によりインタフェースがシャットダウンしています。 • **UP**—インタフェースが運用上も物理的にも起動している状態です。
Line protocol state	インタフェースのリンクレイヤの状態 リンクレイヤのパラメータのネゴシエーションによって決まります。 • **UP**—インタフェースがリンクレイヤでupしています。 • **UP (spoofing)**—インタフェースがリンクレイヤでupしていますが、オンデマンドのリンクあるいは準備ができて

フィールド	説明

	いない状態です。この属性はNullインタフェースとループバックインタフェースの一般的な状態です。
	• **DOWN**—インタフェースのリンクレイヤでdownしています。
	• **DOWN** (*protocols*)—1つ以上のプロトコルにより、インタフェースのリンクレイヤがdownしています。プロトコルはDLDP、OAM、LAGG、BFD、MACSECです。
	  • *protocol*にDLDPを含む場合、リンクが片方向であるとDLDPが検出したため、インタフェースがリンクレイヤでdownしています。装置は現在のソフトウェアバージョンでは本フィールドをサポートしていません。
	  • *protocol*にOAMを含む場合、OAMがリモートリンクの問題を検出したため、インタフェースがリンクレイヤでdownしています。装置は現在のソフトウェアバージョンでは本フィールドをサポートしていません。
	  • *protocol*にLAGGを含む場合、アグリゲートインタフェースがSelectedポートでないため、インタフェースがリンクレイヤでdownしています。装置は現在のソフトウェアバージョンでは本フィールドをサポートしていません。
	  • *protocol*にBFDを含む場合、リンク障害を検出したためインタフェースがリンクレイヤでdownしています。装置は現在のソフトウェアバージョンでは本フィールドをサポートしていません。
	  • *protocol*にMACSECを含む場合、MACSECが暗号化パラメータのネゴシエーションに失敗したため、インタフェースがリンクレイヤでdownしています。装置は現在のソフトウェアバージョンでは本フィールドをサポートしていません。

Bandwidth	インタフェースの期待される帯域幅
Maximum transmission unit	インタフェースのMTU
Internet protocol processing: Disabled	インタフェースがIPパケットを処理できません。
Internet address is 192.168.1.200/24 Primary	プライマリインタフェースのIPアドレス
IP packet frame type	IPv4パケットのフレームタイプ

フィールド	説明
hardware address	インタフェースのMACアドレス
IPv6 packet frame type	IPv6パケットのフレームタイプ
Output queue	出力キューに関する情報
Urgent queuing	Urgentキュー
Protocol queuing	Protocolキュー
FIFO queuing	FIFOキュー
Size	キュー内のパケット数
Length	キュー長
Discards	廃棄パケット数
Loopback is set internal	インタフェースで内部ループバックテストが動作しています。
Loopback is set external	インタフェースで外部ループバックテストが動作しています。
Loopback is not set	インタフェースでループバックテストが動作していません。
10Mbps-speed mode	インタフェースが10Mbpsで動作しています。
100Mbps-speed mode	インタフェースが100Mbpsで動作しています。
1000Mbps-speed mode	インタフェースが1000Mbpsで動作しています。
Unknown-speed mode	通信速度のネゴシエーションに失敗あるいはインタフェースが物理的に切断しているため、インタフェースの速度が不明です。
half-duplex mode	インタフェースがhalf duplexモードで動作しています。
full-duplex mode	インタフェースがfull duplexモードで動作しています。
unknown-duplex mode	通信モードのネゴシエーションに失敗あるいはインタフェースが物理的に切断しているため、インタフェースの通信モードが不明です。
Link speed type is autonegotiation	**speed auto**コマンドでインタフェースに設定されています。
Link speed type is force link	**speed**コマンドで通信速度（たとえば10Mbpsや100Mbps）がインタフェースに設定されています。
link duplex type is autonegotiation	**duplex auto**コマンドでインタフェースに設定されています。

フィールド	説明
link duplex type is force link	**duplex**コマンドで通信モード（たとえばhalfあるいはfull）がインタフェースに設定されています。
Flow-control is not enabled	インタフェースでフローコントロールが無効です。
Maximum frame length	インタフェースの最大フレーム長
Allow jumbo frame to pass	インタフェースがジャンボフレームをサポートしています。
Broadcast max-	ブロードキャストストーム抑制のしきい値 単位はratio、pps、kbpsです。しきい値のユニットは設定に依存します。
Multicast max-	マルチキャストストーム抑制のしきい値 単位はratio、pps、kbpsです。しきい値のユニットは設定に依存します。
Unicast max-	ユニキャストストーム抑制のしきい値 単位はratio、pps、kbpsです。しきい値のユニットは設定に依存します。
PVID	インタフェースのポートVLANのID（PVID
MDI type	インタフェースのMDIXタイプ ● automdix ● mdi ● mdix
Port link-type	インタフェースのリンクタイプ ● access ● trunk ● hybrid
Tagged VLANs	VLANタグを削除しないでパケット送信するVLAN
Untagged VLANs	VLANタグを削除したのち、パケット送信するVLAN
Port priority	インタフェースの優先度
Last link flapping	リンクがフラッピングしてからの経過時間 **Never**は装置が起動してから一度もリンクのフラッピングが発生していないことを示します。
Last clearing of counters	インタフェースで**reset counters interface**コマンドを最後に使用した時間 **Never**は装置が起動してから**reset counters interface**コマンドを一度も使用していないことを示します。
Last 300 second input: 0 packets/sec 0 bytes/sec 0%	過去300秒以内の平均送受信トラフィック（単位はpps、bps）および最大インタフェース速度に対する実際の速度の比率

フィールド	説明
Last 300 second output:　0 packets/sec 0 bytes/sec 0%	ハイフン（-）はその統計アイテムをサポートしていないことを示します。
Input(total):　0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	フィールドの1行目はインタフェースの受信トラフィックの統計情報（パケット、バイト数） すべての正常な受信パケット、異常なパケット、正常なpauseフレームがカウントされます。 2行目の4つのフィールドは以下を示します。 ● ユニキャストパケットの受信数 ● ブロードキャストの受信数 ● マルチキャストの受信数 ● pauseフレームの受信数 ハイフン（-）はその統計アイテムをサポートしていないことを示します。
Input(normal):　0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	フィールドの1行目はインタフェースの正常な受信トラフィックとの統計情報（パケット、バイト数） すべての正常な受信パケット、正常なpauseフレームがカウントされます。 2行目の4つのフィールドは以下を示します。 ● 正常なユニキャストパケットの受信数 ● 正常なブロードキャストの受信数 ● 正常なマルチキャストの受信数 ● 正常なpauseフレームの受信数 ハイフン（-）はその統計アイテムをサポートしていないことを示します。
input errors	受信エラーパケットの統計情報
runts	以下の状況にある受信フレーム数 ● 64バイト長未満のフレーム ● 不正なフォーマットのフレーム ● 有効なCRCが含まれるフレーム
giants	インタフェースでサポートされるフレーム長よりも長い受信フレーム数 ジャンボフレームをサポートしていないインタフェースでは、最大フレーム長は以下です。 ● 1518バイト（VLANタグなし）。 ● 1522バイト（VLANタグつき）。 ジャンボフレームをサポートしているインタフェースでは、giantsはインタフェースを通過することを許可されたフレームの最大長より長いフレームを示します。

フィールド	説明
throttles	整数倍バイト長でない入力フレーム数
CRC	正常なフレーム長ですが、CRCエラーが含まれている受信フレームの総数
frame	CRCエラーが含まれ、整数バイトでない受信フレームの総数
overruns	ポートの受信レートがキューの容量を超過したため、廃棄されたパケット数

aborts	不正な受信パケットの総数
	• **Fragment frames**—64バイトよりも短いフレームのCRCエラーフレームです。フレーム長は整数あるいは非整数の値です。
	• **Jabber frames**—インタフェースでサポートされている最大フレーム長よりも長いフレームのCRCエラーフレームです。フレーム長は整数あるいは非整数の値です。
	  • ジャンボフレームを許可しない場合、最大フレーム長は1518バイト（VLANタグなし）あるいは1540バイト（VLANタグつき）よりも長いCRCエラーフレームを示します。
	  • ジャンボフレームを許可する場合、jabberフレームはインタフェースを通過することを許可されたフレームの最大長より長いフレームを示します。
	• **Symbol error frames**—少なくとも1つ以上の定義されていないシンボルを含むフレーム
	• **Unknown operation code frames**— pauseフレームでないMAC制御フレーム
	• **Length error frames**—802.3のlengthフィールドが実際のフレーム長に合致していないフレーム（46～1500バイト）

ignored	ポートの受信バッファの能力不足により、インタフェースに廃棄された受信フレームの数
parity errors	パリティエラーのフレームの総数
Output(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	フィールドの1行目はインタフェースの送信トラフィックの統計情報（パケット、バイト数） すべての正常な送信パケット、異常なパケット、正常なpauseフレームがカウントされます。 2行目の4つのフィールドは以下を示します。 • ユニキャストパケットの送信数 • ブロードキャストの送信数 • マルチキャストの送信数

フィールド	説明
	● pauseフレームの送信数 ハイフン（-）はその統計アイテムをサポートしていないことを示します。
Output(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	フィールドの1行目はインタフェースの正常な送信トラフィックとの統計情報（パケット、バイト数） すべての正常な送信パケット、正常なpauseフレームがカウントされます。 2行目の4つのフィールドは以下を示します。 ● 正常なユニキャストパケットの送信数 ● 正常なブロードキャストの送信数 ● 正常なマルチキャストの送信数 ● 正常なpauseフレームの送信数 ハイフン（-）はその統計アイテムをサポートしていないことを示します。
output errors	送信エラーパケットの統計情報
underruns	ポートの送信レートがキューの容量を超過したため廃棄されたパケット数 これはハードウェア異常により、まれに発生する可能性があります。
buffer failures	ポートの送信バッファの能力不足によりインタフェースに廃棄されたパケットの数
aborts	Ethernetコリジョンなどにより転送に失敗したパケット数
deferred	検出したコリジョンによりフレームを遅延させた数
collisions	フレームの送信中にEthernetコリジョンが検出されたため転送を停止したフレーム数
late collisions	最初の512ビットをネットワークに送信した後にコリジョンが検出されフレームの送信が遅延した回数
lost carrier	伝送中にキャリアが失われた回数 このカウンタは、キャリアが失われたときに増加し、シリアルWANインタフェースに適用されます。装置は現在のソフトウェアバージョンでは本フィールドをサポートしていません。
no carrier	フレームを送信しようとしたときポートがキャリアの検出に失敗した回数 このカウンタは、ポートがキャリアの検出に失敗したときに増加し、シリアルWANインタフェースに適用されます。装置は現在のソフトウェアバージョンでは本フィールドをサポートしていません。

フィールド	説明
Peak input rate	受信トラフィックレートのピークレートおよび受信トラフィックのピークが発生したときの時間 ピークレートの単位はbpsです。
Peak output rate	送信トラフィックレートのピークレートおよび送信トラフィックのピークが発生したときの時間 ピークレートの単位はbpsです。

すべてのインタフェースの概要情報を表示します。

<AC> display interface brief

```
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP     Description
CMTunnel1          DOWN DOWN     --
InLoop0            UP   UP(s)    --
Loop0              UP   UP(s)    --
MGE0/0/0           UP   UP       192.168.100.66
NULL0              UP   UP(s)    --
Tun0               DOWN DOWN     --
Tun1               DOWN DOWN     --
Tun2               DOWN DOWN     --
Tun99              DOWN DOWN     --
Tun101             DOWN DOWN     --
Vlan1              DOWN DOWN     --
Vlan2              DOWN DOWN     --
Vlan10             DOWN DOWN     10.1.1.1
Vlan20             DOWN DOWN     --
Vlan100            DOWN DOWN     --

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface          Link Speed   Duplex Type PVID Description
BAGG1              DOWN auto    A      A    1
BAGG2              DOWN auto    A      A    20
BAGG3              DOWN auto    A      T    1
GE1/0/1            DOWN auto    A      A    1
GE1/0/2            DOWN auto    A      T    1
GE1/0/3            DOWN auto    A      A    1
```

```
GE1/0/4            ADM  auto    A     A    1
GE1/0/5            DOWN auto    A     A    1
GE1/0/6            DOWN auto    A     A    1
GE1/0/7            DOWN auto    A     A    1
GE1/0/8            DOWN auto    A     A    1
```

インタフェースの完全な説明を含む GigabitEthernet 1/0/3 の概要情報を表示します。

<AC> display interface gigabitethernet 1/0/3 brief description

```
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface          Link Speed   Duplex Type PVID Description
GE1/0/3            UP   100M(a) F(a)   A    1    link to router C
```

DOWN 状態のインタフェースの情報と原因を表示します。

<AC> display interface brief down

```
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface          Link Cause
GE1/0/1            DOWN Not connected

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Interface          Link Cause
GE1/0/2            DOWN Not connected
GE1/0/4            DOWN Not connected
GE1/0/5            DOWN Not connected
GE1/0/7            DOWN Not connected
```

表 1-4 コマンド出力

フィールド	説明
Brief information on interfaces in route mode:	レイヤ3インタフェースの概要情報
Link: ADM - administratively down; Stby - standby	リンク状態 • **ADM**—リンクが運用上、**shutdown**コマンドでシャットダウンしています。物理状態を回復する場合、**undo shutdown**コマンドを実行します。 • **Stby**—インタフェースがバックアップインタフェースとして動作します。プライマリインタフェースを確認するには、**display interface-backup state**コマンドを実行します。

フィールド	説明
Protocol: (s) – spoofing	以下に示す状態が存在する場合、本フィールドは**UP(s)**と表示され、**s**はスプーフィングフラグを表します。 ● インタフェースのデータリンクレイヤプロトコルがUPである ● インタフェースのリンクがオンデマンドリンクであるか、存在しない 本属性は、Null 0インタフェースおよびループバックインタフェースで表示されます。
Interface	インタフェース名
Link	インタフェースの物理リンク状態 ● **UP**—リンクがupです。 ● **DOWN**—リンクが物理的にdownしています。 ● **ADM**—リンクが運用上、**shutdown**コマンドでシャットダウンしています。物理状態を回復する場合、**undo shutdown**コマンドを実行します。 ● **Stby**—インタフェースがバックアップインタフェースとして動作します。
Protocol	インタフェースのリンクレイヤの状態 ● **UP**－インタフェースのリンクがupです。 ● **DOWN**－インタフェースのリンクがdownです。 ● **UP(s)**—インタフェースのリンクがオンデマンドリンクあるいは準備ができていない状態です。ここで（**s**）はスプーフィングフラグを示します。Nullインタフェース、ループバックインタフェースで表示されます。
Primary IP	インタフェースのプライマリIPアドレス ハイフン（**--**）はIPアドレスが設定されていないことを示します。
Description	**descrption**コマンドで設定されたインタフェースの部分的または完全な説明 ● **display interface brief**コマンドで**description**キーワードを指定しなかった場合、本フィールドはインタフェース説明の最初の27文字のみ表示します。 ● **display interface brief**コマンドで**description**キーワードを指定した場合、本フィールドはインタフェース説明を完全に表示します。
Brief information of interfaces in bridge mode:	レイヤ2インタフェースの概要情報
Speed: (a) - auto	インタフェースの通信速度 インタフェースが自動でネゴシエーションされる場合、（**a**）

フィールド	説明
	で示されたオートネゴシエーションのフラグが含まれます。インタフェースにオートネゴシエーションが設定されているがオートネゴシエーションが開始していない場合、**auto**と表示されます。
Duplex: (a)/A - auto; H - half; F – full	インタフェースの通信モードが自動的にネゴシエーションされた場合、インタフェースの通信モード属性が（**a**）で表示されます。**H**はhalf duplexモードを、**F**はfull duplexモードを示します。 インタフェースが通信モードをオートネゴシエーションするよう設定されているが、オートネゴシエーションが開始されていない場合、通信モード属性は**A**と表示されます。
Type: A - access; T - trunk; H – hybrid	インタフェースのリンクタイプオプション
Speed	インタフェースの通信速度
Duplex	インタフェースの通信モード ● **A**—オートネゴシエーション ● **F**—Full Duplx ● **F(a)**—オートネゴシエーションでFull Duplx ● **H**—Half Duplex ● **H(a)**— オートネゴシエーションでhalf Duplx
Type	インタフェースのリンクタイプ ● **A**—Access ● **H**—Hybrid ● **T**—Trunk
PVID	ポートVLAN ID
Cause	インタフェースの物理リンク状態がDOWNとなった原因 ● **Administratively—shutdown**コマンドでインタフェースがシャットダウンしています。インタフェースは運用上においてdownしています。物理状態を回復する場合、**undo shutdown**コマンドを実行します。 ● **DOWN (Link-Aggregation interface down)**—アグリゲートインタフェースがシャットダウンしているとき、アグリゲートインタフェースのすべてのメンバポートの物理状態がdownです。 ● **DOWN (Loopback detection down)**—ループバック検出モジュールがループバックを検出したため、ポートがシャットダウンしています。 ● **DOWN (Monitor-Link uplink down)**—モニタリンクモジュー

フィールド	説明
	ルがアップリンクのダウンを検出したため、ポートがシャットダウンしています。 • **Not connected**—物理接続がありません（ネットワークが切断された、あるいは故障している可能性があります）。 • **Storm-Constrain**—不明なユニキャストトラフィック、マルチキャストトラフィック、ブロードキャストトラフィックが上限を超過したため、ポートがシャットダウンしています。装置は現在のソフトウェアバージョンでは、本フィールドをサポートしません。 • **STP DOWN**—STP BPDUガード機能によってインタフェースがシャットダウンしています。 • **Port Security Disabled—**ポートが不正なパケットを受信したため、侵入検出メカニズムによってインタフェースはダウしています。 • **Standby**—インタフェースがstandby状態です。

関連コマンド

reset counters interface

1.1.5 duplex

Syntax

duplex { **auto** | **full** | **half** }

undo duplex

デフォルト

auto

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

auto: ピアとの通信モードをオートネゴシエーションに設定します。

full: インタフェースが同時にパケットの送受信を行えるように通信モードを full（全 2 重モード）に設定します。

half: インタフェースが受信時にパケットの送信あるいは受信のみを行えるように通信モードを half（半 2 重モード）に設定します。1000Mbps で動作する RJ-45 ポートは、未サポートです。

説明

duplex コマンドはインタフェースの通信モードを設定します。

undo duplex コマンドはインタフェースの通信モードをデフォルトに戻します。

例

GigabitEthernet 1/0/1 の通信モードを full に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] duplex full

1.1.6 flow-interval

Syntax

flow-interval *interval*

undo flow-interval

デフォルト

300 秒

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

interval: ポートの統計情報を収集する間隔を設定します。設定範囲は 5～300 で、5 の倍数にする必要があります。

説明

flow-interval コマンドはポートの統計情報を収集する間隔を設定します。

undo flow-interval コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 の統計情報収集間隔を 100 秒に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] flow-interval 100

1.1.7 interface

Syntax

interface *interface-type interface-number*

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-type: インタフェースタイプを指定します。

interface-number: インタフェース番号を指定します。

説明

interface コマンドは interface view に移行します。

例

GigabitEthernet 1/0/1 の interface view に移行します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1]

1.1.8 jumboframe enable

Syntax

jumboframe enable [*value*]

undo jumboframe enable

デフォルト

1600 バイトまでのジャンボフレームを許可します。

View

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

value: Ethernet フレームの通過を許可する最大フレーム長を設定します。値の範囲は 1518～4000 です。

説明

jumboframe enable コマンドは指定したフレーム長以内のジャンボフレームの通過を許可します。

undo jumboframe enable コマンドはジャンボフレームの通過を拒否します。

value が複数回設定された場合、最後に指定された設定が適用されます。

例

GigabitEthernet 1/0/1 でジャンボフレームの通過を許可します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] jumboframe enable

1.1.9 loopback

注意:

Ethernet インタフェースでループバックテストを有効にした場合、インタフェースはトラフィックデータを転送しません。

Syntax

loopback { **external** | **internal** }

undo loopback

デフォルト

無効

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

external: Ethernet インタフェースの外部ループバックテストを有効にします。

internal: Ethernet インタフェースの内部ループバックテストを有効にします。

説明

loopback コマンドは Ethernet インタフェースのループバックテストを有効にします。

undo loopback コマンドは Ethernet インタフェースのループバックテストを無効にします。

shutdown コマンドと **loopback** コマンドを同時に設定することはできません。

Ethernet インタフェースでループバックテストを有効にすると、Ethernet インタフェー通信モードを full に切り替わります。Ethernet インタフェースでループバックテストを無効にすると、Ethernet インタフェースの通信モードテスト終了後はもとの設定で動作します。

例

GigabitEthernet 1/0/1 の内部ループバックテストを有効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] loopback internal

1.1.10 reset counters interface

Syntax

reset counters interface [*interface-type* [*interface-number*]]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface-type: インタフェースタイプを指定します。

interface-number: インタフェース番号を指定します。

説明

reset counters interface コマンドはインタフェースの統計情報をクリアします。

一定期間のトラフィックの統計情報を収集したい場合、本コマンドを使用して以前に収集された統計情報の履歴をクリアします。

インタフェースタイプを指定しなかった場合、VA インタフェースを除くすべてのインタフェースの統計情報をクリアします。

インタフェースタイプのみを指定した場合、インタフェースタイプのすべてのインタフェースの統計情報をクリアします。

インタフェースタイプとインタフェースの番号を両方指定した場合、指定したインタフェースの統計情報を削除します。

例

GigabitEthernet 1/0/1 の統計情報をクリアします。

<AC> reset counters interface gigabitethernet 1/0/1

関連コマンド

- **display counters interface**
- **display counters rate interface**
- **display interface**

1.1.11 shutdown

Syntax

shutdown

undo shutdown

デフォルト

インタフェースはアップ状態です。

View

Ethernet interface view

定義済みユーザロール

network-admin

説明

shutdown コマンドはインタフェース、サブインタフェースをシャットダウンします。

undo shutdown コマンドはインタフェース、サブインタフェースをアップします。

インタフェース設定には、有効にするためにインタフェースの再起動を要求するものがあります。

shutdown コマンドと **loopback** コマンドを同時に設定することはできません。

例

GigabitEthernet 1/0/1 をシャットダウンし、それからアップします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] shutdown

[AC-GigabitEthernet1/0/1] undo shutdown

GigabitEthernet 1/0/1.1 をシャットダウンし、それからアップします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1.1

[AC-GigabitEthernet1/0/1.1] shutdown

[AC-GigabitEthernet1/0/1.1] undo shutdown

1.1.12 speed

Syntax

speed { **100** | **1000 | auto** }

undo speed

デフォルト

auto

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

100: インタフェースの通信速度を 100Mbps に設定します。

1000: インタフェースの通信速度を 1000Mbps に設定します。

auto: ピアとの通信速度をオートネゴシエーションに設定します。

説明

speed コマンドは Ethernet インタフェースの通信速度を設定します。

undo speed コマンドはデフォルトに戻します。

RJ-45 ポートでは、ピアのインタフェースの通信速度に一致するように **speed** コマンドを使用します。

1000BASE-T SFP を含む SFP トランシーバモジュールで動作するポートでは、**speed** コマンドはトランシーバモジュールの速度に一致するように設定します。

例

GigabitEthernet 1/0/1 の通信速度を auto に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] speed auto

目次

このセクションのページは **3-x-x** です。

2 章 ループバックインタフェースと Null インタフェース 2-1
2.1 ループバックインタフェースと Null インタフェース設定コマンド 2-1
2.1.1 description 2-1
2.1.2 display interface loopback 2-2
2.1.3 display interface null 2-6
2.1.4 interface loopback 2-8
2.1.5 interface null 2-9
2.1.6 reset counters interface loopback 2-9
2.1.7 reset counters interface null 2-10
2.1.8 shutdown 2-11

2章 ループバックインタフェースと Null インタフェース

2.1 ループバックインタフェースとNullインタフェース設定コマンド

2.1.1 description

Syntax

description *text*

undo description

デフォルト

インタフェース名＋Interface です。（たとえば、LoopBack0 Interface です）

View

Loopback interface view

Null interface view

定義済みユーザロール

network-admin

パラメータ

text: インタフェースの説明を記載します。設定範囲は 1～255 文字です。大文字、小文字を区別します。

説明

description コマンドはインタフェースの説明を設定します。

undo description コマンドはデフォルトに戻します。

インタフェースの説明を設定することで、インタフェースの識別、管理しやすさを向上させることができます。

設定された説明を表示する場合、**display interface** コマンドを使用します。

例

ループバック 0 の説明を RouterID に設定します。

<AC> system-view

[AC] interface loopback 0

[AC-LoopBack1] description for RouterID

2.1.2 display interface loopback

Syntax

display interface loopback [*interface-number*] [**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-number: ループバックインタフェースの番号を指定します。番号は存在するループバックのインタフェースの番号です。番号を指定しない場合、装置のすべての既存のループバックインタフェースの情報を表示します。

brief: インタフェースの概要を表示します。指定しない場合、詳細なインタフェースの情報を表示します。

description: 完全なインタフェースの説明を表示します。指定しない場合、説明の最初の 27 文字のみを表示します。

down: down 状態のインタフェースの情報と原因を表示します。指定しない場合、すべての状態のインタフェースの情報を表示します。

説明

display interface loopback コマンドは指定した、あるいはすべての既存のループバックインタフェースの情報を表示します。

ループバックインタフェースが作成されたのち、適用されます。

loopback キーワードを指定しなかった場合、コマンドは装置のすべてのインタフェースの情報を表示します。

loopback キーワードを指定したが *interface-argument* 引数を指定しなかった場合、コマンドは存在するすべてのループバックインタフェースの情報を表示します。

例

ループバック 0 のインタフェースの詳細情報を表示します。

<AC> display interface loopback 0

```
LoopBack0
Current state: UP
Line protocol state: UP(spoofing)
```

```
Description: LoopBack0 Interface
Bandwidth: 1000 kbps
Maximum transmission unit: 1536
Internet protocol processing: Disabled
Physical: Loopback
Last clearing of counters:  Never
Last 300 seconds input rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

loopback 0 インタフェースの詳細情報を表示します（ループバックインタフェースがトラフィック統計情報の収集をサポートしていない場合）。

<AC> display interface loopback 0

```
LoopBack0
Current state: UP
Line protocol state: UP(spoofing)
Description: LoopBack0 Interface
Maximum transmit unit: 1536
Internet protocol processing : Disabled
Physical: Loopback
Last clearing of counters:  Never
```

表 2-1 コマンド出力

フィールド	説明
Current state	ループバックインタフェースの物理レイヤの状態です。 ● **UP**–ループバックインタフェースがパケットの送受信を行うことができます。 ● **Administratively DOWN**–インタフェースが**shutdown**コマンドにより手動でシャットダウンしています。
Line protocol state	インタフェースのリンクレイヤプロトコルの状態です。 **UP (spoofing)**はインタフェースのリンクレイヤプロトコルですが、オンデマンドのリンクあるいは準備ができていない状態です。
Description	インタフェースの説明です。
Bandwidth	インタフェースの帯域幅です。値が0の場合、このフィールドは表示されません。
Maximum transmission unit	インタフェースのMTUです。
Internet protocol processing: Disabled	インタフェースがレイヤ3パケットを処理できないことを示します。 （インタフェースにIPアドレスが設定されていない場合に

フィールド	説明
	表示されます）
Internet address: 1.1.1.1/32 (primary)	インタフェースのIPアドレスです。primaryはIPアドレスがプライマリIPアドレスであることを示します。
Physical: Loopback	インタフェースの物理タイプがループバックです。
Last clearing of counters	インタフェースで**reset counters interface**コマンドを最後に使用した時間です。 **Never**は装置が起動してから**reset counters interface**コマンドを一度も使用していないことを示します。
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	最新の300秒の平均受信レートです。 ● **bytes/sec**–1秒間に受信した平均バイト数です。 ● **bits/sec**–1秒間に受信した平均ビット数です。 ● **packets/sec**–1秒間に受信した平均パケット数です。
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	最新の300秒の平均送信レートです。 ● **bytes/sec**–1秒間に送信した平均バイト数です。 ● **bits/sec**–1秒間に送信した平均ビット数です。 ● **packets/sec**–1秒間に送信した平均パケット数です。
Input: 0 packets, 0 bytes, 0 drops	インタフェースの受信パケットの総数とサイズ（単位はバイトです）と廃棄したパケット数（インタフェースがトラフィック統計情報の収集をサポートしている場合に表示されます）。
Output: 0 packets, 0 bytes, 0 drops	インタフェースの送信パケットの総数とサイズ（単位はバイトです）と廃棄したパケット数インタフェースがトラフィック統計情報の収集をサポートしている場合に表示されます）。

すべてのループバックインタフェースの概要情報を表示します。

<AC> display interface loopback brief

```
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP       Description
Loop1              UP   UP(s)     --            forLAN1
```

down 状態のすべてのループバックインタフェースの情報と原因を表示します。

<AC> display interface loopback brief down

```
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface          Link Cause
```

```
Loop1                ADM  Administratively
```

表 2-2 コマンド出力

フィールド	説明
Brief information on interfaces in route mode:	ループバックインタフェースの概要情報
Link: ADM - administratively down; Stby - standby	Linkフィールドの値を説明します。 ● **ADM**–リンクが運用上、**shutdown**コマンドでシャットダウンしています。物理状態を回復する場合、**undo shutdown**コマンドを実行します。 ● **Stby**–インタフェースがバックアップインタフェースとして動作します。プライマリインタフェースを確認するには、**display interface-backup state**コマンドを実行します。
Protocol: (s) – spoofing	Protocolフィールドの値を説明します。 (s)はスプーフィングを表します。インタフェースのリンクレイヤプロトコルがupだが、リンクがオンデマンドリンクであるかまたは存在しない場合、ProtocolフィールドはUP(s)と表示されます。本属性は通常、Null 0インタフェースおよびループバックインタフェースで表示されます。
Interface	インタフェース名
Link	インタフェースの物理リンク状態です。 ● **UP**–リンクがupです。 ● **DOWN**–リンクが物理的にdownしています。 ● **ADM**–リンクが運用上でシャットダウンしています。物理状態を回復するために、**undo shutdown**コマンドを実行します。 ● **Stby**–インタフェースがstandbyインタフェースです。
Protocol	インタフェースのデータリンクレイヤプロトコルフィールドの説明です。このフィールドは**UP(s)**と表示されます。
Primary IP	インタフェースのプライマリIPアドレスです。
Description	**descrption**コマンドで設定されたインタフェースの説明 display interface briefコマンドでdescriptionキーワードを指定しなかった場合、本フィールドはインタフェース説明の最初の27文字のみ表示します。display interface briefコマンドでdescriptionキーワードを指定した場合、本フィールドはインタフェース説明を完全に表示します。
Cause	インタフェースの物理リンク状態がDOWNとなった原因です。**shutdown**コマンドでインタフェースがシャットダウン状態であるとき、このフィールドは**Administratively**と表示されます。物理状態を回復するために、**undo shutdown**コマンド

フィールド	説明
	を実行します。

関連コマンド

- **interface loopback**
- **reset counters interface loopback**

2.1.3 display interface null

Syntax

display interface null [**0**] [**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

0: Null 0 インタフェースを指定します。

brief: インタフェースの概要情報を表示します。指定しない場合、詳細なインタフェースの情報を表示します。

description: 完全なインタフェースの説明を表示します。指定しない場合、説明の最初の 27 文字のみを表示します。

down: down 状態のインタフェースの情報と原因を表示します。指定しない場合、すべての状態のインタフェースの情報を表示します。

説明

display interface null コマンドは Null インタフェースの情報を表示します。

null キーワードを指定しなかった場合、コマンドは装置のすべてのインタフェースの情報を表示します。

null キーワードを指定したが 0 キーワードを指定しなかった場合、コマンドは Null 0 インタフェースの情報を表示します（Null インタフェースがトラフィック統計情報の収集をサポートしている場合）。

例

Null 0 インタフェースの詳細情報を表示します。(Null インタフェースがトラフィック統計情報の収集をサポートしている場合)。

<AC> display interface null 0

```
NULL0
Current state: UP
Line protocol state: UP(spoofing)
Description: NULL0 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Internet protocol processing: Disabled
Physical: NULL DEV
Last clearing of counters: Never
Last 300 seconds input rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Null 0 インタフェースの概要情報を表示します。(Null インタフェースがトラフィック統計情報の収集をサポートしていない場合)。

<AC> display interface null 0

```
NULL0
Current state: UP
Line protocol state: UP(spoofing)
Description:  NULL0 Interface
Maximum transmit unit: 1500
Internet protocol processing: Disabled
Physical: NULL DEV
Last clearing of counters: Never
```

Null 0 インタフェースの概要情報を表示します。

<AC> display interface null 0 brief

```
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP       Description
NULL0              UP   UP(s)    --
```

コマンド出力は表 2-1、表 2-2 を参照してください。

関連コマンド

- **interface null**

- **reset counters interface null**

2.1.4 interface loopback

Syntax

interface loopback *interface-number*

undo interface loopback *interface-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

*interface-numbe*r: ループバックインタフェースを指定します。値は 0 です。

説明

interface loopback コマンドはループバックインタフェースを作成し、loopback interface view に移行します。

undo interface loopback コマンドはループバックインタフェースを削除します。

ループバックインタフェースの物理レイヤの状態とリンクレイヤプロトコルは手動でシャットダウンしない限り、常に up 状態です。このため、以下の目的に使用することができます。

- インタフェースの物理状態に影響されることなく、接続状態となります。
- 接続の信頼性を改善します。

たとえば、次のようなことができます。

- FTP 接続を確立するために送信元インタフェースとしてループバックインタフェースを設定
- BGP においてルータ ID としてのループバックインタフェースアドレス。

例

インタフェースループバック 0 を作成します。

<AC> system-view

[AC] interface loopback 0

[AC-LoopBack0]

2.1.5 interface null

Syntax

interface null 0

デフォルト

装置は 1 つの Null インタフェース(Null 0)があります。作成あるいは削除することができません。

View

System view

定義済みユーザロール

network-admin

パラメータ

0: Null 0 インタフェースを指定します。Null インタフェースの番号は常に 0 です。

説明

interface null コマンドは null interface view に移行します。

例

null 0 interface view に移行します。

<AC> system-view

[AC] interface null 0

[AC-NULL0]

2.1.6 reset counters interface loopback

Syntax

reset counters interface loopback [*interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface-number: ループバックインタフェースの番号を指定します。番号は存在するループバックのインタフェースの番号です。番号を指定しない場合、装置のすべての既存するループバックインタフェースの統計情報を削除します。

説明

reset counters interface loopback コマンドは指定した、あるいはすべての既存のループバックインタフェースの統計情報を削除します。

一定期間、ループバックインタフェースのトラフィックの統計情報を収集する場合、以前に収集された統計情報の履歴を削除するために **reset counters interface** [**loopback** [*interface-number*]]コマンドを使用します。その後、自動で統計情報を収集します。

このコマンドは少なくとも 1 つのループバックインタフェースが作成されている場合のみ有効です。

例

ループバックインタフェース 0 の統計情報を削除します。

<AC> reset counters interface loopback 0

関連コマンド

display interface loopback

2.1.7 reset counters interface null

Syntax

reset counters interface null [**0**]

View

User view

定義済みユーザロール

network-admin

パラメータ

0: Null 0 インタフェースを指定します。Null インタフェースの番号は常に 0 です。

説明

reset counters interface null コマンドは Null インタフェースの統計情報を削除します。

一定期間、Null インタフェースのトラフィックの統計情報を収集する場合、以前に収集された統計情報の履歴を削除するために**reset counters interface** [**null** [**0**]]コマンドを使用します。その後、自動で統計情報を収集します。

例

Null 0 インタフェースの統計情報を削除します。

<AC> reset counters interface null 0

関連コマンド

display interface null

2.1.8 shutdown

Syntax

shutdown

undo shutdown

デフォルト

up

View

Loopback interface view

定義済みユーザロール

network-admin

説明

shutdown コマンドはループバックインタフェースをシャットダウンします。

undo shutdown コマンドはループバックインタフェースを up にします。

このコマンドはインタフェースの接続を切断し、通信を行うためのインタフェースを無効にするため、**shutdown** コマンドを使用する際には影響を考慮してください。

例

ループバックインタフェース Loopback 0 をシャットダウンします。

<AC> system-view

[AC] interface loopback 0

[AC-LoopBack0] shutdown

目次

このセクションのページは **3-x-x** です。

3 章 Interface range 3-1
3.1 Interface range 設定コマンド 3-1
3.1.1 display interface range 3-1
3.1.2 interface range 3-2
3.1.3 interface range name 3-3

3章 Interface range

3.1 Interface range設定コマンド

3.1.1 display interface range

Syntax

display interface range [**name** *name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *name*: インタフェースレンジの名前を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。指定しない場合、**interface range name** コマンドで作成されたすべてのインタフェースレンジの情報を表示します。

説明

display interface range コマンドは **interface range name** コマンドを使用して作成されたインタフェースレンジの情報を表示します。

例

interface range name コマンドを使用して作成されたすべての既存のインタフェースレンジの情報を表示します。

<AC> display interface range

```
Interface range name t2 GigabitEthernet1/0/1 GigabitEthernet1/0/2
Interface range name test GigabitEthernet1/0/5 GigabitEthernet1/0/6
```

出力は以下のことを示します。

- インタフェースレンジ **t2** に GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 が追加されています。
- インタフェースレンジ **test** に GigabitEthernet 1/0/5 と GigabitEthernet 1/0/6 が追加されています。

関連コマンド

interface range name

3.1.2 interface range

Syntax

interface range *interface-list*

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-list: インタフェースを指定します。半角スペースで区切り、5 までインタフェースを指定するか、インタフェースの範囲を指定します。インタフェースの範囲の形式は *interface-type interface-number* **to** *interface-type interface-number* です。*interface-type interface-number1* **to** *interface-type interface-number2* を指定したとき、*interface-number2* は *interface-number1* 以上の値にしてください。

説明

interface range コマンドはインタフェースレンジを作成し、interface range view に移行します。

同じ機能を 1 つずつインタフェースに設定するかわりに、interface range view に移行して複数のインタフェースをまとめて実行することができます。たとえば、インタフェースの範囲をシャットダウンするため、interface range view で **shutdown** コマンドを実行します。

interface range view では、最初に指定したインタフェースでサポートされるコマンドのみが有効です。最初に指定するインタフェースは **interface range** コマンドで指定されます。インタフェースレンジのコマンドを表示する場合、interface range view に移行し、インタフェースのコマンドラインで疑問符（**?**）を入力します。

interface range view でコマンドを実行した後、以下のいずれかの状態が起こる可能性があります。

- システムは、エラーメッセージを表示し interface range view にとどまります。それは、メンバインタフェースで実行が失敗したことを意味します。
  - □ 最初のメンバインタフェースで失敗した場合、コマンドはどのメンバインタフェースでも実行されません。
  - □ 最初のメンバインタフェース以外で失敗した場合、コマンドは他のメンバインタフェースでは有効となります。
- システムは system view に戻ります。それは、以下を意味します。
  - □ コマンドは system view と interface view のいずれでもサポートされています。

- □ interface range view において、メンバインタフェースでの実行に失敗しましたが、system view で成功しました。
- □ コマンドは、それ以降のメンバインタフェースで実行されませんでした。

display this コマンドで、それぞれのメンバインタフェースの interface view における設定を確認することができます。また、system view での設定が不要な場合、設定を取り消すために **undo** コマンドを使用してください。

インタフェースレンジの最初に指定したインタフェースの設定を確認する場合、interface range view で **display this** コマンドを実行します。

インタフェースレンジの設定を行う場合、以下のガイドラインに従ってください。

- インタフェースレンジで最初に指定するインタフェースを設定する前に、**interface** *interface-type interface-number* コマンドを使用してインタフェースの view に移行できることを確認してください。
- インタフェースレンジにアグリゲートインタフェースとアグリゲートインタフェースのメンバインタフェースの両方を割り当てないでください。アグリゲートインタフェースとアグリゲートインタフェースのメンバインタフェースの両方で実行すると、コマンドはアグリゲーションに失敗します。
- インタフェースレンジのインタフェースの最大数の制限の設定はありません。インタフェースレンジで多くのインタフェースを設定する場合、実行時間が長くなります。

例

GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 をシャットダウンします。

<AC> system-view

[AC] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/4

[AC-if-range] shutdown

3.1.3 interface range name

Syntax

interface range name *name* [**interface** *interface-list*]

undo interface range name *name*

View

System view

定義済みユーザロール

network-admin

パラメータ

name: インタフェースレンジの名前を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

interface-list: インタフェースを指定します。半角スペースで区切り、5 つまでインタフェースを指定するか、インタフェースの範囲を指定します。インタフェースの範囲の形式は *interface-type interface-number* **to** *interface-type interface-number* です。*interface-type interface-number1* **to** *interface-type interface-number2* を指定したとき、*interface-number2* は *interface-number1* 以上の値にしてください。

説明

interface range name *name* **interface** *interface-list* コマンドはインタフェースレンジを作成し、インタフェースレンジの名前を設定し、interface range view に移行します。

interface パラメータを指定しない **interface range name** *name* コマンドは、指定された名前のインタフェースレンジの view に移行します。

undo interface range name コマンドは指定された名前のインタフェースレンジを削除します。

インタフェースレンジに名前を割り当てるために、コマンドを使用することができます。インタフェースレンジではなくインタフェースの名前を指定して interface range view に移行することができます。

interface range view では、最初に指定したインタフェースでサポートされているコマンドのみ有効です。インタフェースレンジの最初に指定したインタフェースでサポートされるコマンドを表示する場合、interface range view に移行し、インタフェースのコマンドラインで疑問符（**?**）を入力します。

interface range view でコマンドを実行した後、以下のいずれかの状態が起こる可能性があります。

- システムは、エラーメッセージを表示し interface range view にとどまります。それは、メンバインタフェースで実行が失敗したことを意味します。
  - □ 最初のメンバインタフェースで失敗した場合、コマンドはどのメンバインタフェースでも実行されません。
  - □ 最初のメンバインタフェース以外で失敗した場合、コマンドは他のメンバインタフェースでは有効となります。
- システムは、system view に戻ります。それは、以下を意味します。
  - □ コマンドは system view と interface view のいずれでもサポートされています。
  - □ interface range view において、メンバインタフェースでの実行に失敗しましたが、system view で成功しました。
  - □ コマンドは、それ以降のメンバインタフェースで実行されませんでした。

display this コマンドで、それぞれのメンバインタフェースの interface view における設定を確認することができます。また、system view での設定が不要な場合、設定を取り消すために **undo** コマンドを使用してください。

インタフェースレンジの最初に指定したインタフェースの設定を確認する場合、interface range view で **display this** コマンドを実行します。

インタフェースレンジのメンバインタフェースを表示する場合、**display interface range** コマンドを使用します。

インタフェースレンジの設定を行う場合、以下のガイドラインに従ってください。

- インタフェースレンジで最初に指定するインタフェースを設定する前に、**interface** *interface-type interface-number* コマンドを使用してインタフェースの view に移行できることを確認してください。
- インタフェースレンジにアグリゲートインタフェースとアグリゲートインタフェースのメンバインタフェースの両方を割り当てないでください。アグリゲートインタフェースとアグリゲートインタフェースのメンバインタフェースの両方で実行すると、コマンドはアグリゲーションに失敗します。
- インタフェースレンジのインタフェースの最大数の制限の設定はありません。インタフェースレンジで多くのインタフェースを設定する場合、実行時間が長くなります。
- インタフェースレンジの名前の最大数はシステムリソースによってのみ制限されます。インタフェースレンジの設定を保証するため、インタフェースレンジの名前は 1000 個より小さくしてください。

例

インタフェースレンジ **myEthPort** に GigabitEthernet 1/0/1～GigabitEthernet 1/0/6 を追加し、interface range view に移行します。

<AC> system-view

[AC] interface range name myEthPort interface gigabitethernet 1/0/1 to gigabitethernet 1/0/6

[AC-if-range-myEthPort]

インタフェースレンジ **myEthPort** の view に移行します。

<AC> system-view

[AC] interface range name myEthPort

[AC-if-range-myEthPort]

関連コマンド

display interface range

QX-W2230AC アクセスコントローラ

コマンドマニュアル

4. アクセス

本マニュアルは以下に示す章で構成されています。

01-MAC アドレステーブル

02-リンクアグリゲーション

03-VLAN

04-STP

05-ループ検出

06-LLDP

07-レイヤ 2 フォワーディングの設定

目次

このセクションのページは **4-x-x** です。

1 章 MAC アドレステーブル 1-1
1.1 MAC アドレステーブル設定コマンド 1-1
1.1.1 display mac-address 1-1
1.1.2 display mac-address aging-time 1-3
1.1.3 display mac-address mac-learning 1-3
1.1.4 mac-address (interface view) 1-4
1.1.5 mac-address (system view) 1-6
1.1.6 mac-address mac-learning enable 1-8
1.1.7 mac-address max-mac-count 1-9
1.1.8 mac-address max-mac-count enable-forwarding 1-10
1.1.9 mac-address timer 1-12
1.1.10 snmp-agent trap enable mac-address 1-13

1章 MAC アドレステーブル

1.1 MACアドレステーブル設定コマンド

1.1.1 display mac-address

Syntax

display mac-address [*mac-address* [**vlan** *vlan-id*] | [[**dynamic** | **static**] [**interface** *interface-type interface-number*] | **blackhole**] [**vlan** *vlan-id*] [**count**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address: MAC アドレスを指定します。形式は H-H-H です。H の先頭から 0 が続く場合は省略できます。たとえば、000f-00e2-0001 は、f-e2-1 と省略できます。

vlan *vlan-id*: VLAN ID を指定します。設定範囲は 1～4094 です。

dynamic: ダイナミック MAC アドレスエントリを表示します。

static: スタティック MAC アドレスエントリを表示します。

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

blackhole: ブラックホール MAC アドレスエントリを表示します。

count: コマンドで指定したすべてのエントリに一致する MAC アドレスエントリ数のみを表示します。MAC アドレスエントリの詳細は表示されません。たとえば、VLAN 20 のダイナミックエントリ数を表示する場合、**display mac-address vlan** *20* **dynamic count** コマンドを使用します。エントリの属性が指定されない場合、MAC アドレステーブルのエントリ数を表示します。**count** を指定しない場合、指定された MAC アドレスエントリの詳細情報を表示します。

説明

display mac-address コマンドは MAC アドレスエントリを表示します。

MAC アドレスエントリは宛先 MAC アドレス、出力インタフェース、VLAN ID が含まれます。

パラメータを指定しない場合、すべての MAC アドレスエントリを表示します。

アグリゲートインタフェースに少なくとも 1 つの Selected メンバポートがある場合、アグリゲートインタフェースのダイナミック MAC アドレスエントリのみ表示します。

例

VLAN 100 の MAC アドレスエントリを表示します。

<AC> display mac-address vlan 100

```
MAC Address      VLAN ID    State          Port/NickName          Aging
0033-0033-0033   100        Blackhole       N/A                   N
0000-0000-0002   100        Static         GE1/0/3                N
0000-0000-5829   100        Learned        GE1/0/4                Y
```

MAC アドレスエントリ数を表示します。

<AC> display mac-address count

```
1 mac address(es) found.
```

表 1-1 コマンド出力

フィールド	説明
VLAN ID	MACアドレスエントリが所属する出力インタフェースのVLAN IDです。
State	MACアドレスエントリの状態です。 ● **Static**—スタティックMACアドレスエントリです。 ● **Learned**—ダイナミックMACアドレスエントリです。ダイナミックエントリは自動あるいは手動で設定されたものがあります。 ● **Blackhole**—ブラックホールMACアドレスエントリです。
Port/NickName	MACアドレスに関連づけられるパケットの出力インタフェースです。ブラックホールMACアドレスエントリの場合、**N/A**と表示されます。
Aging	エントリがエージングアウト可能かどうかを示します。 ● **Y**—エントリはエージングアウト可能です。 ● **N**—エントリはエージングアウトできません。
mac address(es) found	MACアドレスエントリに一致する数です。

関連コマンド

- **mac-address**
- **mac-address timer**

1.1.2 display mac-address aging-time

Syntax

display mac-address aging-time

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display mac-address aging-time コマンドはダイナミック MAC アドレスエントリのエージングタイマを表示します。

例

ダイナミック MAC アドレスエントリのエージングタイマを表示します。

<AC> display mac-address aging-time

```
MAC address aging time: 300s.
```

関連コマンド

mac-address timer

1.1.3 display mac-address mac-learning

Syntax

display mac-address mac-learning [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

インタフェースを指定しない場合、グローバル MAC アドレスの学習状態とすべてのインタフェースの MAC アドレスの学習状態を表示します。

説明

display mac-address mac-learning コマンドはグローバル MAC アドレスの学習状態と指定された、あるいはすべてのインタフェースの MAC アドレスの学習状態を表示します。

例

グローバル MAC アドレスの学習状態とすべてのインタフェースの MAC アドレスの学習状態を表示します。

<AC> display mac-address mac-learning

```
Global MAC address learning status: Enabled.

Port                    Learning Status
GE1/0/1                  Enabled
GE1/0/2                  Enabled
GE1/0/3                  Enabled
GE1/0/4                  Enabled
```

表 1-2 コマンド出力

フィールド	説明
Global MAC address learning status	グローバルMACアドレスの学習状態です。 ● 有効です。 ● 無効です。
Learning Status	インタフェースのMACアドレスの学習状態を表示します。 ● 有効です。 ● 無効です。

関連コマンド

mac-address mac-learning enable

1.1.4 mac-address (interface view)

Syntax

mac-address { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*

undo mac-address { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

dynamic: ダイナミック MAC アドレスエントリを指定します。

static: スタティック MAC アドレスエントリを指定します。

mac-address: MAC アドレスを指定します。マルチキャスト MAC アドレスとすべてが 0 の MAC アドレスを除きます。形式は H-H-H です。H の先頭から 0 が続く場合は省略できます。たとえば、000f-00e2-0001 は、f-e2-1 と省略できます。

vlan *vlan-id*: 指定されたインタフェースが所属する既存の VLAN ID を指定します。設定範囲は 1～4094 です。

説明

mac-address コマンドはインタフェースの MAC アドレスエントリを追加あるいは修正します。

undo mac-address コマンドはインタフェースの MAC アドレスエントリを削除します。

一般的に、装置は自動で各インタフェースの受信フレームの送信元 MAC アドレスによって学習された MAC アドレステーブルを構築します。しかし、手動でスタティック MAC アドレスエントリを設定することができます。手動で設定されたスタティック MAC アドレスエントリはダイナミック MAC アドレスエントリよりも優先されます。インタフェースに接続されたユーザの装置のセキュリティを向上するため、ユーザの装置をインタフェースに関連づけるため、スタティックエントリを設定します。ユーザの装置（たとえばホスト A）のフレームは常にインタフェースから送信されます。ホスト A の偽の MAC アドレスを使用するほかのホストはホスト A からのフレームを取得することができません。

MAC アドレスエントリの設定は、設定を保存しないと、再起動により削除されます。ただしダイナミック MAC アドレスエントリは設定の保存に関わらず、再起動により削除されます。

例

VLAN 2 に所属する GigabitEthernet 1/0/1 に MAC アドレス 000f-e201-0101 のスタティック MAC アドレスエントリを追加します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] mac-address static 000f-e201-0101 vlan 2

VLAN 1 に所属するアグリゲートインタフェース Bridge-Aggregation 1/0/1 に MAC アドレス 000f-e201-0101 のスタティック MAC アドレスエントリを追加します。

<AC> system-view

[AC] interface bridge-aggregation 1

[AC-Bridge-Aggregation1] mac-address static 000f-e201-0102 vlan 1

関連コマンド

- **display mac-address**
- **mac-address (system view)**

1.1.5 mac-address (system view)

Syntax

mac-address { **dynamic** | **static** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

mac-address blackhole *mac-address* **vlan** *vlan-id*

undo mac-address [[**dynamic** | **static**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*]

undo mac-address [**blackhole** | **dynamic** | **static**] [*mac-address*] **vlan** *vlan-id*

undo mac-address [**dynamic** | **static**] **interface** *interface-type interface-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

dynamic: ダイナミック MAC アドレスエントリを指定します。

static: スタティック MAC アドレスエントリを指定します。

blackhole: ブラックホール MAC アドレスエントリを指定します。宛先 MAC アドレスがブラックホール MAC アドレスに一致している場合、パケットは廃棄されます。

mac-address: MAC アドレスを指定します。マルチキャスト MAC アドレスとすべてが 0 の MAC アドレスを除きます。形式は H-H-H です。H の先頭から 0 が続く場合は省略できます。たとえば、000f-00e2-0001 は、f-e2-1 と省略できます。

vlan *vlan-id*: 指定されたインタフェースが所属する既存の VLAN ID を指定します。設定範囲は 1～4094 です。

interface *interface-type interface-number*: 出力インタフェースのタイプと番号を指定します。

説明

mac-address コマンドは MAC アドレスエントリを追加あるいは修正します。

undo mac-address コマンドは 1 つあるいはすべての MAC アドレスエントリを削除します。

以下のタイプの MAC アドレスエントリを設定することができます。

- ダイナミックエントリ

ダイナミックエントリは手動で設定されたダイナミックエントリと自動で学習されたダイナミックエントリが含まれます。

- スタティックエントリ

手動で設定されたスタティックエントリはダイナミックエントリよりも優先します。インタフェースに接続された装置のセキュリティを向上するため、インタフェースに割り当てる装置のスタティックエントリを設定します。装置向け（たとえば、Host A）のフレームは常にインタフェースに送信されます。Host A の MAC アドレスに偽造させた MAC アドレスを使用するほかのホストは Host A 向けのフレームを受信することができません。

- ブラックホールエントリ

指定された宛先 MAC アドレスのフレームを廃棄するため、ブラックホールエントリを設定することができます。

スタティックあるいはブラックホール MAC アドレスエントリはダイナミック MAC アドレスエントリに上書きすることができます。ダイナミック MAC アドレスエントリはスタティックあるいはブラックホール MAC アドレスエントリに上書きすることはできません。

パラメータを指定しないで **undo mac-address** コマンドを実行した場合、すべてのユニキャスト MAC アドレスエントリを削除します。

指定した VLAN のすべての MAC アドレスエントリを削除することができます。また特定のタイプ（ダイナミック、スタティック、ブラックホール）の MAC アドレスエントリのみを削除することができます。1 つのインタフェースのみを選択することで、対応する MAC アドレスエントリを削除します。

MAC アドレスエントリの設定は、設定を保存しないと、再起動により削除されます。ただしダイナミック MAC アドレスエントリは設定の保存に関わらず、再起動により削除されます。

例

MAC アドレス 000f-e201-0101 のスタティックエントリを追加します。次に、この MAC アドレスを宛先とするすべてのフレームが VLAN 2 に所属する GigabitEthernet 1/0/1 から送信します。

<AC> system-view

[AC] mac-address static 000f-e201-0101 interface gigabitethernet 1/0/1 vlan 2

関連コマンド

- **display mac-address**
- **mac-address (interface view)**

1.1.6 mac-address mac-learning enable

Syntax

mac-address mac-learning enable

undo mac-address mac-learning enable

デフォルト

有効

View

System view

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

mac-address mac-learning enable コマンドはグローバル、インタフェースで MAC アドレスの学習を有効にします。

undo mac-address mac-learning enable コマンドはグローバル、インタフェースで MAC アドレスの学習を無効にします。

MAC アドレステーブルが一杯になることを防ぐため、MAC アドレステーブルの学習を無効にすることができます。

たとえば、攻撃者からの異なる送信元 MAC アドレスの大量のパケットを学習しないように、以下のガイドラインに従い、装置で MAC アドレスの学習を無効にすることができます。

- インタフェースごとに MAC アドレスの学習を無効にすることができます。グローバルで MAC アドレスの学習を無効にした場合、すべてのインタフェースで MAC アドレスの学習が無効になります。装置は MAC アドレスの学習を停止し、ダイナミックに MAC アドレステーブルのアップデートを行うことができません。
- MAC アドレスの学習を無効にすると、ブロードキャストストームが発生する可能性あるため、インタフェースで MAC アドレスの学習を無効にしたのち、ブロードキャストストームの抑制を行ってください。ブロードキャストストームの抑制の詳細は、オペレーションマニュアルのセクション 3 *インタフェース　"Ethernet インタフェース"* を参照してください。
- グローバルで MAC アドレスの学習を有効にし、インタフェースで MAC アドレスの学習を無効にすることができます。
- MAC アドレスの学習を無効にしたとき、装置はインタフェースにある既存のダイナミック MAC アドレスエントリを即座に削除します。

例

グローバルで MAC アドレスの学習を無効にします。

<AC> system-view

[AC] undo mac-address mac-learning enable

GigabitEthernet 1/0/1 で MAC アドレスの学習を無効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] undo mac-address mac-learning enable

アグリゲートインタフェース Bridge-Aggregation 1 で MAC アドレスの学習を無効にします。

<AC> system-view

[AC] interface bridge-aggregation 1

[AC-Bridge-Aggregation1] undo mac-address mac-learning enable

関連コマンド

display mac-address mac-learning

1.1.7 mac-address max-mac-count

Syntax

mac-address max-mac-count *count*

undo mac-address max-mac-count

デフォルト

3072

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

count: インタフェースで学習できる MAC アドレスの最大数を指定します。値の範囲は 0～3072 です。引数が 0 に設定されている場合、インタフェースは MAC アドレスの学習が行われません。

説明

mac-address max-mac-count コマンドはインタフェースで学習できる MAC アドレスの最大数を設定します。

undo mac-address max-mac-count コマンドはデフォルトに戻します。

mac-address max-mac-count コマンドは MAC アドレステーブルのサイズを制限するため、MAC アドレスエントリ数を制限します。

MAC アドレステーブルが大きくなるとフォワーディングの性能に影響します。インタフェースで学習した MAC アドレスの数が上限に達した場合、インタフェースは MAC アドレスエントリの学習を停止します。

例

GigabitEthernet 1/0/1 で学習できる MAC アドレスエントリの最大数を 600 に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] mac-address max-mac-count 600

関連コマンド

- **mac-address**
- **mac-address max-mac-count enable-forwarding**

1.1.8 mac-address max-mac-count enable-forwarding

Syntax

mac-address max-mac-count enable-forwarding

undo mac-address max-mac-count enable-forwarding

デフォルト

有効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

mac-address max-mac-count enable-forwarding コマンドはインタフェースで学習できる MAC アドレスの数が制限に到達したのち、インタフェースで受信された未知のフレームを装置が転送することを有効にします。

undo mac-address max-mac-count enable-forwarding コマンドはインタフェースで学習できる MAC アドレスの数が制限に到達したのち、インタフェースで受信された未知のフレームを装置が転送することを無効にします。

未知のフレームとは、送信元 MAC アドレスが MAC アドレステーブルにないフレームを指します。

例

MAC アドレスエントリを最大 600 まで学習できるように GigabitEthernet 1/0/1 を設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] mac-address max-mac-count 600

GigabitEthernet 1/0/1 で学習できる MAC アドレスの数が制限に到達したのち、GigabitEthernet 1/0/1 で受信された未知のフレームを装置が転送することを無効にします。

[AC-GigabitEthernet1/0/1] undo mac-address max-mac-count enable-forwarding

関連コマンド

- **mac-address**
- **mac-address max-mac-count**

1.1.9 mac-address timer

Syntax

mac-address timer { **aging** *seconds* | **no-aging** }

undo mac-address timer

デフォルト

300 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

aging *seconds*: ダイナミック MAC アドレスエントリのエージングタイマー（秒単位）を設定します。範囲は 10～1400 です。

no-aging: ダイナミック MAC アドレスエントリをエージアウトしないように設定します。

説明

mac-address timer コマンドはダイナミック MAC アドレスエントリのエージングタイマを設定します。

undo mac-address timer コマンドはデフォルトに戻します。

適切にエージングタイマを設定するために、以下のガイドラインに従ってください。

- エージング間隔が長いと、エージング時間が終了したエントリを MAC アドレステーブルに残す可能性があり、最新のネットワークの変化に対応できなくなる可能性があります。
- エージング間隔が短いと、有効なエントリを削除してしまい、装置のパフォーマンスに影響を及ぼす不要なブロードキャストを送信する結果になる可能性があります。

例

ダイナミック MAC アドレスエントリのエージングタイマを 500 秒に設定します。

<AC> system-view

[AC] mac-address timer aging 500

関連コマンド

display mac-address aging-time

1.1.10 snmp-agent trap enable mac-address

Syntax

snmp-agent trap enable mac-address

undo snmp-agent trap enable mac-address

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable mac-address コマンドは MAC アドレステーブルの SNMP notification の送信を有効にします。

undo snmp-agent trap enable mac-address コマンドは MAC アドレステーブルの SNMP notification の送信を無効にします。

MAC アドレステーブルの SNMP notification の送信が無効であるとき、MAC アドレスが移動した場合、information center モジュールに作成されたログメッセージを通知します。MAC アドレステーブルは、MAC アドレスの移動に関する SNMP notification の送信のみをサポートします。

MAC アドレスの移動に関する SNMP notification の送信が有効であるとき、MAC アドレステーブルの SNMP notification のすべてのタイプを有効にします。MAC アドレスの移動に関する SNMP notification の送信が無効であるとき、MAC アドレステーブルの SNMP notification のすべてのタイプを無効にします。

例

MAC アドレステーブルで MAC アドレスが移動した場合 SNMP notification の送信を無効にします。

<AC> system-view

[AC] undo snmp-agent trap enable mac-address mac-move

関連コマンド

mac-address notification mac-move

目次

このセクションのページは **4-x-x** です。

2 章 リンクアグリゲーション.....2-1
2.1 リンクアグリゲーション設定コマンド.....2-1
2.1.1 description.....2-1
2.1.2 display interface.....2-2
2.1.3 display link-aggregation load-sharing mode.....2-5
2.1.4 display link-aggregation member-port.....2-7
2.1.5 display link-aggregation summary.....2-9
2.1.6 display link-aggregation verbose.....2-10
2.1.7 interface bridge-aggregation.....2-13
2.1.8 link-aggregation global load-sharing mode.....2-14
2.1.9 link-aggregation load-sharing mode.....2-15
2.1.10 link-aggregation selected-port maximum.....2-16
2.1.11 link-aggregation selected-port minimum.....2-17
2.1.12 port link-aggregation group.....2-18
2.1.13 reset counters interface.....2-19
2.1.14 shutdown.....2-20

2章 リンクアグリゲーション

2.1 リンクアグリゲーション設定コマンド

2.1.1 description

Syntax

description *text*

undo description

デフォルト

インタフェース名＋Interface です。（たとえばアグリゲートインタフェース Bridge-Aggregation1 のデフォルトは Bridge-Aggregation1 Interface です）

View

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

text: インタフェースの説明を指定します。設定範囲は 1～255 文字です。

説明

description コマンドはインタフェースの説明を設定します。

undo description コマンドはデフォルトに戻します。

例

アグリゲートインタフェース Bridge-Aggregation 1 の説明を connect to the lab に設定します。

<AC> system-view

[AC] interface bridge-aggregation 1

[AC-Bridge-Aggregation1] description connect to the lab

2.1.2 display interface

Syntax

display interface bridge-aggregation [*interface-number*] [**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

bridge-aggregation: レイヤ 2 アグリゲートインタフェースを指定します。

interface-number: 既存のアグリゲートインタフェース番号を指定します。設定範囲は、すべての既存のアグリゲートインタフェース番号の範囲です。

brief: インタフェースの概要情報を表示します。指定されない場合、コマンドは詳細なインタフェース情報を表示します。

description: インタフェースの説明をすべて表示します。指定しない場合、インタフェースの説明の最初の 27 文字のみ表示します。

down: down 状態のインタフェースの情報と原因を表示します。指定しない場合、すべての状態のインタフェース情報を表示します。

説明

display interface コマンドはアグリゲートインタフェースの情報を表示します。

bridge-aggregation パラメータを指定しない場合、すべてのインタフェースの情報を表示します。

bridge-aggregation パラメータとインタフェース番号を指定した場合、指定したアグリゲートインタフェースの情報を表示します。

例

レイヤ 2 アグリゲートインタフェース Bridge-Aggregation 1 の詳細情報を表示します。

<AC> display interface bridge-aggregation 1

```
Bridge-Aggregation1
Current state: UP
IP packet frame type: PKTFMT_ETHNT_2, hardware address: 000f-e207-f2e0
Description: Bridge-Aggregation1 Interface
Bandwidth: 1000kbps
2Gbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
```

```
PVID: 1
Port link-type: Access
 Tagged VLANs:   None
 UnTagged VLANs: 1
Last clearing of counters:  Never
Last 300 second input:  6900 packets/sec 885160 bytes/sec    0%
Last 300 second output:  3150 packets/sec 404430 bytes/sec    0%
Input (total):  5364747 packets, 686688416 bytes
        2682273 unicasts, 1341137 broadcasts, 1341337 multicasts, 0 pauses
Input (normal):  5364747 packets, 686688416 bytes
        2682273 unicasts, 1341137 broadcasts, 1341337 multicasts, 0 pauses
Input:  0 input errors, 0 runts, 0 giants, 0 throttles
        0 CRC, 0 frame, 0 overruns, - aborts
        - ignored, - parity errors
Output (total): 1042508 packets, 133441832 bytes
        1042306 unicasts, 0 broadcasts, 202 multicasts, - pauses
Output (normal): 1042508 packets, 133441832 bytes
        1042306 unicasts, 0 broadcasts, 202 multicasts, 0 pauses
Output: 0 output errors, - underruns, - buffer failures
        0 aborts, 0 deferred, 0 collisions, 0 late collisions
        - lost carrier, - no carrier
```

レイヤ2アグリゲートインタフェース Bridge-Aggregation 1 の概要情報を表示します。

<AC> display interface bridge-aggregation 1 brief

```
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) – auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface          Link Speed   Duplex Type PVID Description
BAGG1              UP   auto    A     A    1
```

表 2-1 コマンド出力

フィールド	説明
Bridge-Aggregation1	レイヤ2アグリゲートインタフェース名です。
Current state	アグリゲートインタフェースの状態です。 ● **Administratively DOWN**–**shutdown**コマンドでインタフェースがシャットダウンしています。 ● **DOWN**–**shutdown**コマンドでシャットダウンしていませんが、物理的にdownしています。（イーサネットケーブルが物理的に接続されていない、あるいはリンクに失敗している可能性があります）

フィールド	説明
	● **UP**–インタフェースが運用上も物理的にも起動している状態です。
IP packet frame type	IPv4パケットのフレームフォーマットです。 PKTFMT_ETHNT_2は、パケットがEthernet Ⅱ形式でカプセル化されていることを示します。
Bandwidth	インタフェースの予期された帯域幅です。帯域幅が0kbpsの場合、フィールドは表示されません。
Unknown-speed mode, unknown-duplex mode	インタフェースの通信速度と通信モードが不明です。
Port link-type	インタフェースのリンクタイプです。 ● accessです。 ● trunkです。 ● hybridです。
Tagged VLANs	パケットがVLANタグをつけてインタフェースに送信されるVLANです。
Untagged VLANs	パケットがVLANタグなしでインタフェースに送信されるVLANです。
Last clearing of counters	インタフェースで**reset counters interface**コマンドを最後に使用してからの総時間です。 **Never**は装置が起動してから**reset counters interface**コマンドを一度も使用していないことを示します。
Last 300 second input/output rate	過去300秒以内の平均送受信のトラフィックレートです。
Input/Output (total)	インタフェースで送受信されたすべてのパケットの統計情報です。
Input/Output (normal)	インタフェースで送受信されたすべての正常なパケットの統計情報です。
Brief information on interfaces in bridge mode	レイヤ2インタフェースの概要情報です。
Link: ADM - administratively down; Stby - standby	リンクの状態です。 ● **ADM**– **shutdown**コマンドでインタフェースがシャットダウンしています。物理状態を回復する場合、**undo shutdown**コマンドを実行します。 ● **Stby**–インタフェースがバックアップインタフェースとして動作します。
Speed: (a) - auto	インタフェースがオートネゴシエーションに設定されている場合、（**a**）で示されたオートネゴシエーションのフラグが含まれます。 インタフェースにオートネゴシエーションが設定されているがオートネゴシエーションが開始していない場合、**auto**

フィールド	説明
	と表示されます。
Duplex: (a)/A - auto; H - half; F - full	インタフェースの通信モードがオートネゴシエーションに設定されている場合、インタフェースの通信モードには（**a**）が含まれます。Hは半二重モードを示します。Fは全二重モードを示します。 インタフェースの通信モードでオートネゴシエーションを行うように設定されているが、オートネゴシエーションが開始されていない場合、通信モードにAと表示されます。
Type: A - access; T - trunk; H - hybrid	インタフェースのポートリンクタイプオプションです。
Interface	省略したインタフェース名です。
Link	インタフェースの物理状態です。 • **UP**—インタフェースが物理的にupしています。 • **DOWN**—インタフェースが物理的にdownしています。 • **ADM**— **shutdown**コマンドでインタフェースがシャットダウンしています。物理状態を回復する場合、**undo shutdown**コマンドを実行します。 • **Stby**—インタフェースがバックアップインタフェースとして動作します。
Speed	インタフェースの通信速度です。単位はbpsです。
Description	**description**コマンドを使用して設定された部分的または完全なインタフェースの説明です。 • **display interface brief**コマンドで**description**キーワードを指定しない場合、このフィールドには説明の最初の27文字が表示されます。 • **display interface brief**コマンドで**description**キーワードを指定した場合、このフィールドに完全な説明が表示されます。

2.1.3 display link-aggregation load-sharing mode

Syntax

display link-aggregation load-sharing mode [**interface** [**bridge-aggregation** *interface-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

bridge-aggregation:レイヤ 2 アグリゲートインタフェースを指定します。

interface-number: 既存のアグリゲートインタフェース番号を指定します。

説明

display link-aggregation load-sharing mode コマンドはリンクアグリゲーションロードシェアリングモードを表示します。

interface パラメータを指定しない場合、グローバルのリンクアグリゲーションロードシェアリングモードを表示します。

interface パラメータを指定し、*interface-number* を指定しない場合、すべてのアグリゲーショングループのリンクアグリゲーションロードシェアリングモードを表示します。

bridge-aggregation パラメータは装置でアグリゲートインタフェースが存在するときのみ有効です。

例

デフォルトのグローバルのリンクアグリゲーションロードシェアリングモードを表示します。

<AC> display link-aggregation load-sharing mode

```
Link-aggregation load-sharing mode:
Layer 2 traffic: packet type-based sharing
```

設定したグローバルのリンクアグリゲーションロードシェアリングモードを表示します。

<AC> display link-aggregation load-sharing mode

```
Link-aggregation load-sharing mode:
destination-mac address, source-mac address
```

レイヤ 2 アグリゲートインタフェースに対応するアグリゲーショングループ 1 のデフォルトのリンクアグリゲーションロードシェアリングモードを表示します。

<AC> display link-aggregation load-sharing mode interface bridge-aggregation 1

```
Bridge-Aggregation1 load-sharing mode:
Layer 2 traffic: packet type-based sharing
```

レイヤ 2 アグリゲートインタフェースに対応するアグリゲーショングループ 1 の設定したリンクアグリゲーションロードシェアリングモードを表示します。

<AC> display link-aggregation load-sharing mode interface bridge-aggregation 1

```
Bridge-Aggregation1 load-sharing mode:
destination-mac address, source-mac address
```

表 2-2 コマンド出力

フィールド	説明
Link-aggregation load-sharing mode	グローバルのリンクアグリゲーションのロードシェアリングモードを表示します。 デフォルトでは、レイヤ2のリンクアグリゲーションのロードシェアリングモードが表示されます。 グローバルのロードシェアリングモードを設定した場合、設定されたモードが表示されます。
Bridge-Aggregation1 load-sharing mode	アグリゲートインタフェースBridge-Aggregation 10に対応するアグリゲーショングループのリンクアグリゲーションのロードシェアリングモードです。 デフォルトでは、グローバルのリンクアグリゲーションのロードシェアリングモードが表示されます。 特にこのアグリゲーショングループのリンクアグリゲーションのロードシェアリングモードを設定した場合、設定されたモードが表示されます。
Layer 2 traffic: destination-mac address, source-mac address	レイヤ2のデフォルトのロードシェアリングモードを示します。この出力は、送信元MACアドレスと宛先MACアドレスに基づいてロードシェアリングされます。
Layer 2 traffic: packet type-based sharing	レイヤ2のデフォルトのロードシェアリングモードを示します。この出力のモードはパケットタイプです。
destination-mac address, source-mac address	設定されたリンクアグリゲーションロードシェアリングモードを示します。この出力例では、トラフィックは送信元と宛先のMACアドレスにもとづいています。

2.1.4 display link-aggregation member-port

Syntax

display link-aggregation member-port [*interface-list*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-list: リンクアグリゲーションメンバポートを指定します。形式は *interface-type interface-number* [**to** *interface-type interface-number*] です。interface-type interface-number 引数は、インタフェースのタイプと番号を指定します。

説明

display link-aggregation member-port コマンドは指定されたメンバポートのリンクアグリゲーションの詳細情報を表示します。

スタティックアグリゲーショングループのメンバポートはピアグループの情報は知りません。スタティックのアグリゲーショングループは、ローカルインタフェースのポート番号、ポートプライオリティ、使用可能なキーのみ表示されます。

例

GigabitEthernet 1/0/1 のリンクアグリゲーションの詳細情報を表示します。そのポートは、スタティックのアグリゲーショングループのメンバポートです。

<AC> display link-aggregation member-port gigabitethernet 1/0/1

```
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
      D -- Synchronization, E -- Collecting, F -- Distributing,
      G -- Defaulted, H -- Expired

GigabitEthernet1/0/1:
Aggregate Interface: Bridge-Aggregation1
Port Number: 1
Port Priority: 32768
Oper-Key: 1
```

表 2-3 コマンド出力

フィールド	説明
Flags	1バイトのLACPの状態フラグです。最下位から最上位のビットまで、以下のようにA～Hで表示されます。1が真、0が偽で示します。 • **A**－LACPが有効か無効かを示します。1が有効、0が無効です。 • **B**－LACPのタイムアウトの長さを示します。1がショートタイムアウト、0がロングタイムアウトです。 • **C**－送信システムがこのリンクを集約可能とみなすかどうかを示します。1は可能、0が不可能です。 • **D**－送信システムがこのリンクを同期しているとみなすかどうかを示します。1が同期している、0が同期していないです。 • **E**－送信システムが、受信フレームをアグリゲートして

フィールド	説明
	いるかどうかを示します。1がアグリゲートしている、0がアグリゲートしていないです。 • **F**－送信システムが、送信フレームを分配しているかどうかを示します。1が分配している、0が分配していないです。 • **G**－送信システムがデフォルトのフレームを受信するかどうかを示します。1が受信する、0が受信しないです。 • **H**－送信システムが期限切れのフレームを受信するかどうかを示します。1が受信する、0が受信しないです。
Aggregate Interface	メンバポートが所属するアグリゲートインタフェースです。
Local	ローカルインタフェースの情報です。
Oper-key	操作キーです。

2.1.5 display link-aggregation summary

Syntax

display link-aggregation summary

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display link-aggregation summary コマンドはすべてのアグリゲーショングループの概要情報を表示します。

スタティックアグリゲーショングループのメンバポートはピアグループの情報は知りません。スタティックリンクアグリゲーションのパートナーID フィールドは、**None** と表示されるか、なにも表示されません。

例

すべてのアグリゲーショングループの概要情報を表示します。

<AC> display link-aggregation summary

```
Aggregate Interface Type:
```

```
BAGG -- Bridge-Aggregation, BLAGG -- Blade-Aggregation, RAGG -- Route-Aggregation,
SCH-B – Schannel-Bundle
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 000f-e267-6c6a

AGG       AGG   Partner ID           Selected  Unselected  Individual  Share
Interface  Mode                      Ports     Ports       Ports       Type
--------------------------------------------------------------------------------
BAGG2     D    0x8000, 000f-e267-6c6a  2         0           0           Shar
```

表 2-4 コマンド出力

フィールド	説明
Aggregate Interface Type	アグリゲートインタフェースのタイプを表示します。 **BAGG** はレイヤ2を表します。
Aggregation Mode	アグリゲーショングループのタイプです。 **S** はstaticを表します。
Loadsharing Type	ロードシェアリングのタイプです。 • **Shar**—負荷分散を行います。 • **NonS**—非負荷分散を行いません。
AGG Interface	アグリゲートインタフェースのタイプと番号です。
AGG Mode	アグリゲーショングループのタイプです。
Selected Ports	Selectedポートの総数です。
Unselected Ports	Unselectedポートの総数です。
Individual Ports	個々のポートの総数です。
Share Type	ロードシェアリングタイプです。

2.1.6 display link-aggregation verbose

Syntax

display link-aggregation verbose [**bridge-aggregation** [*interface-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

bridge-aggregation:アグリゲートインタフェースを指定します。

interface-number: 既存のアグリゲートインタフェース番号を指定します。

説明

display link-aggregation verbose コマンドは指定されたアグリゲートインタフェースに対応するアグリゲーショングループの詳細情報を表示します。

bridge-aggregation パラメータのみを指定した場合、すべてのアグリゲートインタフェースの詳細情報を表示します。

bridge-aggregation パラメータのみを指定しない場合、すべてのアグリゲーショングループの詳細情報を表示します。

bridge-aggregation パラメータは装置でアグリゲートインタフェースが存在するときのみ有効です。

例

レイヤ2のダイナミックアグリゲーショングループ2に関する詳細情報を表示します。

<AC> display link-aggregation verbose bridge-aggregation 2

```
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation2
Aggregation Mode: Static
Loadsharing Type: Shar
  Port            Status  Priority Oper-Key
--------------------------------------------------------------------------------
  GE1/0/1         U       32768    1
  GE1/0/2         U       32768    1
  GE1/0/3         U       32768    1
```

表 2-5 コマンド出力

フィールド	説明
Loadsharing Type	ロードシェアリングのタイプです。 • **Shar**—負荷分散を行います。 • **NonS**—非負荷分散を行いません。
Port Status	ポートの状態です。

フィールド	説明
	• Selected • Unselected • Individual
Flags	1バイトのLACPの状態フラグです。最下位から最上位のビットまで、以下のようにA～Hで表示されます。1が真、0が偽で示します。 • **A**－LACPが有効か無効かを示します。1が有効、0が無効です。 • **B**－LACPのタイムアウトの長さを示します。1がショートタイムアウト、0がロングタイムアウトです。 • **C**－送信システムがこのリンクを集約可能とみなすかどうかを示します。1は可能、0が不可能です。 • **D**－送信システムがこのリンクを同期しているとみなすかどうかを示します。1が同期している、0が同期していないです。 • **E**－送信システムが、受信フレームをアグリゲートしているかどうかを示します。1がアグリゲートしている、0がアグリゲートしていないです。 • **F**－送信システムが、送信フレームを分配しているかどうかを示します。1が分配している、0が分配していないです。 • **G**－送信システムがデフォルトのフレームを受信するかどうかを示します。1が受信する、0が受信しないです。 • **H**－送信システムが期限切れのフレームを受信するかどうかを示します。1が受信する、0が受信しないです。
Aggregate Interface	アグリゲートインタフェースの名前です。
Aggregation Mode	アグリゲーショングループのタイプです。 **S** はstaticを表します。
Local	ローカルインタフェースの情報です。 • **Port**–ポートタイプと番号です。 • **Status**–ポート状態です。SelectedあるいはUnselected、Individualがあります。 • **Priority**–ポートプライオリティです。 • **Oper-Key**–操作キーです。 🕮 **メモ：** スタティックのアグリゲーショングループでは、Flagは表示されません。

フィールド	説明
Remote	ピアエンドの情報です。 • **Actor**–ローカルポートのタイプと番号です。 • **Partner**–ピアポートのインデックスです。 • **Priority**–ピアポートのプライオリティです。 • **Oper-Key**–ピアポートの操作キーです。 • **System ID**–ピアエンドのシステムIDです。

2.1.7 interface bridge-aggregation

Syntax

interface bridge-aggregation *interface-number*

undo interface bridge-aggregation *interface-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-number: アグリゲートインタフェースの番号を指定します。(1 で固定です。)

説明

interface bridge-aggregation コマンドはアグリゲートインタフェースを作成し、aggregate interface view に移行します。すでにアグリゲートインタフェースが存在する場合、aggregate interface view に移行します。

undo interface bridge-aggregation コマンドはアグリゲートインタフェースを削除します。

アグリゲートインタフェースを作成したとき、システムは自動的に同一番号のアグリゲーショングループを作成します。デフォルトのアグリゲーショングループはスタティックのアグリゲーションモードです。

アグリゲートインタフェースを削除するとアグリゲートグループも削除されます。同時にアグリゲーショングループのメンバポートがアグリゲーショングループから除外されます。

例

アグリゲートインタフェース Bridge-Aggregation 1 を作成し、aggregate interface view に移行します。

<AC> system-view

[AC] interface bridge-aggregation 1

[AC-Bridge-Aggregation1]

2.1.8 link-aggregation global load-sharing mode

Syntax

link-aggregation global load-sharing mode { **destination-ip** | **destination-mac** | **source-ip** | **source-mac** } *

undo link-aggregation global load-sharing mode

デフォルト

アグリゲーショングループは、宛先 IP アドレスに基づいてトラフィックを分散します。

View

System view

定義済みユーザロール

network-admin

パラメータ

destination-ip: 宛先 IP アドレスに基づいてトラフィックを分散します。

destination-mac: 宛先 MAC アドレスに基づいてトラフィックを分散します。

source-ip: 送信元 IP アドレスに基づいてトラフィックを分散します。

source-mac: 送信元 MAC アドレスに基づいてトラフィックを分散します。

説明

link-aggregation global load-sharing mode コマンドはグローバルのリンクアグリゲーションのロードシェアリングのモードを設定します。

undo link-aggregation global load-sharing mode コマンドはデフォルトに戻します。

設定したロードシェアリングのモードは前のロードシェアリングのモードに上書きされます。

コマンドを複数回実行した場合、最後に行った設定が適用されます。

サポートされていないリンクアグリゲーションのロードシェアリングモードが設定された場合、エラーが発生します。

例

宛先 MAC アドレスをもとにしてグローバルのリンクアグリゲーショングループのロードシェアリングのモードを設定します。

<AC> system-view

[AC] link-aggregation global load-sharing mode destination-mac

2.1.9 link-aggregation load-sharing mode

Syntax

link-aggregation load-sharing mode { **destination-ip** | **destination-mac** | **source-ip** | **source-mac** } *

undo link-aggregation load-sharing mode

デフォルト

ロードシェアリングモードはグローバルのロードシェアリングモードと同一です。

View

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

destination-ip: 宛先 IP アドレスをもとにしてリンクアグリゲーショングループのロードシェアリングを実行します。

destination-mac: 宛先 MAC アドレスをもとにしてリンクアグリゲーショングループのロードシェアリングを実行します。

source-ip: 送信元 IP アドレスをもとにしてリンクアグリゲーショングループのロードシェアリングを実行します。

source-mac: 送信元 MAC アドレスをもとにしてリンクアグリゲーショングループのロードシェアリングを実行します。

説明

link-aggregation load-sharing mode コマンドはリンクアグリゲーションのロードシェアリングのモードを設定します。

undo link-aggregation load-sharing mode コマンドはデフォルトに戻します。

設定したロードシェアリングのモードは前のロードシェアリングのモードに上書きされます。

サポートされていないリンクアグリゲーションのロードシェアリングモードが設定された場合、エラーが発生します。

例

宛先 MAC アドレスをもとにしてアグリゲートインタフェース Bridge-Aggregation 1 のリンクアグリゲーショングループのロードシェアリングのモードを設定します。

<AC> system-view

[AC] interface bridge-aggregation 1

[AC-Bridge-Aggregation1] link-aggregation load-sharing mode destination-mac

関連コマンド

link-aggregation global load-sharing mode

2.1.10 link-aggregation selected-port maximum

Syntax

link-aggregation selected-port maximum *number*

undo link-aggregation selected-port maximum

デフォルト

8

View

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

number: アグリゲーショングループで使用できる Selected ポートの最大数を設定します。範囲は 1～8 です。

説明

link-aggregation selected-port maximum コマンドはアグリゲーショングループで使用できる Selected ポートの最大数を設定します。

undo link-aggregation selected-port maximum コマンドはデフォルトに戻します。

このコマンドを実行すると、アグリゲーショングループのいくつかの Selected ポートは Unselected ポートになる可能性があります。

アグリゲーショングループで使用できる Selected ポートの最大数は、ローカルとピアエンドで同一にする必要があります。

アグリゲーショングループで使用できる Selected ポートの最大数は、以下の値の小さい方に制限されます。

- **link-aggregation selected-port maximum** コマンドで設定された最大数
- ハードウェアの制限

以下の処理を実行することによって 2 つのポート間でバックアップを設定することができます。

- アグリゲーショングループに 2 つのポートを割り当てます。
- アグリゲーショングループで使用できる Selected ポートの最大数を 1 に設定します。

そして、アグリゲーショングループの Selected ポートはすべてのポイントで使用できますが、Unselected ポートはバックアップポートとして動作します。

例

アグリゲートインタフェース Bridge-Aggregation 1 に対応するアグリゲーショングループで使用できる Selected ポートの最大数を 5 に設定します。

<AC> system-view

[AC] interface bridge-aggregation 1

[AC-Bridge-Aggregation1] link-aggregation selected-port maximum 5

関連コマンド

link-aggregation selected-port minimum

2.1.11 link-aggregation selected-port minimum

Syntax

link-aggregation selected-port minimum *number*

undo link-aggregation selected-port minimum

デフォルト

1

View

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

number: アグリゲートインタフェースを UP にするのに必要なアグリゲーショングループで使用できる Selected ポートの最小数を設定します。最小数は 1 で固定です。

説明

link-aggregation selected-port minimum コマンドはアグリゲーショングループで使用できる Selected ポートの最小数を設定します。

undo link-aggregation selected-port minimum コマンドはデフォルトに戻します。

このコマンドを実行すると、アグリゲーショングループのすべてのメンバポートは Unselected ポートになる可能性があります。

アグリゲーショングループで使用できる Selected ポートの最小数は、ローカルとピアエンドで同一にする必要があります。

例

アグリゲートインタフェース Bridge-Aggregation 1 に対応するアグリゲーショングループで使用できる Selected ポートの最小数を 3 に設定します。

<AC> system-view

[AC] interface bridge-aggregation 1

[AC-Bridge-Aggregation1] link-aggregation selected-port minimum 3

関連コマンド

link-aggregation selected-port maximum

2.1.12 port link-aggregation group

Syntax

port link-aggregation group *number*

undo port link-aggregation group

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

number: アグリゲーショングループに対応するアグリゲートインタフェースの数を指定します。値の範囲は 1～4 です。

説明

port link-aggregation group コマンドは指定したアグリゲーショングループにインタフェースを割り当てます。

undo port link-aggregation group コマンドは所属しているアグリゲーショングループからインタフェースを削除します。

インタフェースは 1 つのアグリゲーショングループのみ所属することができます。

例

アグリゲーショングループ 1 に GigabitEthernet 1/0/1 を割り当てます。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] port link-aggregation group 1

2.1.13 reset counters interface

Syntax

reset counters interface [**bridge-aggregation** [*interface-number*]]

View

User view

定義済みユーザロール

network-admin

パラメータ

bridge-aggregation: アグリゲートインタフェースを指定します。

interface-number: アグリゲートインタフェース番号を指定します。

説明

reset counters interface コマンドは指定されたアグリゲートインタフェースの統計情報を削除します。

一定期間、トラフィックの統計情報を収集する場合、以前に収集された統計情報の履歴を削除し、このコマンドを使用します。

パラメータを指定しない場合、システムのすべてのインタフェースの統計情報を削除します。

bridge-aggregation パラメータのみを使用する場合、すべてのレイヤ 2 のアグリゲートインタフェースの統計情報を削除します。

bridge-aggregation *interface-number* パラメータを指定した場合、指定したレイヤ 2 のアグリゲートインタフェースの統計情報を削除します。

bridge-aggregation パラメータは装置でレイヤ 2 のアグリゲートインタフェースが存在するときのみ有効です。

例

アグリゲートインタフェース Bridge-Aggregation 1 の統計情報を削除します。

<AC> reset counters interface bridge-aggregation 1

2.1.14 shutdown

Syntax

shutdown

undo shutdown

View

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

shutdown コマンドはアグリゲートインタフェースをシャットダウンします。

undo shutdown コマンドはアグリゲートインタフェースを up にします。

例

アグリゲートインタフェース Bridge-Aggregation 1 を up にします。

<AC> system-view

[AC] interface bridge-aggregation 1

[AC-Bridge-Aggregation1] undo shutdown

目次

このセクションのページは **4-x-x** です。

3 章 VLAN 3-1
3.1 VLAN 設定コマンド 3-1
3.1.1 description 3-1
3.1.2 display interface vlan-interface 3-3
3.1.3 display vlan 3-6
3.1.4 display vlan brief 3-8
3.1.5 interface vlan-interface 3-9
3.1.6 name 3-10
3.1.7 reset counters interface vlan-interface 3-11
3.1.8 shutdown 3-12
3.1.9 vlan 3-13
3.2 ポートベース VLAN 設定コマンド 3-14
3.2.1 display port 3-14
3.2.2 port 3-15
3.2.3 port access vlan 3-16
3.2.4 port hybrid pvid 3-17
3.2.5 port hybrid vlan 3-18
3.2.6 port link-type 3-19
3.2.7 port trunk permit vlan 3-20
3.2.8 port trunk pvid 3-21

3章 VLAN

3.1 VLAN設定コマンド

3.1.1 description

Syntax

description *text*

undo description

デフォルト

VLAN の説明は VLAN *vlan-id* です。*vlan-id* は VLAN の ID です。たとえば、VLAN 100 の VLAN の説明は VLAN 0100 です。

VLAN インタフェースの説明はインタフェースの名前です。たとえば Vlan-interface1 Interface です。

View

VLAN view

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

text: VLAN あるいは VLAN インタフェースの説明を指定します。設定範囲は 1～255 です。文字列には、大文字と小文字を区別する文字、数字、特殊記号（表 3-1 を参照）、スペース、その他の Unicode 文字と記号を含めることができます。

表 3-1 特殊記号

名前	記号
チルダ	~
エクスクラメーションマーク	!
アットマーク	@
シャープ	#
ダラーマーク	$
パーセント	%
キャロット	^
アンパサンド	&
アスタリスク	*

名前	記号
左波括弧	{
右波括弧	}
左丸括弧	(
右丸括弧	)
左角括弧	[
右角括弧	]
左アングルブラケット	<
右アングルブラケット	>
ハイフン	-
アンダーライン	_
＋マーク	+
イコールマーク	=
バーティカルバー	|
バックスラッシュ	¥
コロン	:
セミコロン	;
ダブルクォーテーション	"
アポストロフィー	'
コンマ	,
ドット	.
スラッシュ	/

説明

description コマンドは VLAN あるいは VLAN インタフェースの説明を指定します。

undo description コマンドはデフォルトに戻します。

VLAN あるいは VLAN インタフェースの機能あるいは説明を設定することができます。

装置で多くの VLAN あるいは VLAN インタフェースを識別するのに役立ちます。

例

VLAN 2 の説明を sales-private に設定します。

<AC> system-view

[AC] vlan 2

[AC-vlan2] description sales-private

VLAN インタフェース 2 の説明を linktoPC56 に設定します。

<AC> system-view

[AC] vlan 2

[AC-vlan2] quit

[AC] interface vlan-interface 2

[AC-Vlan-interface2] description linktoPC56

関連コマンド

- **display interface vlan-interface**
- **display vlan**

3.1.2 display interface vlan-interface

Syntax

display interface vlan-interface [*interface-number*] [**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan-interface *interface-number*: VLAN インタフェース番号を指定します。指定しない場合、すべての VLAN インタフェースの情報を表示します。

brief: インタフェースの概要情報を表示します。指定しない場合、VLAN インタフェースの詳細情報を表示します。

description: 完全なインタフェースの説明を表示します。指定しない場合、説明の最初の 27 文字のみを表示します。

down: down 状態の VLAN インタフェース、原因を表示します。指定しない場合、すべての状態の VLAN インタフェースの情報を表示します。

説明

display interface vlan-interface コマンドは VLAN インタフェースの情報を表示します。

例

VLAN インタフェース 2 の情報を表示します。

<AC> display interface vlan-interface 2

```
Vlan-interface2
Current state: DOWN
Line protocol state: DOWN
Description: Vlan-interface2 Interface
Bandwidth: 100000kbps
```

```
Maximum transmission unit: 1500
Internet protocol processing : Disabled
IP packet frame type: PKTFMT_ETHNT_2, hardware address: 000f-e249-8050
IPv6 packet frame type: PKTFMT_ETHNT_2, hardware address: 000f-e249-8050
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

VLAN インタフェース 2 の概要情報を表示します。

<AC> display interface vlan-interface 2 brief

```
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP       Description
Vlan2                DOWN DOWN     --
```

表 3-2 コマンド出力

フィールド	説明
Vlan-interface2	VLANインタフェース名です。
Current state	VLANインタフェースの物理状態です。 • **DOWN (Administratively)**–**shutdown**コマンドでVLANインタフェースがシャットダウンしています。インタフェースは運用上においてdownしています。 • **DOWN**–**shutdown**コマンドでVLANインタフェースがシャットダウンしていませんが、物理的にdownしています。VLANインタフェースのVLANはup状態の物理ポートがありません。ポートが物理的に接続されていない、あるいはリンクに失敗している可能性があります。 • **UP**–VLANインタフェースが運用上も物理的にも起動している状態です。
Line protocol state	VLANインタフェースのプロトコルリンクレイヤの状態です。 • **DOWN**–VLANインタフェースがプロトコルリンクレイヤでdownしています。 • **UP**–VLANインタフェースがプロトコルリンクレイヤでupしています。
Description	VLANインタフェースの一部または全部の説明です。 • **display interface brief**コマンドで**description**キーワードを指定しない場合、このフィールドにはインタフェースの

フィールド	説明
	説明の最初の27文字が表示されます。 ● **display interface brief**コマンドで**description**キーワードを指定した場合、このフィールドには完全なインタフェースの説明が表示されます。
Bandwidth	VLANインタフェースの予期された帯域幅です。
Maximum Transmission Unit	VLANインタフェースのMTUです。
Internet protocol processing : Disabled	VLANインタフェースにIPアドレスが設定されておらず、IPパケットの処理できません。
Internet address	VLANインタフェースのIPアドレスです。**primary**はIPアドレスがプライマリIPアドレスであることを示します。
IP packet frame type	IPv4の送信フレームタイプです。
hardware address	VLANインタフェースに対応するMACアドレスです。
IPv6 packet frame type	IPv6の送信フレームタイプです。
Last clearing of counters	インタフェースで**reset counters interface**コマンドを最後に使用した時間です。 **Never**は装置が起動してから**reset counters interface**コマンドを一度も使用していないことを示します。
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	過去300秒以内の平均送受信トラフィックです。単位はバイト/秒、bps、ppsです。
Input: 0 packets, 0 bytes, 0 drops	インタフェースで受信されたパケットの総数、パケットサイズと廃棄されたパケット数です。パケットサイズの単位はバイトです。
Output: 0 packets, 0 bytes, 0 drops	インタフェースで送信されたパケットの総数、パケットサイズと廃棄されたパケット数です。パケットサイズの単位はバイトです。
Brief information on interfaces in route mode	レイヤ3インタフェースの概要情報です。
Link: ADM - administratively down; Stby – standby	インタフェースのリンクレイヤの状態です。 ● **ADM**–リンクが運用上でシャットダウンしています。物理状態を回復するために、**undo shutdown**コマンドを実行します。 ● **Stby**–インタフェースがバックアップインタフェースとして動作します。プライマリインタフェースを表示する

フィールド	説明
	場合、**display interface-backup state**コマンドを使用します。
Protocol: (s) - spoofing	インタフェースのプロトコル属性に、次の条件が存在する場合フラグ（s）が含まれます。 ● インタフェースのデータリンクレイヤプロトコル状態は、**UP**として示されている。 ● リンクはオンデマンドリンクであるか存在しません。
Interface	省略したインタフェース名です。
Link	インタフェースの物理リンク状態です。 ● **UP**–リンクがupです。 ● **DOWN**–リンクが物理的にdownしています。 ● **ADM**–リンクが運用上でシャットダウンしています。物理状態を回復するために、**undo shutdown**コマンドを実行します。 ● **Stby**–インタフェースがバックアップインタフェースとして動作します。
Protocol	インタフェースのリンクレイヤの状態です。 ● **UP**－インタフェースのリンクがupです。 ● **DOWN**－インタフェースのリンクがdownです。 ● **UP(s)**–インタフェースのリンクがオンデマンドリンクあるいは準備ができていない状態です。ここで（**s**）はスプーフィングのフラグを示します。
Primary IP	インタフェースのプライマリIPアドレスです。

関連コマンド

reset counters interface vlan-interface

3.1.3 display vlan

Syntax

display vlan [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **static**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan-id1: VLAN ID で指定された VLAN の情報を表示します。設定範囲は 1～4094 です。

vlan-id1 **to** *vlan-id2*: VLAN ID の範囲を指定します。*vlan-id1* と *vlan-id2* の設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* よりも大きい値にする必要があります。

all: 作成されたすべての VLAN の情報を表示します。

dynamic: ダイナミック VLAN の番号と各ダイナミック VLAN の ID を表示します。ダイナミック VLAN は RADIUS サーバによって作成されます。

static: スタティック VLAN 番号と各スタティック VLAN の ID を表示します。スタティック VLAN は手動で作成されます。

説明

display vlan コマンドは VLAN 情報を表示します。

例

VLAN 2 の情報を表示します。

<AC> display vlan 2

```
VLAN ID: 2
VLAN type: Static
Route interface: Not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged ports:  None
Untagged ports:
  GigabitEthernet1/0/1  GigabitEthernet1/0/2  GigabitEthernet1/0/3
```

VLAN 3 の情報を表示します。

<AC> display vlan 3

```
VLAN ID: 3
VLAN type: static
Route interface: Configured
IPv4 address: 1.1.1.1
IPv4 subnet mask: 255.255.255.0
Description: VLAN 0003
Name: VLAN 0003
Tagged ports:  None
Untagged ports: None
```

表 3-3 コマンド出力

フィールド	説明
VLAN type	VLANタイプです。スタティックあるいはダイナミックがあります。
Route interface	VLANインタフェースが設定されているかどうかを示します。 ● **Not configured**－設定されていません。 ● **Configured**－設定されています。
Description	VLANの説明です。
Name	VLANに設定された名前です。
IP address	VLANインタフェースのプライマリIPv4アドレスです。このフィールドはVLANインタフェースにIPv4アドレスが設定されている場合のみ表示されます。セカンダリIPアドレスが存在する場合、以下のいずれかの方法で表示することができます。 ● **display interface vlan-interface**コマンドを使用します。 ● VLAN interface viewで**display this**コマンドを使用します。
Subnet mask	プライマリIPアドレスのサブネットマスクです。このフィールドはVLANインタフェースにIPアドレスが設定されている場合のみ表示されます。
Tagged ports	タグ付きVLANパケットを通すポートです。
Untagged ports	タグなしVLANパケットを通すポートです。

関連コマンド

vlan

3.1.4 display vlan brief

Syntax

display vlan brief

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display vlan brief コマンドは VLAN の概要情報を表示します。

例

VLAN の概要情報を表示します。

<AC> display vlan brief

```
Brief information about all VLANs:
Supported Minimum VLAN ID: 1
Supported Maximum VLAN ID: 4094
Default VLAN ID: 1
VLAN ID   Name                          Port
1         VLAN 0001                     GE1/0/1  GE1/0/2  GE1/0/3  GE1/0/4
                                        GE1/0/5  GE1/0/6
2         VLAN 0002
3         VLAN 0003
```

表 3-4 コマンド出力

フィールド	説明
Default VLAN ID	システムのデフォルトVLAN IDです。
Name	VLAN名です。
Port	VLANを通してパケットを許可するポートです。

3.1.5 interface vlan-interface

Syntax

interface vlan-interface *interface-number*

undo interface vlan-interface *interface-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-number: VLAN インタフェース番号を指定します。設定範囲は 1～4094 です。

サポートされる VLAN インタフェースの最大数は 48 です。

説明

interface vlan-interface コマンドは VLAN インタフェースを作成し、作成された VLAN インタフェースの view に移行あるいは既存の VLAN インタフェースの view に移行します。

undo interface vlan-interface コマンドは VLAN インタフェースを削除します。

VLAN インタフェースを作成する前に、VLAN を作成してください。

例

VLAN インタフェース 2 を作成し、作成された VLAN インタフェースの view に移行します。

<AC> system-view

[AC] vlan 2

[AC-vlan2] quit

[AC] interface vlan-interface 2

[AC-Vlan-interface2]

関連コマンド

display interface vlan-interface

3.1.6 name

Syntax

name *text*

undo name

デフォルト

デフォルトの VLAN 名は VLAN *vlan-id* です。*vlan-id* は 4 桁の VLAN の ID です。ID が 4 桁よりも少ない場合、先頭に 0 が追加されます。たとえば、VLAN 100 の VLAN 名は VLAN 0100 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

text: VLAN 名を指定します。設定範囲は 1～32 です。文字列には、大文字と小文字を区別する文字、数字、特殊記号（表 3-1 を参照してください。）、スペース、その他の Unicode 文字と記号を含めることができます。

説明

name コマンドは VLAN の名前を設定します。

undo name コマンドは VLAN の名前をデフォルトに戻します。

装置に 802.1X または MAC アドレス認証の設定が行われる場合、VLAN ID または VLAN 名を使用して許可 VLAN を指定することができます。VLAN の数が非常に多い場合、識別するために VLAN 名を使用します。

例

VLAN 2 の名前を test vlan として設定します。

<AC> system-view

[AC] vlan 2

[AC-vlan2] name test vlan

関連コマンド

display vlan

3.1.7 reset counters interface vlan-interface

Syntax

reset counters interface vlan-interface [*interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

vlan-interface *interface-number*: VLAN インタフェース番号を指定します。

説明

reset counters interface vlan-interface コマンドは VLAN インタフェースの統計情報を削除します。

一定期間、トラフィックの統計情報を収集する場合、以前に収集された統計情報の履歴を削除し、このコマンドを使用します。

interface-number 引数を指定しない場合、このコマンドはすべての VLAN インタフェースの統計情報を削除します。

interface-number 引数を指定すると、このコマンドは指定された VLAN インタフェースの統計情報を削除します。

例

VLAN インタフェース 2 の統計情報を削除します。

<AC> reset counters interface vlan-interface 2

関連コマンド

display interface vlan-interface

3.1.8 shutdown

Syntax

shutdown

undo shutdown

デフォルト

VLAN インタフェースは手動でシャットダウンしていません。以下のガイドラインが適用されます。

- VLAN のすべてのポートが down している場合、VLAN インタフェースは down になります。
- 1 つ以上の VLAN が up である場合、VLAN インタフェースは up になります。

View

VLAN interface view

定義済みユーザロール

network-admin

説明

shutdown コマンドは VLAN インタフェースをシャットダウンします。

undo shutdown コマンドは VLAN インタフェースを up にします。

コマンドを使用した場合、VLAN インタフェースは DOWN（Administratively）状態のままになります。この場合、VLAN インタフェースの状態は VLAN のポートの状態に影響しません。

VLAN インタフェースのパラメータを設定する前に、ネットワークへの影響から設定を防ぐため、**shutdown** コマンドで VLAN インタフェースをシャットダウンしてください。

VLAN インタフェースのパラメータを設定した後、設定を適用するため、**undo shutdown** コマンドを使用してください。

故障した VLAN インタフェースのトラブルシューティングを行うため、**shutdown** コマンドを使用してください。インタフェースが回復したかどうかを確認するため、**undo shutdown** コマンドを使用してください。

VLAN 内のすべての Ethernet ポートの状態は、VLAN インタフェースの状態とは無関係です。

例

VLAN インタフェース 2 をシャットダウンし、up にします。

<AC> system-view

[AC] interface vlan-interface 2

[AC-Vlan-interface2] shutdown

[AC-Vlan-interface2] undo shutdown

3.1.9 vlan

Syntax

vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

undo vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

デフォルト

VLAN 1（システムデフォルト VLAN）

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan-id1, vlan-id2: VLAN ID を指定します。設定範囲は 1～4094 です。

vlan-id1 **to** *vlan-id2*: VLAN の範囲を指定します。*vlan-id1* と *vlan-id2* は VLAN ID を指定します。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: VLAN 1～4094 を指定します。

説明

vlan *vlan-id* コマンドは VLAN を作成し、その view あるいは既存の VLAN の view に移行します。

vlan *vlan-id1* **to** *vlan-id2* コマンドは *vlan-id1* から *vlan-id2* の VLAN を作成します。

vlan all コマンドは VLAN 1～VLAN 4094 を作成します。

undo vlan コマンドは指定された VLAN を削除します。

システムデフォルト VLAN（VLAN 1）を作成あるいは削除することはできません。

ダイナミック VLAN、アプリケーションによって固定された VLAN を削除するため、**undo vlan** コマンドを使用することはできません。これらの VLAN を削除するため、最初に VLAN から設定を削除してください。

例

VLAN 2 を作成し、その view に移行します。

<AC> system-view

[AC] vlan 2

[AC-vlan2]

VLAN 4～VLAN 100 を作成します。

<AC> system-view

[AC] vlan 4 to 100

関連コマンド

display vlan

3.2 ポートベースVLAN設定コマンド

3.2.1 display port

Syntax

display port { **hybrid** | **trunk** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

hybrid: ハイブリッドポートを指定します。

trunk: トランクポートを指定します。

説明

display port コマンドはハイブリッドポートあるいはトランクポートに関する情報を表示します。

例

ハイブリッドポートの情報を表示します。

<AC> display port hybrid

```
Interface           PVID  VLAN Passing
GE1/0/4             100   Tagged:  1000, 1002, 1500, 1600-1611, 2000,
                                2555-2558, 3000, 4000
                          Untagged:1, 10, 15, 18, 20-30, 44, 55, 67, 100,
                                150-160, 200, 255, 286, 300-302
```

トランクポートの情報を表示します。

<AC> display port trunk

```
Interface           PVID  VLAN Passing
GE1/0/6             2     1-4, 6-100, 145, 177, 189-200, 244, 289, 400,
                          555, 600-611, 1000, 2006-2008
```

表 3-5 コマンド出力

フィールド	説明
Interface	ポート名です。
PVID	ポートのVLAN IDです。
VLAN Passing	ポートで許可されたVLANです。
Tagged	VLANタグを削除しないでポートがパケットを送信するVLANです。
Untagged	VLANタグを削除した後、ポートがパケットを送信するVLANです。

3.2.2 port

Syntax

port *interface-list*

undo port *interface-list*

デフォルト

VLAN 1

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

interface-list: インタフェースを指定します。半角スペースで区切り 10 まで設定するか、インタフェースの範囲で設定することができます。インタフェースを範囲で指定する形式は *interface-type interface-number1* [**to** *interface-type interface-number2*]です。*interface-number2* は *interface-number1* 以上の値にしてください。

説明

port コマンドは指定したアクセスポートに VLAN を割り当てます。

undo port コマンドは VLAN から指定したアクセスポートを削除します。

このコマンドはアクセスポートのみ適用可能です。

デフォルトですべてのポートはアクセスポートです。ポートタイプを **port link-type** コマンドで設定することができます。

例

GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 に VLAN 2 を割り当てます。

<AC> system-view

[AC] vlan 2

[AC-vlan2] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3

関連コマンド

display vlan

3.2.3 port access vlan

Syntax

port access vlan *vlan-id*

undo port access vlan

デフォルト

すべての VLAN は VLAN1 に所属しています。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を指定します。設定範囲は 1～4094 です。

説明

port access vlan コマンドはアクセスポートを指定した VLAN に割り当てます。

undo port access vlan コマンドはデフォルトに戻します。

アクセスポートを VLAN に割り当てる前に、VLAN が作成されていることを確認してください。

例

GigabitEthernet 1/0/1 に VLAN 3 を割り当てます。

<AC> system-view

[AC] vlan 3

[AC-vlan3] quit

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] port access vlan 3

3.2.4 port hybrid pvid

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

デフォルト

リンクタイプがアクセスであるとき、ハイブリッドポートの PVID はポートが所属している VLAN の ID です。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を指定します。設定範囲は 1～4094 です。

説明

port hybrid pvid コマンドはハイブリッドポートの PVID を設定します。

undo port hybrid pvid コマンドはハイブリッドポートの PVID を 1 に設定します。

ハイブリッドポートの PVID として存在しない VLAN を使用することができます。**undo vlan** コマンドでハイブリッドポートの PVID を削除する場合、ポートの PVID の設定は適用されません。

ローカルとリモートのハイブリッドポートに同じ PVID を設定することを推奨します。

PVID からのパケットの転送を許可するためにハイブリッドポートの設定に **port hybrid pvid** コマンドを使用してください。

例

ハイブリッドポートの GigabitEthernet 1/0/1 の PVID を VLAN 100 に設定し、GigabitEthernet 1/0/1 に VLAN 100 をタグなしメンバとして割り当てます。

<AC> system-view

[AC] vlan 100

[AC-vlan100] quit

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] port link-type hybrid

[AC-GigabitEthernet1/0/1] port hybrid pvid vlan 100

[AC-GigabitEthernet1/0/1] port hybrid vlan 100 untagged

関連コマンド

- **port hybrid vlan**
- **port link-type**

3.2.5 port hybrid vlan

Syntax

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

デフォルト

リンクタイプがアクセスであるとき、ハイブリッドポートはポートが所属している VLAN のタグなしメンバです。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN ID の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* **to** *vlan-id2* です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

tagged: ポートは VLAN タグを削除しないで指定した VLAN のパケットを送信するように設定します。

untagged: ポートは VLAN タグを削除したのち、指定した VLAN のパケットを送信するように設定します。

説明

port hybrid vlan コマンドは指定した VLAN にハイブリッドポートを割り当てます。

undo port hybrid vlan コマンドは指定した VLAN からハイブリッドポートを削除します。

ハイブリッドポートは、複数の VLAN が通過できます。**port hybrid vlan** コマンドを繰り返し実行すると、ハイブリッドポートを通過する VLAN は、各実行の *vlan-id-list* により指定された VLAN に設定されます。

例

GigabitEthernet 1/0/1 をハイブリッドポートに設定します。VLAN 2、VLAN 4 および VLAN 50～VLAN 100 に割り当て、これらの VLAN のパケットにタグを付けて送信するよう GigabitEthernet 1/0/1 に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] port link-type hybrid

[AC-GigabitEthernet1/0/1] port hybrid vlan 2 4 50 to 100 tagged

関連コマンド

port link-type

3.2.6 port link-type

Syntax

port link-type { **access** | **hybrid** | **trunk** }

undo port link-type

デフォルト

access

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

access: ポートのリンクタイプをアクセスとして指定します。

hybrid: ポートのリンクタイプをハイブリッドとして指定します。

trunk: ポートのリンクタイプをトランクとして指定します。

説明

port link-type コマンドはポートのリンクタイプを設定します。

undo port link-type コマンドはデフォルトに戻します。

トランクポートからハイブリッドポート（またはその逆）のリンクタイプを変更するには、まずリンクタイプをアクセスに設定する必要があります。

例

GigabitEthernet 1/0/1 のリンクタイプをトランクポートに設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] port link-type trunk

3.2.7 port trunk permit vlan

Syntax

port trunk permit vlan { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

デフォルト

トランクポートは VLAN 1 からのパケットのみ通過できるように許可します。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: インタフェースを指定します。半角スペースで区切り 10 まで設定するか、VLAN ID の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* **to** *vlan-id2* です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: すべての VLAN を通過できるように許可します。許可されていない VLAN ユーザがポートを通して制限されたリソースにアクセスすることを防ぐため、注意して **port trunk permit vlan all** コマンドを使用してください。

説明

port trunk permit vlan コマンドはトランクポートを指定した VLAN に割り当てます。

undo port trunk permit vlan コマンドはトランクポートを指定した VLAN から削除します。

トランクポートは複数の VLAN を通過できます。**port trunk permit vlan** コマンドを繰り返し実行すると、トランクポートを通過する VLAN は、各 *vlan-id-list* により指定された VLAN に設定されます。

トランクポート上では、PVID のトラフィックのみタグなしで通過することができます。

例

GigabitEthernet 1/0/1 をトランクポートに設定します。VLAN 2、VLAN 4 および VLAN 50～VLAN 100 に割り当てます。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] port link-type trunk

[AC-GigabitEthernet1/0/1] port trunk permit vlan 2 4 50 to 100

関連コマンド

port link-type

3.2.8 port trunk pvid

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

デフォルト

VLAN 1

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を指定します。設定範囲は 1～4094 です。

説明

port trunk pvid コマンドはトランクポートの PVID を設定します。

undo port trunk pvid コマンドはデフォルトに戻します。

トランクポートの PVID として存在しない VLAN を使用することができます。**undo vlan** コマンドを使用してトランクポートの PVID を削除しても、ポートの PVID の設定には影響しません。

ローカルおよびリモートのトランクポートは、PVID のトラフィックが正常に送信されるために同じ PVID を使用する必要があります。

PVID からのパケットの転送を許可するためにトランクポートの設定に **port trunk permit vlan** コマンドを使用してください。

例

GigabitEthernet 1/0/1 をトランクポートに設定します。PVID を VLAN 100 に設定し、GigabitEthernet 1/0/1 に VLAN 100 を割り当てます。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] port link-type trunk

[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100

[AC-GigabitEthernet1/0/1] port trunk permit vlan 100

関連コマンド

- **port link-type**
- **port trunk permit vlan**

目次

このセクションのページは **4-x-x** です。

4 章 STP 4-1
4.1 STP 設定コマンド 4-1
4.1.1 active region-configuration 4-1
4.1.2 check region-configuration 4-2
4.1.3 display stp 4-3
4.1.4 display stp abnormal-port 4-12
4.1.5 display stp bpdu-statistics 4-13
4.1.6 display stp down-port 4-16
4.1.7 display stp history 4-17
4.1.8 display stp region-configuration 4-19
4.1.9 display stp root 4-20
4.1.10 display stp tc 4-21
4.1.11 instance 4-23
4.1.12 region-name 4-24
4.1.13 reset stp 4-25
4.1.14 revision-level 4-26
4.1.15 snmp-agent trap enable stp 4-27
4.1.16 stp bpdu-protection 4-28
4.1.17 stp bridge-diameter 4-28
4.1.18 stp compliance 4-30
4.1.19 stp config-digest-snooping 4-31
4.1.20 stp cost 4-32
4.1.21 stp edged-port 4-33
4.1.22 stp enable 4-34
4.1.23 stp global config-digest-snooping 4-35
4.1.24 stp global enable 4-36
4.1.25 stp global mcheck 4-37
4.1.26 stp loop-protection 4-38
4.1.27 stp max-hops 4-39
4.1.28 stp mcheck 4-40
4.1.29 stp mode 4-41
4.1.30 stp no-agreement-check 4-42
4.1.31 stp pathcost-standard 4-43
4.1.32 stp point-to-point 4-44
4.1.33 stp port priority 4-45
4.1.34 stp port-log 4-47

4.1.35 stp priority 4-48
4.1.36 stp pvst-bpdu-protection 4-49
4.1.37 stp region-configuration 4-50
4.1.38 stp role-restriction 4-50
4.1.39 stp root primary 4-51
4.1.40 stp root secondary 4-52
4.1.41 stp root-protection 4-54
4.1.42 stp tc-protection 4-55
4.1.43 stp tc-protection threshold 4-55
4.1.44 stp timer forward-delay 4-56
4.1.45 stp timer hello 4-57
4.1.46 stp timer max-age 4-59
4.1.47 stp timer-factor 4-60
4.1.48 stp transmit-limit 4-61
4.1.49 stp vlan enable 4-62
4.1.50 vlan-mapping modulo 4-63

4章 STP

4.1 STP設定コマンド

4.1.1 active region-configuration

Syntax

active region-configuration

View

MST region view

定義済みユーザロール

network-admin

説明

active region-configuration コマンドは MST(multiple spanning tree)リージョン設定をアクティブにします。

MST リージョンパラメータを設定するとき、MSTP は新しいスパニングツリーの計算プロセスを行います。スパニングツリーの計算プロセスが実行されるとネットワークが不安定になります。VLAN-インスタンスマッピングテーブルを設定するときに、よく発生します。このため **active region-configuration** コマンドあるいは **stp global enable** コマンドを実行したのち、MSTP を有効にします。

このコマンドを実行する前に、**check region-configuration** コマンドを使用して MST のリージョンの設定が正しいことを確認してください。MST のリージョンの設定が正しいことが確認できたら、このコマンドを実行してください。

例

MSTI 1 に VLAN 2 をマッピングし、MST リージョンの設定を有効にします。

<AC> system-view

[AC] stp region-configuration

[AC-mst-region] instance 1 vlan 2

[AC-mst-region] active region-configuration

関連コマンド

- **check region-configuration**
- **instance**
- **region-name**
- **revision-level**

- **stp global enable**
- **vlan-mapping modulo**

4.1.2 check region-configuration

Syntax

check region-configuration

View

MST region view

定義済みユーザロール

network-admin

説明

check region-configuration コマンドはリージョン名、リビジョンレベル、VLAN-インスタンスマッピング設定などの、まだアクティブにされていない MST リージョンの設定の情報を表示します。

スパニングツリーの装置は物理リンクを通して接続され、以下の設定が同一であるときのみ、同じ MST リージョンに属します。

- フォーマットセレクタ（デフォルトは 0 で設定できません。）
- MST リージョン名
- MST リージョンリビジョンレベル
- MST リージョンの VLAN-インスタンスマッピングエントリ

MST リージョンの設定をアクティブにする前に、MST のリージョン設定が正しいかどうかをチェックするために、このコマンドを使うことを推奨します。結果が正しいときのみ、MST リージョン設定をアクティブにしてください。

例

MST リージョンのまだアクティブにされていない設定の情報を表示します。

<AC> system-view

[AC] stp region-configuration

[AC-mst-region] check region-configuration

```
Admin Configuration
  Format selector      : 0
  Region name          : 001122334400
  Revision level       : 0
  Configuration digest : 0x3ab68794d602fdf43b21c0b37ac3bca8

  Instance  VLANs Mapped
```

```
0        1, 3 to 4094
15       2
```

表 4-1 コマンド出力

フィールド	説明
Format selector	フォーマットセレクタです。値は0です（設定はできません）
Region name	MST リージョン名です。
Revision level	MSTリージョンのリビジョンレベルです。
Instance VLANs Mapped	MSTリージョンのVLAN-インスタンスマッピングエントリです。

関連コマンド

- **active region-configuration**
- **instance**
- **region-name**
- **revision-level**
- **vlan-mapping modulo**

4.1.3 display stp

Syntax

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] [**interface** *interface-list* | **slot** *slot-number*] [**brief**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

interface *interface-list*: インタフェースを指定します。半角スペースで区切り 10 まで設定するか、インタフェースの範囲で設定することができます。インタフェースを範囲で指定する形式は *interface-type interface-number 1* [**to** *interface-type interface-number 2*]です。*interface-number 2* は *interface-number 1* 以上の値にしてください。

brief: スパニングツリーの状態と統計情報の概要を表示します。指定しない場合、詳細なスパニングツリーの状態と統計情報を表示します。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのすべてのメンバ装置に適用されます。

説明

display stp コマンドはスパニングツリーの状態と統計情報を表示します。スパニングツリーの状態および統計情報にもとづいて、ネットワークトポロジの分析および維持、あるいはスパニングツリーが正常に動作しているか確認することができます。

STP あるいは RSTP モード：コマンド出力はポート名の順番で表示されます。

- ポートを指定しない場合、すべてのポートに適用されます。
- ポートリストを指定した場合、指定したポートに適用されます。

PVST モード：コマンド出力はそれぞれの VLAN の VLAN ID とポート名の順番で表示されます。

- VLAN あるいはポートを指定しない場合、すべての VLAN のすべてのポートに適用されます。
- VLAN を指定し、ポートを指定しない場合、すべての VLAN の指定したポートに適用されます。
- VLAN およびポートリストを指定した場合、指定した VLAN のポートに適用されます。

MSTP モード：コマンド出力はそれぞれの MSTI の MSTI ID とポート名の順番で表示されます。

- MSTI あるいはポートを指定しない場合、すべてのポートの MSTI に適用されます。
- MSTI を指定し、ポートを指定しない場合、指定した MSTI のすべてのポートに適用されます。
- MSTI およびポートリストを指定した場合、指定した MSTI の指定ポートに適用されます。

ネットワークの収束中、最新のスパニングツリーの情報は表示されません。

例

MSTP モードで、MSTI0 の GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 のスパニングツリーの状態と概要情報を表示します。

<AC> display stp instance 0 interface gigabitethernet 1/0/1 to gigabitethernet 1/0/4 brief

```
MST ID     Port                           Role  STP State     Protection
0          GigabitEthernet1/0/1           ALTE  DISCARDING    LOOP
0          GigabitEthernet1/0/2           DESI  FORWARDING    NONE
0          GigabitEthernet1/0/3           DESI  FORWARDING    NONE
0          GigabitEthernet1/0/4           DESI  FORWARDING    NONE
```

PVST モードで、VLAN2 の GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 のスパニングツリーの状態と概要情報を表示します。

<AC> system-view

[AC] stp mode pvst

[AC] display stp vlan 2 interface gigabitethernet 1/0/1 to gigabitethernet 1/0/4 brief

```
VLAN ID    Port                           Role  STP State     Protection
2          GigabitEthernet1/0/1           ALTE  DISCARDING    LOOP
2          GigabitEthernet1/0/2           DESI  FORWARDING    NONE
2          GigabitEthernet1/0/3           DESI  FORWARDING    NONE
2          GigabitEthernet1/0/4           DESI  FORWARDING    NONE
```

表 4-2 コマンド出力

フィールド	説明
MST ID	MSTリージョンのMSTI IDです。
Port	各MSTIあるいはVLANに対応するポート名です。
Role	ポートの役割です。 • **ALTE**—代理ポートです。 • **BACK**—バックアップポートポートです。 • **ROOT**—ルートポートです。 • **DESI**—Designatedポートです。 • **MAST**—マスタポートです。 • **DISA**—ポートが無効です。
STP State	ポートのスパニングツリーの状態です。 • **FORWARDING**—ポートはBPDUを送受信し、ユーザトラフィックを転送します。 • **DISCARDING**—ポートはBPDUを送受信できますが、ユーザトラフィックを転送できません。 • **LEARNING**—ポートは過渡状態です。ポートはBPDUを送受信できますが、ユーザトラフィックを転送できません。
Protection	ポートの保護タイプです。 • **ROOT**—Rootガードです。

フィールド	説明
	• **LOOP**—Loopガードです。 • **BPDU**—BPDUガードです。 • **NONE**—保護していません。

#MSTP モードで、すべてのポートのすべての MSTI のスパニングツリーの状態と詳細情報を表示します。

<AC> display stp

```
-------[CIST Global Info][Mode MSTP]-------
 Bridge ID          : 32768.0440-A900-0000
 Bridge times       : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
 Root ID/ERPC       : 32768.0440-A900-0000, 0
 RegRoot ID/IRPC    : 32768.0440-A900-0000, 0
 RootPort ID        : 0.0
 BPDU-Protection    : Disabled
 Bridge Config-
 Digest-Snooping    : Disabled
 TC or TCN received  : 2
 Time since last TC  : 0 days 0h:0m:58s

----[Port3(GigabitEthernet1/0/2)][FORWARDING]----
 Port protocol      : Enabled
 Port role          : Designated Port (Boundary)
 Port ID           : 128.3
 Port cost(Legacy)   : Config=auto, Active=200
 Desg.bridge/port    : 32768.0440-A900-0000, 128.3
 Port edged         : Config=disabled, Active=disabled
 Point-to-Point     : Config=auto, Active=true
 Transmit limit     : 10 packets/hello-time
 TC-Restriction     : Disabled
 Role-Restriction    : Disabled
 Protection type     : Config=none, Active=none
 MST BPDU format     : Config=auto, Active=802.1s
 Port Config-
 Digest-Snooping    : Disabled
 Rapid transition    : True
 Num of VLANs mapped : 0
 Port times         : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 0s RemHops 20
 BPDU sent          : 32
        TCN: 0, Config: 0, RST: 0, MST: 32
 BPDU received      : 2
```

```
        TCN: 0, Config: 0, RST: 0, MST: 2

-------[MSTI 1 Global Info]-------
 Bridge ID          : 32768.0440-A900-0000
 RegRoot ID/IRPC    : 32768.0440-A900-0000, 0
 RootPort ID        : 0.0
 Master bridge      : 32768.0440-A900-0000
 Cost to master     : 0
 TC received        : 0

----[Port3(GigabitEthernet1/0/2)][FORWARDING]----
 Port protocol      : Enabled
 Port role          : Designated Port (Boundary)
 Port ID            : 128.3
 Port cost(Legacy)  : Config=auto, Active=200
 Desg.bridge/port   : 32768.0440-A900-0000, 128.3
 Protection type    : Config=none, Active=none
 Rapid transition   : True
 Num of VLANs mapped : 64
 Port times         : RemHops 20
```

PVST モードで、すべての VLAN のすべてのポートのスパニングツリーの状態と詳細情報を表示します。

<AC> system-view

[AC] stp mode pvst

[AC] display stp

```
-------[VLAN 1 Global Info]-------
Protocol status    : Enabled
Bridge ID          : 32768.0440-A900-0000
Bridge times       : Hello 2s MaxAge 20s FwdDelay 15s
VlanRoot ID/RPC    : 0.0440-A900-0000, 200200
RootPort ID        : 128.48
BPDU-Protection    : Disabled
TC or TCN received  : 2
Time since last TC  : 0 days 0h:5m:42s

 ----[Port1(Ethernet1/0/1)][FORWARDING]----
 Port protocol      : Enabled
 Port role          : Designated Port
 Port ID            : 128.153
 Port cost(Legacy)  : Config=auto, Active=200
 Desg. bridge/port  : 32768.0440-A900-0000, 128.2
 Port edged         : Config=disabled, Active=disabled
```

```
 Point-to-Point     : Config=auto, Active=true
 Transmit limit     : 10 packets/hello-time
 Protection type    : Config=none, Active=none
 Rapid transition   : False
 Port times         : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 2s

-------[VLAN 2 Global Info]-------
Protocol status     : Enabled
Bridge ID          : 32768.0440-A900-0000
Bridge times        : Hello 2s MaxAge 20s FwDly 15s
VlanRoot ID/RPC     : 0.0440-A900-0000, 200200
RootPort ID         : 128.48
BPDU-Protection     : Disabled
TC or TCN received  : 2
Time since last TC  : 0 days 0h:5m:42s
```

MSTP モードで、スパニングツリー機能が無効であるときのスパニングツリーの状態と詳細情報を表示します。スパニングツリー機能がグローバルで有効でない場合、**STP is not configured** と表示されます。

<AC> display stp

```
 Protocol status   : Disabled
 Protocol Std.     : IEEE 802.1s
 Version          : 3
 Bridge-Prio.  : 32768
 MAC address       : 0440-A900-0000
 Max age(s)        : 20
 Forward delay(s)  : 15
 Hello time(s)     : 2
 Max hops          : 20
 TC Snooping       : Disabled
```

#PVST モードで、スパニングツリー機能が無効であるときのスパニングツリーの状態と詳細情報を表示します。

<AC> display stp

```
 Protocol status   : Disabled
 Protocol Std.     : IEEE 802.1w (pvst)
 Version          : 2
 Bridge-Prio.      : 32768
 MAC address       : 0440-A900-0000
 Max age(s)        : 20
 Forward delay(s)  : 15
 Hello time(s)     : 2
 TC Snooping       : Disabled
```

表 4-3 コマンド出力

フィールド	説明
Bridge ID	ブリッジのIDです。装置のプライオリティとMACアドレスを含みます。たとえば32768.000f-e200-2200において、ピリオド（．）の前の値は装置のプライオリティを示し、ピリオド（．）の後の値は装置のMACアドレスを示します。
Bridge times	ブリッジの主要パラメータです。 • **Hello**—Hello時間です。 • **MaxAge**—最大エージング時間です。 • **FwdDelay**—転送遅延時間です。 • **MaxHops**—MSTリージョンの最大ホップ数です。
Root ID/ERPC	CISTルートIDと外部パスコストです。（装置からCISTルートまでのパスコストです）
RegRoot ID/IRPC	CISTリージョナルルートIDと内部パスコストです。（装置からCISTリージョナルルートまでのパスコストです）
VlanRoot ID/RPC	VLANルートIDと内部パスコストです。（装置からVLANルートブリッジまでのパスコストです）
RootPort ID	ルートポートIDです。0.0は装置がルートでルートポートがないことを示します。
BPDU-Protection	BPDU保護のグローバル状態を示します。
Bridge Config-Digest-Snooping	Digest Snoopingのグローバル状態を示します。
TC or TCN received	MSTIあるいはVLANで受信されたTC/TCNパケット数です。
Time since last TC	MSTIあるいはVLANで最後にトポロジが変更されてからの経過時間です。
[FORWARDING]	ポートがforwarding状態です。
[DISCARDING]	ポートが廃棄状態です。
[LEARNING]	ポートがlearning状態です。
Port protocol	ポートのスパニングツリーの状態です。
Port role	ポートの役割です。 • **Alternate**—代理ポートです。 • **Backup**—バックアップポートポートです。 • **Root**—ルートポートです。 • **Designated**—Designatedポートです。 • **Master**—マスタポートです。 • **Disabled**—ポートが無効です。

フィールド	説明
(Boundary)	ポートが境界ポートです。
Port cost(Legacy)	ポートのパスコストです。括弧の中身はポートパスコストの計算で使用される標準(**legacy**、**dot1d-1998**、あるいは **dot1t**)を示します。 ● **Config**－設定値です。 ● **Active**－実際の値です。
Desg.bridge/port	ポートのDesignated ブリッジIDとポートIDです。 表示されたポートIDは、ポートプライオリティをサポートしないポートであるため、重要ではありません。
Port edged	edgeポートあるいは非edgeポートです。 ● **Config**－設定値です。 ● **Active**－実際の値です。
Point-to-Point	ポートがポイントツーポイントで接続されているかどうかを示します。 ● **Config**－設定値です。 ● **Active**－実際の値です。
Transmit limit	各Hello時間以内に送信されたBPDU数です。
Protection type	ポートの保護タイプです。 ● **ROOT**—Rootガードです。 ● **LOOP**—Loopガードです。 ● **BPDU**—BPDUガードです。 ● **NONE**—保護していません。
TC-Restriction	ポートのTC転送の制限の状態です。 TC-Restrictionはサポートしていません。
Role-Restriction	ポートのポート役割の制限の状態です。
MST BPDU format	ポートが送信可能なMST BPDUの形式です。 ● **Config**－設定値（legacyあるいは802.1s準拠）です。 ● **Active**－実際の値（legacyあるいは802.1s準拠）です。
Port Config-Digest-Snooping	ポートのDigest Snoopingの状態です。
Rapid transition	MSTIあるいはVLANでポートの転送状態が高速状態遷移であるかどうかを示します。
Num of VLANs mapped	MSTIにマッピングされたVLAN数です。
Port times	ポートの主要パラメータです。 ● **Hello**—Hello時間です。 ● **MaxAge**—最大エージング時間です。

フィールド	説明
	• **FwdDelay**—転送遅延時間です。 • **MsgAge**—メッセージのエージング時間 • **RemHops**—残りのホップ数です。
BPDU sent	送信BPDUの統計情報です。
BPDU received	受信BPDUの統計情報です。
RegRoot ID/IRPC	MSTIリージョナルルートと内部パスのコストです。
Root Type	MSTIルートタイプです。 • プライマリルートです。 • セカンダリルートです。
Master bridge	MSTIルートブリッジIDです。
Cost to master	MSTIからマスタブリッジへのパスコストです。
TC received	受信TC BPDUの数です。
Protocol status	スパニングツリープロトコルの状態です。
Protocol Std.	スパニングツリープロトコルが標準です。
Version	スパニングツリープロトコルのバージョンです。
Bridge-Prio.	• MSTPモードで、CISTの装置のプライオリティです。 • PVSTモードで、VLAN1の装置のプライオリティです。
Max age(s)	BPDUのエージング時間です。（単位は秒です。PVSTモードのVLAN1のエージング時間と同一です）
Forward delay(s)	ポートの状態遷移遅延です。（単位は秒です。PVSTモードのVLAN1の状態遷移遅延と同一です）
Hello time(s)	BPDUを送信するルートブリッジの送信間隔です。（単位は秒です。PVSTモードのVLAN1の送信間隔と同一です）
Max hops	MSTIの最大ホップ数です。
TC Snooping	TC snoopingの状態です。 • 有効 • 無効

関連コマンド

reset stp

4.1.4 display stp abnormal-port

Syntax

display stp abnormal-port

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display stp abnormal-port コマンドは、STP 保護処理によってブロックされたポートに関する情報を表示します。

例

Version 7.2.11 を含む以降のソフトウェア：

MSTI モードで STP 保護処理によってブロックされたポートに関する情報を表示します。

<AC> display stp abnormal-port

```
MST ID     Blocked Port              Reason
 1         GigabitEthernet1/0/1       Root-Protected
 2         GigabitEthernet1/0/2       Loop-Protected
 12        GigabitEthernet1/0/3       Loopback-Protected
```

PVST モードで STP 保護処理によってブロックされたポートに関する情報を表示します。

<AC> system-view

[AC] stp mode pvst

[AC] display stp abnormal-port

```
VLAN ID     Blocked Port              Reason
 1          GigabitEthernet1/0/1       Root-Protected
 2          GigabitEthernet1/0/2       Loop-Protected
 2          GigabitEthernet1/0/3       Loopback-Protected
```

表 4-4 コマンド出力

フィールド	説明
MST ID	ブロックされたポートのMSTIです。
VLAN ID	ブロックされたポートのVLANです。

フィールド	説明
Blocked Port	ブロックされたポートの名前です。
Reason	ポートがブロックされた理由です。 • **Root-Protected**—Rootガード機能です。 • **Loop-Protected**—Loopガード機能です。 • **Loopback-Protected**—自己ループの保護です。MSTIのポートが送信したBPDUを受信しました。 • **Disputed**—Disputeの保護です。ポートは非ブロックのDesignatedポートから低いプライオリティのBPDUを受信しました。 • **InconsistentPortType-Protected**—ポートタイプ不一致保護です。 • **InconsistentPvid-Protected**—PVID不一致保護です。

4.1.5 display stp bpdu-statistics

Syntax

display stp bpdu-statistics [**interface** *interface-type interface-number* [**instance** *instance-list*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

説明

display stp bpdu-statistics コマンドはポートの BPDU 統計情報を表示します。

MSTP モード：コマンド出力はポート名と MSTI ID の順番で表示されます。

- MSTI あるいはポートを指定しない場合、すべてのポートのすべての MSTI に適用されます。
- ポートを指定し、MSTI を指定しない場合、ポートのすべての MSTI に適用されます。
- MSTI およびポートを指定した場合、指定したポートの指定した MSTI に適用されます。

STP、RSTP あるいは PVST モード：コマンド出力はポート名の順番で表示されます。

- ポートを指定しない場合、すべてのポートに適用されます。
- ポート名を指定した場合、ポートに適用されます。

例

MSTP モードで GigabitEthernet 1/0/1 のすべての MSTI の BPDU 統計情報を表示します。

<AC> display stp bpdu-statistics interface gigabitethernet 1/0/1

```
Port: GigabitEthernet1/0/1

Instance-Independent:

Type                     Count     Last Updated
------------------------- ---------- -----------------
Invalid BPDUs             0
Looped-back BPDUs         0
Max-aged BPDUs            0
TCN sent                  0
TCN received              0
TCA sent                  0
TCA received              2         10:33:12 01/13/2011
Config sent               0
Config received           0
RST sent                  0
RST received              0
MST sent                  4         10:33:11 01/13/2011
MST received              151       10:37:43 01/13/2011

Instance 0:
Type                     Count     Last Updated
------------------------- ---------- -----------------
Timeout BPDUs             0
Max-hoped BPDUs           0
TC detected               1         10:32:40 01/13/2011
TC sent                   3         10:33:11 01/13/2011
TC received               0
```

PVST モードで GigabitEthernet 1/0/1 の BPDU 統計情報を表示します。

<AC> system-view

[AC] stp mode pvst

[AC] display stp bpdu-statistics interface gigabitethernet 1/0/1

```
Port: GigabitEthernet1/0/1

Type                     Count     Last Updated
-------------------------- ---------- -----------------
Invalid BPDUs             0
Looped-back BPDUs         0
Max-aged BPDUs            0
TCN sent                  0
TCN received              0
TCA sent                  0
TCA received              2          10:33:12 01/13/2010
Config sent               0
Config received           0
RST sent                  0
RST received              0
MST sent                  4          10:33:11 01/13/2010
MST received              151        10:37:43 01/13/2010
Timeout BPDUs             0
Max-hoped BPDUs           0
TC detected               511        10:32:40 01/13/2010
TC sent                   8844       10:33:11 01/13/2010
TC received               1426       10:33:32 01/13/2010
```

表 4-5 コマンド出力

フィールド	説明
Port	ポート名です。
Instance-Independent	特定のMSTIに関係ない統計情報です。
Type	統計項目です。
Looped-back BPDUs	BPDUを送信したのち、同一ポートで受信したBPDUです。
Max-aged BPDUs	最大エージングを超過したBPDUです。
TCN sent	TCN BPDUの送信数です。
TCN received	TCN BPDUの受信数です。
TCA sent	TCA BPDUsの送信数です。

フィールド	説明
TCA received	TCA BPDUの受信数です。
Config sent	Configuration BPDUの送信数です。
Config received	Configuration BPDUの受信数です。
RST sent	Configuration BPDUの送信数です。
RST received	RSTP BPDUの受信数です。
MST sent	RSTP BPDUの受信数です。
MST received	MSTP BPDUの送信数です。
Instance	特定のMSTIの統計情報です。
Timeout BPDUs	タイムアウトしたBPDUです。
Max-hoped BPDUs	最大ホップ数が超過したBPDUです。
TC detected	TC BPDUの検出数です。
TC sent	TC BPDUの送信数です。
TC received	TC BPDUの受信数です。

4.1.6 display stp down-port

Syntax

display stp down-port

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display stp down-port コマンドは STP 保護機能によってシャットダウンされたポートに関する情報を表示します。

例

STP 保護機能によってシャットダウンされたポートに関する情報を表示します。

<AC> display stp down-port

```
Down Port                      Reason
GigabitEthernet1/0/1           BPDU-Protected
```

表 4-6 コマンド出力

フィールド	説明
Down Port	STP保護機能によってシャットダウンされたポート名です。
Reason	ポートがシャットダウンされた理由です。**BPDU-Protected**はBPDUガード機能を示します。

4.1.7 display stp history

Syntax

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **history** [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのすべてのメンバ装置に適用されます。

説明

display stp history コマンドはポートのロール計算の履歴情報を表示します。

STP あるいは RSTP モードではポートのロール計算の時間の順番で表示されます。

PVST モード：コマンド出力は VLAN ID と各 VLAN のポートのロール計算の時間の順番で表示されます。

- VLAN を指定しない場合、すべての VLAN に適用されます。
- VLAN リストを指定した場合、指定した VLAN に適用されます。

MSTP モード：コマンド出力は MSTI ID と各 MSTI のポートのロール計算の時間の順番で表示されます。

- MSTI を指定しない場合、すべての MSTI に適用されます。
- MSTI リストを指定した場合、指定した MSTI に適用されます。

例

MSTP モードで、MSTI 2 の IRF スタックメンバ装置 1 のポートのロール計算の履歴情報を表示します。

<AC> display stp instance 2 history slot 1

```
 -------------- STP slot 1 history trace ---------------
 ------------------  Instance 2   ---------------------
Port GigabitEthernet1/0/1
  Role change        : ROOT->DESI (Aged)
  Time               : 2009/02/08 00:22:56
  Port priority      : 0.0440-A900-0000 0 0.0440-A900-0000 128.1
  Designated priority : 0.0440-A900-0000 0 0.0440-A900-0000 128.1
 Port GigabitEthernet1/0/2
  Role change        : ALTER->ROOT
  Time               : 2009/02/08 00:22:56
  Port priority      : 0.0440-A900-0000 0 0.0440-A900-0000 128.2
                     128.153
  Designated priority : 0.0440-A900-0000 0 0.0440-A900-0000 128.2
                     128.153
```

PVST モードで、VLAN 2 の IRF スタックメンバ装置 1 のポートのロール計算の履歴情報を表示します。

<AC> display stp vlan 2 history slot 1

```
 -------------- STP slot 1 history trace ---------------
 ------------------  VLAN 2   ---------------------
 Port GigabitEthernet1/0/1
  Role change        : ROOT->DESI (Aged)
  Time               : 2009/02/08 00:22:56
  Port priority      : 0.0440-A900-0000 0 0.0440-A900-0000 128.1
  Designated priority : 0.0440-A900-0000 0 0.0440-A900-0000 128.1
 Port GigabitEthernet1/0/2
  Role change        : ALTER->ROOT
  Time               : 2009/02/08 00:22:56
```

```
Port priority      : 0.0440-A900-0000 0 0.0440-A900-0000 128.2
Designated priority : 0.0440-A900-0000 0 0.0440-A900-0000 128.2
```

表 4-7 コマンド出力

フィールド	説明
Port	ポート名です。
Role change	ポートの役割変更です。（**Aged**は設定BPDUのタイムアウトによって変更が起きたことを示します）
Time	ポートのロール計算の時間です。

4.1.8 display stp region-configuration

Syntax

display stp region-configuration

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display stp region-configuration コマンドは有効な MST リージョンの設定情報を表示します。以下の情報があります。

- リージョン名
- リビジョンレベル
- ユーザ定義の VLAN-インスタンスマッピング

例

MSTP モードで有効な MST リージョンの設定情報を表示します。

<AC> display stp region-configuration

```
Oper Configuration
  Format selector     : 0
  Region name         : hello
  Revision level      : 0
  Configuration digest : 0x5f762d9a46311effb7a488a3267fca9f

  Instance   VLANs Mapped
```

```
0         21 to 4094
1         1 to 10
2         11 to 20
```

表 4-8 コマンド出力

フィールド	説明
Format selector	スパニングツリープロトコルで定義されたフォーマットセレクタです。デフォルト値は0です。セレクタは設定できません。
Region name	MSTリージョン名です。
Revision level	MSTリージョンのリビジョンレベルです。**revision-level**コマンドを使って設定できます。デフォルトは0です。
VLANs Mapped	MSTIにマッピングされたVLANです。

関連コマンド

- **instance**
- **region-name**
- **revision-level**
- **vlan-mapping modulo**

4.1.9 display stp root

Syntax

display stp root

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display stp root コマンドはスパニングツリーのルートブリッジ情報を表示します。

例

MSTP モードですべてのスパニングツリーのルートブリッジ情報を表示します。

<AC> display stp root

```
MST ID  Root Bridge ID       ExtPathCost IntPathCost Root Port
0       0.0440-A900-0000     200200      0           GigabitEthernet1/0/1
```

PVST モードですべてのスパニングツリーのルートブリッジ情報を表示します。

<AC> display stp root

```
VLAN ID  Root Bridge ID       ExtPathCost IntPathCost Root Port
1        0.0440-A900-0000     200200      0           GigabitEthernet1/0/1
```

表 4-9 コマンド出力

フィールド	説明
ExtPathCost	外部パスコストです。装置は自動的にポートのデフォルトパスコストを計算します。あるいはポートのパスコストを設定するために**stp cost** コマンドを使用することができます。
IntPathCost	内部パスコストです。装置は自動的にポートのデフォルトパスコストを計算します。あるいはポートのパスコストを設定するために**stp cost** コマンドを使用することができます。
Root Port	ルートポート名です。（装置のポートがMSTIのルートポートである場合のみ表示されます）

4.1.10 display stp tc

Syntax

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **tc** [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

slot *slot-number*: IRF スタックメンバ装置を指定します。*slot-number* は IRF スタックメンバ装置の ID を示します。指定しない場合、IRF スタックユニットのすべてのメンバ装置に適用されます。

説明

display stp tc コマンドはポートで送受信する TC/TCN BPDU の統計情報を表示します。

STP あるいは RSTP モードでは、出力はポート名の順番で表示されます。

PVST モード：コマンド出力は VLAN ID と各 VLAN のポート名の順番で表示されます。

- VLAN を指定しない場合、すべての VLAN に適用されます。
- VLAN リストを指定した場合、指定した VLAN に適用されます。

MSTP モード：コマンド出力は MSTI ID と各 MSTI のポート名の順番で表示されます。

- MSTI を指定しない場合、すべての MSTI に適用されます。
- MSTI リストを指定した場合、指定した MSTI に適用されます。

例

MSTP モードで MSTI 0 の IRF スタックメンバ装置 1 のすべてのポートで送受信する TC/TCN BPDU の統計情報を表示します。

<AC> display stp instance 0 tc slot 1

```
-------------- STP slot 1 TC or TCN count -------------
MST ID     Port                          Receive     Send
0          GigabitEthernet1/0/1             6          4
0          GigabitEthernet1/0/2             0          2
```

PVST モードで VLAN 2 の IRF スタックメンバ装置 1 のすべてのポートで送受信する TC/TCN BPDU の統計情報を表示します。

<AC> display stp vlan 2 tc slot 1

```
-------------- STP slot 1 TC or TCN count -------------
VLAN ID    Port                           Receive     Send
2          GigabitEthernet1/0/1             6          4
2          GigabitEthernet1/0/2             0          2
```

表 4-10 コマンド出力

フィールド	説明
Port	ポート名です。
Receive	各ポートが受信したTC/TCN BPDUの数です。
Send	各ポートが送信したTC/TCN BPDUの数です。

4.1.11 instance

Syntax

instance *instance-id* **vlan** *vlan-id-list*

undo instance *instance-id* [**vlan** *vlan-id-list*]

デフォルト

CIST

View

MST region view

定義済みユーザロール

network-admin

パラメータ

instance-list: MSTI ID を指定します。設定範囲は 0～4094 です。0 は CIST を示します。コマンドの設定範囲は 1～4094 です。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

説明

⚠ **注意:**

以下の状況下でグローバル Digest Snooping を使用する場合、注意してください。
- VLAN-インスタンスマッピングを修正します。
- デフォルトの MST リージョンの設定に戻します。

もしローカル装置が隣接装置と異なる VLAN-インスタンスマッピングを持っている場合、ループあるいはトラフィックの中断が発生します。

instance コマンドは VLAN のリストを MSTI にマッピングします。

undo instance コマンドは指定した VLAN あるいはすべての VLAN を CIST（MSTI 0）に再マッピングします。

undo instance コマンドで VLAN を指定しない場合、指定された MSTI にマッピングされたすべての VLAN は CIST に再マッピングされます。

同一の VLAN を異なる MSTI にマッピングすることはできません。インスタンスにマッピングされている VLAN を新たなインスタンスにマッピングすると、古いマッピングは自動的に削除されます。

VLAN-インスタンスマッピングを最大 65 の MSTI にマッピングすることができます。

このコマンドを設定した後、VLAN-インスタンスマッピングをアクティブにするため、**active region-configuration** コマンドを実行します。

例

VLAN 2 を MSTI 1 にマッピングします。

<AC> system-view

[AC] stp region-configuration

[AC-mst-region] instance 1 vlan 2

関連コマンド

- **active region-configuration**
- **check region-configuration**
- **display stp region-configuration**

4.1.12 region-name

Syntax

region-name *name*

undo region-name

デフォルト

装置の MST リージョン名は MAC アドレスです。

View

MST region view

定義済みユーザロール

network-admin

パラメータ

name: MST リージョン名を指定します。設定範囲は 1～32 です。

説明

region-name コマンドは MST リージョン名を設定します。

undo region-name コマンドはデフォルトに戻します。

装置の MST リージョンは、装置の MST リージョン名、VLAN-インスタンスマッピングテーブルおよび MSTP リビジョンレベルによって決まります。

このコマンドを設定した後、MST リージョン名をアクティブにするため、**active region-configuration** コマンドを実行します。

例

装置の MST リージョン名を hello に設定します。

<AC> system-view

[AC] stp region-configuration

[AC-mst-region] region-name hello

関連コマンド

- **active region-configuration**
- **check region-configuration**
- **display stp region-configuration**
- **instance**
- **revision-level**
- **vlan-mapping modulo**

4.1.13 reset stp

Syntax

reset stp [**interface** *interface-list*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-list*: インタフェースを指定します。半角スペースで区切り 10 まで設定するか、インタフェースの範囲で設定することができます。インタフェースを範囲で指定する形式は *interface-type interface-number 1* [**to** *interface-type interface-number 2*]です。*interface-number 2* は *interface-number 1* 以上の値にしてください。指定しない場合すべてのポートのスパニングツリーに関する統計情報を削除します。

説明

reset stp コマンドはスパニングツリーの統計情報を削除します。スパニングツリーの統計情報は、TCN BPDU の数、configuration BPDU、RST BPDU、および指定したポートで送受信された MST BPDU が含まれます。

例

GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 のスパニングツリーの統計情報を削除します。

<AC> reset stp interface gigabitethernet 1/0/1 to gigabitethernet 1/0/3

関連コマンド

display stp

4.1.14 revision-level

Syntax

revision-level *level*

undo revision-level

デフォルト

0

View

MST region view

定義済みユーザロール

network-admin

パラメータ

level: MSTP リビジョンレベルを指定します。設定範囲は 0～65535 です。

説明

revision-level コマンドは MSTP リビジョンレベルを設定します。

undo revision-level コマンドはデフォルトに戻します。

装置の MSTP リビジョンレベル、MST リージョン名、VLAN-インスタンスマッピングテーブルは、装置の MST リージョンによって決まります。

このコマンドを設定した後、MST リージョン名をアクティブにするため、**active region-configuration** コマンドを実行します。

例

MST リージョンの MSTP リビジョンレベルを 5 に設定します。

<AC> system-view

[AC] stp region-configuration

[AC-mst-region] revision-level 5

関連コマンド

- **active region-configuration**
- **check region-configuration**

- **display stp region-configuration**
- **instance**
- **region-name**
- **vlan-mapping modulo**

4.1.15 snmp-agent trap enable stp

Syntax

snmp-agent trap enable stp tc

undo snmp-agent trap enable stp tc

デフォルト

MSTP モードでは、SNMP notification は MSTI 0 で有効です。ほかの MSTI では無効です。

PVST モードでは無効です。

View

System view

定義済みユーザロール

network-admin

パラメータ

tc: 装置が TCN BPDU を受信した場合、SNMP notification の送信を有効にします。PVST モードでのみ有効です。

説明

snmp-agent trap enable stp コマンドはスパニングツリートポロジの変更に関する SNMP notification を有効にします。

undo snmp-agent trap enable stp コマンドはスパニングツリートポロジの変更に関する SNMP notification を無効にします。

例

スパニングツリートポロジの変更に関する SNMP notification を有効にします。

<AC> system-view

[AC] snmp-agent trap enable stp tc

4.1.16 stp bpdu-protection

Syntax

stp bpdu-protection

undo stp bpdu-protection

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

stp bpdu-protection コマンドは BPDU ガード機能を有効にします。

undo stp bpdu-protection コマンドは BPDU ガード機能を無効にします。

例

BPDU ガード機能を有効にします。

<AC> system-view

[AC] stp bpdu-protection

4.1.17 stp bridge-diameter

Syntax

stp [**vlan** *vlan-id-list*] **bridge-diameter** *diameter*

undo stp [**vlan** *vlan-id-list*] **bridge-diameter**

デフォルト

7

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。STP、RSTP、MSTP では使用しません。

diameter: スイッチネットワークのダイアメータを指定します。設定範囲は 2～7 です。

説明

stp bridge-diameter コマンドはスイッチネットワークのネットワークダイアメータを設定します。

undo stp bridge-diameter コマンドはデフォルトに戻します。

ネットワークダイアメータは、端末装置がルートブリッジを経由して、スイッチネットワーク上の別の端末装置に到達するためのステーションの最大数を示します。

Hello 時間、転送遅延、最大エージング時間を適切に設定するとネットワーク収束の速度を上げることができます。これらのタイマの値はネットワークサイズに関連しています。ネットワークダイアメータを設定することで、これら 3 つのタイマを間接的に設定することができます。ネットワークダイアメータが 7（デフォルト値）に設定されていると、3 つのタイマもデフォルトに設定されます。

STP、RSTP、MSTP モードでは、各 MST リージョンは装置と認識され、CIST（あるいは共通ルートブリッジ）のみ適用することができます。

PVST モードでは、指定した VLAN のルートブリッジのみ適用することができます。

例

MSTP モードでスイッチネットワークのネットワークダイアメータを 5 に設定します。

<AC> system-view

[AC] stp bridge-diameter 5

MSTP モードでスイッチネットワークの VLAN 2 のネットワークダイアメータを 5 に設定します。

<AC> system-view

[AC] stp vlan 2 bridge-diameter 5

関連コマンド

- **stp timer forward-delay**
- **stp timer hello**
- **stp timer max-age**

4.1.18 stp compliance

Syntax

stp compliance { **auto** | **dot1s** | **legacy** }

undo stp compliance

デフォルト

auto

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

auto: ポートが自動で MSTP BPDU フォーマットを認識し、それに従って送信する MSTP BPDU のフォーマットを決定するよう設定します。

dot1s: ポートが標準フォーマット（802.1s 準拠）の MSTP BPDU のみ送受信するよう設定します。

legacy: ポートが互換性のあるフォーマットの MSTP BPDU のみを送受信するよう設定します。

説明

stp compliance コマンドは指定したポートが MSTP BPDU の認識および送信に使用するモードを設定します。

undo stp compliance コマンドはデフォルトに戻します。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 が標準フォーマット（802.1s）の MSTP パケットのみを送信するよう設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] stp compliance dot1s

4.1.19 stp config-digest-snooping

Syntax

stp config-digest-snooping

undo stp config-digest-snooping

デフォルト

無効

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp config-digest-snooping コマンドは Digest Snooping を有効にします。

undo stp config-digest-snooping コマンドは Digest Snooping を無効にします。

この設定はグローバル、およびほかのベンダの装置に接続されたポートの両方で有効にする必要があります。影響を最小限にするため、グローバルで有効にする前に関連したポートの機能を有効にしてください。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

Digest Snooping を GigabitEthernet 1/0/1 とグローバルで有効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] stp config-digest-snooping

[AC-GigabitEthernet1/0/1] quit

[AC] stp global config-digest-snooping

関連コマンド

- **display stp**
- **stp global config-digest-snooping**

4.1.20 stp cost

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **cost** *cost*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **cost**

デフォルト

装置は各スパニングツリーのポートのパスコストを、対応する標準にもとづいて自動的に計算します。

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

cost: ポートのパスコストを指定します。設定範囲は、採用されているパスコスト計算基準によって決まります。

- パスコスト計算に IEEE 802.1d-1998 が選択されている場合、設定範囲は 1～65535 です。
- パスコスト計算に IEEE 802.1t が選択されている場合、設定囲は 1～200000000 です。
- パスコスト計算にプライベート標準が選択されている場合、コスト範囲は 1～200000 です。

説明

stp cost コマンドはポートのパスコストを設定します。

undo stp cost コマンドはデフォルトに戻します。

パスコストはスパニングツリー計算を行う際の重要な要素です。MSTI のポートに異なるパスコストを設定すると、VLAN トラフィックのフローが異なる物理的リンクを通って転送され、VLAN ベースのロードバランスを行うことができます

ポートのパスコストの設定はポートの役割に影響します。ポートの役割が変更されたとき、システムはポートの役割を計算し、状態遷移を開始します。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

MSTI あるいは VLAN を指定しない場合、このコマンドは MSTP CIST あるいは STP、RSTP スパニングツリーのポートのパスコストを設定します。

例

MSTP モードで MSTI 2 の GigabitEthernet 1/0/3 のパスコストを 200 に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/3

[AC-GigabitEthernet1/0/3] stp instance 2 cost 200

PVST モードで VLAN 2 の GigabitEthernet 1/0/3 のパスコストを 200 に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/3

[AC-GigabitEthernet1/0/3] stp vlan 2 cost 200

関連コマンド

- **display stp**
- **stp pathcost-standard**

4.1.21 stp edged-port

Syntax

stp edged-port

undo stp edged-port

デフォルト

すべてのポートは非エッジポートです。

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp edged-port コマンドはポートを Edge ポートに設定します。

undo stp edged-port コマンドはポートを非 Edge ポートに設定します。

ユーザ端末に直接接続しているポートは別の装置あるいは共有 LAN セグメントに接続されているポートよりも、Edge ポートとして設定されることができます。

ネットワークトポロジが変化した場合、Edge ポートは一時ループを起こしません。

ポートを Edge ポートとして設定すると、そのポートは早急に転送状態に遷移することができます。ユーザ端末に直接接続されているポートを Edge ポートとして設定することを推奨します。

通常、Edge ポートはほかの装置に接続されていないため、ほかの装置からの configuration BPDU は、Edge ポートには到達しません。BPDU ガード機能が無効であるとき、configuration BPDU を受信すると、Edge ポートとして設定されたポートは非 Edge ポートとして動作します。

ポートでループガード機能と Edge ポートの設定は同時に設定することはできません。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 を Edge ポートとして設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] stp edged-port

関連コマンド

- **stp bpdu-protection**
- **stp loop-protection**
- **stp root-protection**

4.1.22 stp enable

Syntax

stp enable

undo stp enable

デフォルト

有効

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp enable コマンドはスパニングツリー機能を有効にします。

undo stp enable コマンドはスパニングツリー機能を無効にします。

スパニングツリー機能を有効にしたとき、装置はスパニングツリーのモードの設定に従い STP、RSTP、PVST、MSTP モードで動作します。

スパニングツリー機能を有効にしたとき、装置は受信した configuration BPDU にもとづいて VLAN のスパニングツリーの状態を自動で維持します。

スパニングツリー機能を無効にしたとき、装置はスパニングツリーの状態の維持を停止します。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

MSTP モードで、GigabitEthernet 1/0/1 のスパニングツリー機能を無効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] undo stp enable

関連コマンド

- **stp global enable**
- **stp mode**
- **stp vlan enable**

4.1.23 stp global config-digest-snooping

Syntax

stp global config-digest-snooping

undo stp global config-digest-snooping

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

stp global config-digest-snooping コマンドはグローバルで Digest Snooping を有効にします。

undo stp global config-digest-snooping コマンドはグローバルで Digest Snooping を無効にします。

この設定はグローバル、およびほかのベンダの装置に接続されたポートの両方で有効にする必要があります。影響を最小限にするため、グローバルで有効にする前に関連したポートの機能を有効にしてください。

例

Digest Snooping を GigabitEthernet 1/0/1 とグローバルで有効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] stp config-digest-snooping

[AC-GigabitEthernet1/0/1] quit

[AC] stp global config-digest-snooping

関連コマンド

- **display stp**
- **stp config-digest-snooping**

4.1.24 stp global enable

Syntax

stp global enable

undo stp global enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

stp global enable コマンドはスパニングツリー機能をグローバルで有効にします。

undo stp global enable コマンドはスパニングツリー機能をグローバルで無効にします。

スパニングツリー機能を有効にしたとき、スパニングツリーのモードの設定により装置は STP、RSTP、PVST、MSTP モードで動作します。

スパニングツリー機能が有効であるとき、装置は受信した configuration BPDU にもとづいて VLAN のスパニングツリーの状態を維持します。スパニングツリー機能が無効であるとき、装置はスパニングツリーの状態の維持を停止します。

例

スパニングツリー機能をグローバルで有効にします。

<AC> system-view

[AC] stp global enable

関連コマンド

- **stp enable**
- **stp mode**

4.1.25 stp global mcheck

Syntax

stp global mcheck

View

System view

定義済みユーザロール

network-admin

説明

stp global mcheck コマンドはグローバルで mCheck を実行します。

MSTP、RSTP、PVST のポートが STP 装置に接続し、STP BPDU を受信すると、ポートは自動で STP モードに遷移します。しかし以下の状況ではポートは自動でもとのモードに戻ることができません。

- ピアの STP 装置がシャットダウンあるいは削除されたとき。
- ポートが変更を検出できないとき。

この場合、mCheck を実行して、ポートをもとのモードに強制的に移行させることができます。

スパニングツリーのモードの設定により装置は STP、RSTP、PVST、MSTP モードで動作します。

装置が MSTP、RSTP、PVST モードで動作しているときのみ **stp global mcheck** コマンドが適用されます。

例

グローバルで mCheck を実行します。

<AC> system-view

[AC] stp global mcheck

関連コマンド

- **stp mcheck**
- **stp mode**

4.1.26 stp loop-protection

Syntax

stp loop-protection

undo stp loop-protection

デフォルト

無効

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp loop-protection コマンドはポートのループガード機能を有効にします。

undo stp loop-protection コマンドはポートのループガード機能を無効にします。

ポートのループガード機能はルートガード機能あるいは Edge ポートの設定を同時に設定することはできません。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 のループガード機能を有効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] stp loop-protection

関連コマンド

- **stp edged-port**
- **stp root-protection**

4.1.27 stp max-hops

Syntax

stp max-hops *hops*

undo stp max-hops

デフォルト

20

View

System view

定義済みユーザロール

network-admin

パラメータ

hops: 最大ホップ数を設定します。設定範囲は 1～40 です。

説明

stp max-hops コマンドは MST リージョンの最大ホップ数を設定します。

undo stp max-hops コマンドはデフォルトに戻します。

例

MST リージョンの最大ホップ数を 35 に設定します。

<AC> system-view

[AC] stp max-hops 35

関連コマンド

display stp

4.1.28 stp mcheck

Syntax

stp mcheck

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp mcheck コマンドはポートで mCheck を実行します。

MSTP、RSTP、PVST のポートが STP 装置に接続し、STP BPDU を受信すると、ポートは自動で STP モードに遷移します。しかし以下の状況ではポートは自動でもとのモードに戻ることができません。

- ピアの STP 装置がシャットダウンあるいは削除されたとき。
- ポートが変更を検出できないとき。

この場合、mCheck オペレーションを実行して、ポートをもとのモードに強制的に移行させることができます。

たとえば、デバイス A、デバイス B、デバイス C が一列に接続されています。デバイス A は STP を動作し、デバイス B はスパニングツリープロトコルが動作しておらず、デバイス C は RSTP、MSTP あるいは PVST で動作します。デバイス C がデバイス B から透過的に転送された STP BPDU を受信すると、受信したポートは STP モードに遷移します。デバイス B をデバイス C と RSTP、MSTP、PVST で動作するように設定した場合、デバイス B とデバイス C に接続しているポートで mCheck を実行します。

スパニングツリーのモードの設定により装置は STP、RSTP、PVST、MSTP モードで動作します。

装置が MSTP、RSTP、PVST モードで動作しているときのみ **stp mcheck** コマンドが適用されます。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 で mCheck を実行します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] stp mcheck

関連コマンド

- **stp global mcheck**
- **stp mode**

4.1.29 stp mode

Syntax

stp mode { **mstp** | **pvst** | **rstp** | **stp** }

undo stp mode

デフォルト

mstp

View

System view

定義済みユーザロール

network-admin

パラメータ

mstp: MSTP モードで動作するように設定します。

pvst: PVST モードで動作するように設定します。

rstp: RSTP モードで動作するように設定します。

stp: STP モードで動作するように設定します。

説明

stp mode コマンドはスパニングツリーの動作モードを設定します。

undo stp mode コマンドはデフォルトに戻します。

MSTP モードは RSTP モードと互換性があります。RSTP モードは STP モードと互換性があります。

PVST モードの互換性はポートのリンクタイプに依存します。

- **アクセスポート**－PVST モードはすべての VLAN でほかのスパニングツリーと互換性があります。
- **トランクポートあるいはハイブリッドポート**－PVST モードは、VLAN1 でほかのスパニングツリーと互換性があります。

例

スパニングツリーの動作モードを STP に設定します。

<AC> system-view

[AC] stp mode stp

関連コマンド

- **stp enable**
- **stp global enable**
- **stp global mcheck**
- **stp mcheck**
- **stp vlan enable**

4.1.30 stp no-agreement-check

Syntax

stp no-agreement-check

undo stp no-agreement-check

デフォルト

無効

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp no-agreement-check コマンドはポートの No Agreement Check（高速切り替え）機能を有効にします。

undo stp no-agreement-check コマンドはポートの No Agreement Check（高速切り替え）機能を無効にします。

このコマンドはルートポートでのみ有効です。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 の No Agreement Check（高速切り替え）機能を有効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] stp no-agreement-check

4.1.31 stp pathcost-standard

Syntax

stp pathcost-standard { **dot1d-1998** | **dot1t** | **legacy** }

undo stp pathcost-standard

デフォルト

legacy

View

System view

定義済みユーザロール

network-admin

パラメータ

dot1d-1998: IEEE 802.1d-1998 規格にもとづいて、ポートのデフォルトパスコストを計算します。

dot1t: IEEE 802.1t 規格にもとづいて、ポートのデフォルトパスコストを計算します。

legacy: 独自の規格にもとづいて、ポートのデフォルトパスコストを計算します。

説明

stp pathcost-standard コマンドはポートのデフォルトパスコストを計算するときに使用する装置の規格を指定します。

undo stp pathcost-standard コマンドはデフォルトに戻します。

装置がデフォルトパスコストの計算に使用する規格を変更すると、ポートパスコストの値はデフォルトに戻ります

例

IEEE 802.1d-1998 規格にもとづいて、ポートのデフォルトパスコストを計算するように設定します。

<AC> system-view

[AC] stp pathcost-standard dot1d-1998

関連コマンド

- **display stp**
- **stp cost**

4.1.32 stp point-to-point

Syntax

stp point-to-point { **auto** | **force-false** | **force-true** }

undo stp point-to-point

デフォルト

デフォルトは auto で、スパニングツリーの装置は自動でポートがポイントツーポイントのリンクに接続するかどうか検出します。

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

auto: リンクタイプの自動検出を指定します。

force-false: 非ポイントツーポイントのリンクタイプを指定します。

force-true: ポイントツーポイントのリンクタイプを指定します。

説明

stp point-to-point コマンドはポートのリンクタイプを設定します。

undo stp point-to-point コマンドはデフォルトに戻します。

非ポイントツーポイントリンクに接続している場合、ポートは高速でステート遷移することはできません。

現在のポートがアグリゲートインタフェースあるいは full モードで動作しているポートである場合、ポートをポイントツーポイントリンクとしてリンクタイプを設定すること

ができます。装置が自動でリンク状態を検出するよう、デフォルト設定を使用することを推奨します。

MSTP モードで **stp point-to-point force-false** コマンドあるいは **stp point-to-point force-true** コマンドが設定されたポートはすべての MSTI あるいは VLAN で有効です。

ポートに接続している物理的リンクがポイントツーポイントリンクではないとき、強制的にポイントツーポイントリンクになるよう設定した場合、一時的なループが発生することがあります。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/3 をポイントツーポイントリンクとして接続するよう設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/3

[AC-GigabitEthernet1/0/3] stp point-to-point force-true

関連コマンド

display stp

4.1.33 stp port priority

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **port priority** *priority*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **port priority**

デフォルト

128

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

priority: ポートのプライオリティを指定します。設定範囲は 0～240 で、16 の倍数です。（0、16、32、・・・のように設定します）

説明

stp port priority コマンドはポートのプライオリティを設定します。ポートのプライオリティはスパニングツリーのポートの役割に影響します。

undo stp port priority コマンドはデフォルトに戻します。

priority を小さい値にするとポートのプライオリティが高くなります。装置上のすべてのプライオリティが同一である場合、プライオリティの値はポートインデックスに依存します。インデックスが小さいとプライオリティが高くなります。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

MSTI あるいは VLAN を指定しない場合、MSTP CIST、STP あるいは RSTP のポートのプライオリティを設定します。

例

MSTP モードで MSTI 2 の GigabitEthernet 1/0/3 のプライオリティを 16 に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/3

[AC-GigabitEthernet1/0/3] stp instance 2 port priority 16

PVST モードで VLAN 2 の GigabitEthernet 1/0/3 のプライオリティを 16 に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/3

[AC-GigabitEthernet1/0/3] stp vlan 2 port priority 16

関連コマンド

display stp

4.1.34 stp port-log

Syntax

stp port-log { **all** | **instance** *instance-list* | **vlan** *vlan-id-list* }

undo stp port-log { **all** | **instance** *instance-list* | **vlan** *vlan-id-list* }

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

all: すべての MSTI あるいは VLAN を指定します。

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

説明

stp port-log コマンドはポート状態の遷移情報の出力を有効にします。

undo stp port-log コマンドはポート状態の遷移情報の出力を有効にします。

例

MSTP モードで MSTI 2 のポート状態の遷移情報の出力を有効にします。

<AC> system-view

[AC] stp port-log instance 2

```
%Aug 16 00:49:41:856 2011 AC STP/3/STP_DISCARDING: Instance 2's port
GigabitEthernet1/0/1 has been set to discarding state.
%Aug 16 00:49:41:856 2011 AC STP/3/STP_FORWARDING: Instance 2's port
GigabitEthernet1/0/2 has been set to forwarding state.
```

出力では、MSTI 2 において GigabitEthernet 1/0/1 のポート状態が破棄に遷移し、GigabitEthernet 1/0/2 のポート状態が転送に遷移したことを示しています。

PVST モードで VLAN 1～4094 のポート状態の遷移情報の出力を有効にします。

<AC> system-view

[AC] stp port-log vlan 1 to 4094

```
%Aug    16    00:49:41:856    2006    AC    STP/3/STP_DISCARDING:    VLAN    2's
GigabitEthernet1/0/1 has been set to discarding state!
%Aug    16    00:49:41:856    2006    AC    STP/3/STP_FORWARDING:    VLAN    2's
GigabitEthernet1/0/2 has been set to forwarding state.
```

出力では、VLAN 2 において GigabitEthernet 1/0/1 のポート状態が破棄に遷移し、GigabitEthernet 1/0/2 のポート状態が転送に遷移したことを示しています。

4.1.35 stp priority

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **priority** *priority*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **priority**

デフォルト

32768

View

System view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

priority: 装置のプライオリティを指定します。設定範囲は 0～61440 で、4096 の倍数です（0、4096、8192・・・のように設定します）。装置で 16 までプライオリティを設定することができます。プライオリティの値を小さくすると、装置のプライオリティが高くなります。

説明

stp priority コマンドは装置のプライオリティを設定します。

undo stp priority コマンドはデフォルトのプライオリティに戻します。

MSTI あるいは VLAN を指定しない場合、MSTP CIST、STP あるいは RSTP のポートのプライオリティを設定します。

例

MSTI モードで MSTI 1 の装置のプライオリティを 4096 に設定します。

<AC> system-view

[AC] stp instance 1 priority 4096

PVST モードで VLAN 1 の装置のプライオリティを 4096 に設定します。

<AC> system-view

[AC] stp vlan 1 priority 4096

4.1.36 stp pvst-bpdu-protection

Syntax

stp pvst-bpdu-protection

undo stp pvst-bpdu-protection

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

stp pvst-bpdu-protection コマンドは PVST BPDU ガード機能を有効にします。

undo stp pvst-bpdu-protection コマンドは PVST BPDU ガード機能を無効にします。

ポートが PVST BPDU を受信する場合、MSTP が有効な装置はポートをシャットダウンします。シャットダウンしたポートは検出間隔が終了したのち、up となります。検出間隔を設定する場合、**shutdown-interval** コマンドを使用します。

例

MSTP モードで PVST BPDU ガード機能を有効にします。

<AC> system-view

[AC] stp pvst-bpdu-protection

関連コマンド

shutdown-interval（コマンドマニュアルのセクション 1 *はじめに “装置管理”*）

4.1.37 stp region-configuration

Syntax

stp region-configuration

undo stp region-configuration

デフォルト

MST リージョンのデフォルト設定は以下です。

- 装置の MST リージョン名は装置の MAC アドレスです。
- すべての VLAN は CIST にマッピングされています。
- MSTP のリージョンレベルは 0 です。

View

System view

定義済みユーザロール

network-admin

説明

stp region-configuration コマンドは MST region view に移行します。

undo stp region-configuration コマンドはデフォルトの MST リージョンの設定に戻します。

MST region view に移行した後、リージョン名、VLAN-インスタンスマッピング、レビジョンレベルを含む MST リージョンのパラメータを設定することができます。

例

MST region view に移行します。

<AC> system-view

[AC] stp region-configuration

[AC-mst-region]

4.1.38 stp role-restriction

Syntax

stp role-restriction

undo stp role-restriction

デフォルト

無効

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp role-restriction コマンドはポート役割の制限機能を有効にします。

undo stp role-restriction コマンドはポート役割の制限機能を無効にします。

ポート役割の制限機能がポートで有効にした場合、ポートはルートポートにできません。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 のポート役割の制限機能を有効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] stp role-restriction

4.1.39 stp root primary

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root primary**

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root**

デフォルト

装置はルートブリッジではありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

説明

stp root primary コマンドは装置をルートブリッジとして設定します。

undo stp root コマンドはデフォルトに戻します。

装置をルートブリッジに指定した後は、装置のプライオリティを変更することはできません。

MSTI あるいは VLAN を指定しない場合、装置を MSTP CIST、STP あるいは RSTP のルートブリッジとして設定します。

例

MSTP モードで MSTI 1 のルートブリッジとして装置を指定します。

<AC> system-view

[AC] stp instance 1 root primary

PVST モードで VLAN 1 のルートブリッジとして装置を指定します。

<AC> system-view

[AC] stp vlan 1 root primary

関連コマンド

- **stp priority**
- **stp root secondary**

4.1.40 stp root secondary

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root secondary**

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root**

デフォルト

装置はセカンダリルートブリッジではありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

説明

stp root secondary コマンドは装置をセカンダリルートブリッジとして設定します。

undo stp root コマンドはデフォルトに戻します。

装置をルートブリッジに指定した後は、装置のプライオリティを変更することはできません。

MSTI あるいは VLAN を指定しない場合、装置を MSTP CIST、STP あるいは RSTP のセカンダリルートブリッジとして設定します。

例

MSTP モードで MSTI 1 のセカンダリルートブリッジとして装置を指定します。

<AC> system-view

[AC] stp instance 1 root secondary

PVST モードで VLAN 1 のセカンダリルートブリッジとして装置を指定します。

<AC> system-view

[AC] stp vlan 1 root secondary

関連コマンド

- **stp priority**
- **stp root primary**

4.1.41 stp root-protection

Syntax

stp root-protection

undo stp root-protection

デフォルト

無効

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp root-protection コマンドはポートでルートガード機能を有効にします。

undo stp root-protection コマンドはポートでルートガード機能を無効にします。

ポートのルートガード機能はループガード機能の設定を同時に設定することはできません。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 でルートガード機能を有効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] stp root-protection

関連コマンド

- **stp edged-port**
- **stp loop-protection**

4.1.42 stp tc-protection

Syntax

stp tc-protection

undo stp tc-protection

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

stp tc-protection コマンドは装置の TC-BPDU ガード機能を有効にします。

undo stp tc-protection コマンドは装置の TC-BPDU ガード機能を無効にします。

TC-BPDU ガードを有効にすると、最初に TC-BPDU を受信した後、10 秒ごとに、転送アドレスエントリを即座に削除する最大数を設定することができます。TC-BPDU を制限以上受信した場合、一定の期間が経過した後、装置は、転送アドレスエントリを削除します。これにより、頻繁に転送アドレスエントリの削除を行うことを防ぐことができます。

例

装置の TC-BPDU ガード機能を無効にします。

<AC> system-view

[AC] undo stp tc-protection

関連コマンド

stp tc-protection threshold

4.1.43 stp tc-protection threshold

Syntax

stp tc-protection threshold *number*

undo stp tc-protection threshold

デフォルト

6

View

System view

定義済みユーザロール

network-admin

パラメータ

number: TC-BPDU を受信した直後から、10 秒ごとに装置が即座に転送アドレスエントリを削除する最大の回数を指定します。設定範囲は 1〜255 です。

説明

stp tc-protection threshold コマンドは TC-BPDU を受信した直後から 10 秒ごとに、装置が即座に転送アドレスエントリを削除する最大の回数を設定します。

undo stp tc-protection threshold コマンドはデフォルトに戻します。

例

10 秒ごとに装置が即座に転送アドレスエントリを削除する最大の回数を 10 に設定します。

<AC> system-view

[AC] stp tc-protection threshold 10

関連コマンド

stp tc-protection

4.1.44 stp timer forward-delay

Syntax

stp [**vlan** *vlan-id-list*] **timer forward-delay** *time*

undo stp [**vlan** *vlan-id-list*] **timer forward-delay**

デフォルト

1500 センチ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。STP、RSTP、MSTP では使用しません。

time: 転送遅延を設定します。単位はセンチ秒です。設定範囲は 400～3000 で、100 の倍数です。（400、500、600、・・・のように設定します）

説明

stp timer forward-delay コマンドは転送遅延タイマを設定します。

undo stp timer forward-delay コマンドはデフォルトに戻します。

転送遅延タイマは状態の遷移の時間間隔を決定します。一時的なループを防ぐため、スパニングツリーのポートは廃棄状態から転送状態に遷移する前に、学習（中間）状態になります。リモート装置と同期を維持するため、ポートは転送遅延タイマの間、状態遷移を待ちます。

stp bridge-diameter コマンドでスイッチネットワークのダイアメータを指定し、**stp timer forward-delay** コマンドで転送遅延を設定しないことを推奨します。

この **stp bridge-diameter** コマンドによってスパニングツリーは転送遅延タイマを最適な値に自動で計算します。ネットワークダイアメータがデフォルト値である場合、転送遅延タイマもデフォルト値を使用します。

例

MSTP モードで転送遅延タイマを 2000 センチ秒に設定します。

<AC> system-view

[AC] stp timer forward-delay 2000

PVST モードで VLAN 2 の転送遅延タイマを 2000 センチ秒に設定します。

<AC> system-view

[AC] stp vlan 2 timer forward-delay 2000

関連コマンド

- **stp bridge-diameter**
- **stp timer hello**
- **stp timer max-age**

4.1.45 stp timer hello

Syntax

stp [**vlan** *vlan-id-list*] **timer hello** *time*

undo stp [**vlan** *vlan-id-list*] **timer hello**

デフォルト

200 センチ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。STP、RSTP、MSTP では使用しません。

time: hello 時間を設定します。単位はセンチ秒です。設定範囲は 100～1000 で、100 の倍数です。（100、200、300、・・・のように設定します）

説明

stp timer hello コマンドは hello 時間を設定します。

undo stp timer hello コマンドはデフォルトに戻します。

hello 時間はスパニングツリーを維持するため、装置が configuration BPDU を送信する間隔です。装置が指定した時間以内に configuration BPDU を受信できない場合、新たなスパニングツリー計算が開始されます。

stp bridge-diameter コマンドでスイッチネットワークのダイアメータを指定し、**stp timer hello** コマンドで hello 時間を設定しないことを推奨します。

この **stp bridge-diameter** コマンドによってスパニングツリーは hello 時間を最適な値に自動で計算します。ネットワークダイアメータがデフォルト値である場合、hello 時間もデフォルト値を使用します。

例

MSTP モードで hello 時間を 400 センチ秒に設定します。

<AC> system-view

[AC] stp timer hello 400

PVST モードで VLAN 2 の hello 時間を 400 センチ秒に設定します。

<AC> system-view

[AC] stp vlan 2 timer hello 400

関連コマンド

- **stp bridge-diameter**
- **stp timer forward-delay**
- **stp timer max-age**

4.1.46 stp timer max-age

Syntax

stp [**vlan** *vlan-id-list*] **timer max-age** *time*

undo stp [**vlan** *vlan-id-list*] **timer max-age**

デフォルト

2000 センチ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。STP、RSTP、MSTP では使用しません。

time: 最大エージングタイマを設定します。単位はセンチ秒です。設定範囲は 600～4000 で、100 の倍数です。（600、700、800、・・・のように設定します）

説明

stp timer max-age コマンドは装置の最大エージングタイマを設定します。

undo stp timer max-age コマンドはデフォルトに戻します。

MSTP ネットワークの CIST で、装置は最大エージングタイマにもとづいて、ポートが受信した configuration BPDU がタイムアウトしているかどうかを判断します。ポートで configuration BPDU の受信がタイムアウトした場合、新しいスパニングツリーの再計算が開始されます。最大エージングタイマは、CIST（あるいは MSTI 0）のみ有効です。

stp bridge-diameter コマンドでスイッチネットワークのダイアメータを指定し、**stp timer max-age** コマンドで最大エージングタイマを設定しないことを推奨します。

この **stp bridge-diameter** コマンドによってスパニングツリーは最大エージングタイマを最適な値に自動で計算します。ネットワークダイアメータがデフォルト値である場合、最大エージングタイマもデフォルト値を使用します。

例

MSTP モードで最大エージングタイマを 1000 センチ秒に設定します。

<AC> system-view

[AC] stp timer max-age 1000

PVST モードで VLAN 2 の最大エージングタイマを 1000 センチ秒に設定します。

<AC> system-view

[AC] stp vlan 2 timer max-age 1000

関連コマンド

- **stp bridge-diameter**
- **stp timer forward-delay**
- **stp timer hello**

4.1.47 stp timer-factor

Syntax

stp timer-factor *factor*

undo stp timer-factor

デフォルト

3

View

System view

定義済みユーザロール

network-admin

パラメータ

factor: タイムアウトファクタを指定します。設定範囲は 1～20 です。

説明

stp timer-factor コマンドはタイムアウト時間を決めるタイムアウトファクタを設定します。

タイムアウト時間 ＝ タイムアウトファクタ × 3 × hello 時間

undo stp timer-factor コマンドはデフォルトに戻します。

ネットワークトポロジが安定した後、各非ルートブリッジは、リンク異常を確認するために周囲の装置に対し、hello 時間の間隔で設定 BPDU を転送します。通常、装置が上流装

置から hello 時間の 9 倍の時間内に BPDU を受信しないと、装置は上流装置が故障しているとみなし、新たなスパニングツリー計算を開始します。

安定したネットワークにおいては、このようなスパニングツリー計算は、上流装置がビジー状態の場合に起こります。この場合、タイムアウト時間を長く（4 以上に）設定することにより、このような不要なスパニングツリー計算を避け、ネットワークリソースを節約できます。安定したネットワークでは、タイムアウトファクタを 5、6、または 7 に設定することが推奨されます。

例

タイムアウトファクタを 7 に設定します。

<AC> system-view

[AC] stp timer-factor 7

関連コマンド

stp timer hello

4.1.48 stp transmit-limit

Syntax

stp transmit-limit *limit*

undo stp transmit-limit

デフォルト

すべてのポートの BPDU の転送レートは 10 です。各ポートは各 hello 時間内に 10 の BPDU を送信します。

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

limit: BPDU 転送レートを設定します。設定範囲は 1～255 です。

説明

stp transmit-limit コマンドはポートの BPDU 転送レートを設定します。

undo stp transmit-limit コマンドはデフォルトに戻します。

各 hello 時間以内にポートが送信できる BPDU の最大数は、BPDU 転送レートと hello 時間の合計に等しいです。

BPDU 転送レートを大きくするとは多くのシステムリソースが必要となります。

最大 BPDU 転送レートを適切に設定することにより、ポートが BPDU を送信するスピードを制限し、ネットワークトポロジが変更した際に過剰な帯域リソースを使用しないようにできます。デフォルト値を使うことを推奨します。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 の BPDU 転送レートを 5 に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] stp transmit-limit 5

4.1.49 stp vlan enable

Syntax

stp vlan *vlan-id-list* **enable**

undo stp vlan *vlan-id-list* **enable**

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。このオプションを指定しない場合、グローバルでスパニングツリー機能（VLAN が含まれません）を有効あるいは無効にしてください。

説明

stp vlan enable コマンドは VLAN でスパニングツリーを有効にします。

undo stp enable コマンドは VLAN でスパニングツリーを無効にします。

スパニングツリー機能を有効にしたとき、スパニングツリーのモードの設定により装置は STP、RSTP、PVST、MSTP モードで動作します。

スパニングツリー機能を有効にしたとき、装置は設定された configuration BPDU にもとづいて自動で VLAN のスパニングツリーの状態を維持します。スパニングツリー機能を無効にしたとき、装置はスパニングツリーの状態の維持を停止します。

例

PVST モードにおいてグローバルでスパニングツリーを有効にし、VLAN 2 でスパニングツリーを有効にします。

<AC> system-view

[AC] stp mode pvst

[AC] stp global enable

[AC] stp vlan 2 enable

関連コマンド

- **stp enable**
- **stp global enable**
- **stp mode**

4.1.50 vlan-mapping modulo

Syntax

vlan-mapping modulo *modulo*

デフォルト

すべての VLAN は CIST（MSTI 0）にマッピングされています。

View

MST region view

定義済みユーザロール

network-admin

パラメータ

modulo: モジュロの値を設定します。設定範囲は 1～64 です。

説明

vlan-mapping modulo コマンドは指定モジュロの値に従って MST リージョンの VLAN を MSTI にマッピングし、VLAN-インスタンスマッピングテーブルの作成を早急に行います。

異なる MSTI に VLAN をマッピングすることはできません。すでに MSTI にマッピングされている VLAN を新しい MSTI にマッピングすると、古いマッピングは自動的に削除されます。

このコマンドは、次の式に従い、VLAN をマッピングする MSTI の ID を決定します。

ID ＝ (VLAN ID － 1) %*modulo* ＋ 1

(VLAN ID － 1) %*modulo* は (VLAN ID － 1)に対してモジュロ演算を行うことを意味します。モジュロの値が 15 である場合、VLAN 1 は MSTI 1 に、VLAN 2 は MSTI 2 に、VLAN 15 は MSTI 15 に、VLAN 16 は MSTI 16 のようにマッピングされます。

例

VLAN を MSTI にモジュロ 8 でマッピングします。

<AC> system-view

[AC] stp region-configuration

[AC-mst-region] vlan-mapping modulo 8

関連コマンド

- **active region-configuration**
- **check region-configuration**
- **display stp region-configuration**
- **region-name**
- **revision-level**

目次

このセクションのページは **4-x-x** です。

5 章 ループ検出 5-1
5.1 ループ検出設定コマンド 5-1
5.1.1 display loopback-detection 5-1
5.1.2 loopback-detection action 5-2
5.1.3 loopback-detection enable 5-3
5.1.4 loopback-detection global action 5-5
5.1.5 loopback-detection global enable 5-6
5.1.6 loopback-detection interval-time 5-7

5章 ループ検出

5.1 ループ検出設定コマンド

5.1.1 display loopback-detection

Syntax

display loopback-detection

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display loopback-detection コマンドはループバック検出の設定と状態を表示します。

例

ループバック検出の設定と状態を表示します。

<AC> display loopback-detection

```
Loopback detection is enabled.
Loopback detection interval is 30 second(s).
Loopback is detected on following interfaces:
 Interface             Action mode
 GigabitEthernet1/0/1    Block
 GigabitEthernet1/0/2    Shutdown
 GigabitEthernet1/0/3    None
 GigabitEthernet1/0/4    No-learning
```

表 5-1 コマンド出力

フィールド	説明

Action mode	ループガードのアクションです。
	• **Block**–ポートでループが検出されたとき、装置は以下の処理を行います。
	  • ログを出力します。
	  • MACアドレスの学習を無効にします。

フィールド	説明
	• ポート上の着信トラフィックをブロックします。 • **None**–ポートでループが検出されたとき、装置はログを出力しますが、ポートでアクションは行いません。 • **No-learning**–ポートでループが検出されたとき、装置はログを出力し、MACアドレスの学習を無効にします。 🕮 **メモ：** **loopback-detection action shutdown**コマンドを設定し、ポートでループが検出されたとき、ポートがシャットダウンします。ポートのシャットダウンによってループ状態が解除されるため、**display loopback-detection**コマンド上に検知ポートは表示されません。“Shutdown”状態が表示されることはありません。

5.1.2 loopback-detection action

Syntax

Layer 2 Ethernet interface view：

loopback-detection action { **block** | **no-learning** | **shutdown** }

undo loopback-detection action

Layer 2 aggregate interface view：

loopback-detection action shutdown

undo loopback-detection action

デフォルト

ポートでループが検出されたとき、装置はログを出力しますが、ポートでアクションは行いません。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

block: ブロックモードを有効にします。ループを検出すると、装置は以下の処理を行います。

- ログを出力します。
- MAC アドレスの学習を無効にします。
- ポートの入力トラフィックをブロックします。

アグリゲートインタフェースではサポートしていません。

no-learning: **no-learning** モードを有効にします。ループを検出すると、装置はログを出力し、MAC アドレスの学習を無効にします。アグリゲートインタフェースではサポートしていません。

shutdown: シャットダウンモードを有効にします。ループを検出すると、装置はログを出力し、すべてのフレームの送受信を無効にするためポートをシャットダウンします。装置は検出タイマが終了すると、自動でポートをアップします。**shutdown-interval** コマンドで検出タイマを設定することができます。詳細はコマンドマニュアルのセクション 1 *はじめに　“装置管理”* を参照してください。

説明

loopback-detection action コマンドはポートのループ保護のアクションを設定します。

undo loopback-detection action コマンドはデフォルトに戻します。

グローバルでループ保護のアクションを設定する場合、**loopback-detection global action** コマンドを使用します。

グローバルの設定はすべてのポートで適用されます。ポートの設定は指定されたポートで適用されます。ポートの設定はグローバルの設定よりも優先されます。

例

GigabitEthernet 1/0/1 のループ保護のアクションをシャットダウンに設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] loopback-detection action shutdown

関連コマンド

- **display loopback-detection**
- **loopback-detection global action**

5.1.3 loopback-detection enable

Syntax

loopback-detection enable vlan { *vlan-id-list* | **all** }

undo loopback-detection enable vlan { *vlan-id-list* | **all** }

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: VLAN リストを指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: 既存のすべての VLAN を指定します。

説明

loopback-detection enable コマンドはポートでループ検出を有効にします。

undo loopback-detection enable コマンドはポートでループ検出を無効にします。

グローバルでループ検出を有効にする場合、**loopback-detection global enable** コマンドを使用します。

ポートのループ検出の設定はグローバルでループ検出の設定が行われたのち適用されます。

グローバル設定は、指定された VLAN のすべてのポートに適用されます。ポート単位の設定は、ポートが指定された VLAN に属する場合にのみ、個々のポートに適用されます。ポート単位の設定は、グローバル設定よりも優先されます。

装置がポートでループを検出した場合、装置のフロントパネルにあるポート LED は 2 秒間隔で点滅します。

例

VLAN 10～VLAN 20 の GigabitEthernet 1/0/1 でループ検出を有効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] loopback-detection enable vlan 10 to 20

関連コマンド

- **display loopback-detection**
- **loopback-detection global enable**

5.1.4 loopback-detection global action

Syntax

loopback-detection global action shutdown

undo loopback-detection global action

デフォルト

ループが検出されたとき、装置はログを出力しますが、保護アクションは行いません。

View

System view

定義済みユーザロール

network-admin

パラメータ

shutdown: シャットダウンモードを有効にします。ループを検出すると、装置はログを出力し、ポートをシャットダウンします。装置は検出タイマが終了すると、自動でポートを転送状態にします。**shutdown-interval** コマンドで検出タイマを設定することができます。詳細はコマンドマニュアルのセクション 1 *はじめに “装置管理”* を参照してください。

説明

loopback-detection global action コマンドはグローバルでループ保護のアクションを設定します。

undo loopback-detection global action コマンドはデフォルトに戻します。

ポートでループ保護のアクションを設定する場合、interface view で **loopback-detection action** コマンドを使用します。

グローバルの設定はすべてのポートで適用されます。ポートの設定は指定されたポートで適用されます。ポートの設定はグローバルの設定よりも優先されます。

🕮 **メモ**:

- **shutdown** アクションを設定し、ポートでループが検出されたとき、ポートをシャットダウンし、ループ状態を解除するため、アクション実行時に RECOVERED のログも出力します。
- **shutdown** アクションによるポートのシャットダウンは、**display interface** コマンドの Current state フィールドの状態が DOWN（Loopback detection down）と表示されます。

例

グローバルでループ保護のアクションをシャットダウンに設定します。

<AC> system-view

[AC] loopback-detection global action shutdown

関連コマンド

- **display loopback-detection**
- **loopback-detection action**

5.1.5 loopback-detection global enable

Syntax

loopback-detection global enable vlan { *vlan-id-list* | **all** }

undo loopback-detection global enable vlan { *vlan-id-list* | **all** }

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: VLAN リストを指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: 既存のすべての VLAN を指定します。

説明

loopback-detection global enable コマンドはグローバルでループ検出を有効にします。

undo loopback-detection global enable コマンドはグローバルでループ検出を無効にします。

ポートでループ検出を有効にする場合、interface view で **loopback-detection enable** コマンドを使用します。

グローバルの設定は指定された VLAN のすべてのポートで適用されます。ポートの設定は指定された VLAN に所属するポートで適用されます。ポート単位の設定は、ポートが

指定された VLAN に属する場合にのみ、個々のポートに適用されます。ポートの設定はグローバルの設定よりも優先されます。

例

VLAN 10～VLAN 20 のすべてのポートでループ検出を有効にします。

<AC> system-view

[AC] loopback-detection global enable vlan 10 to 20

関連コマンド

- **display loopback-detection**
- **loopback-detection enable**

5.1.6 loopback-detection interval-time

Syntax

loopback-detection interval-time *interval*

undo loopback-detection interval-time

デフォルト

5 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: ループ検出間隔を設定します。設定範囲は 1～300 秒です。

説明

loopback-detection interval-time コマンドはループ検出間隔を設定します。

undo loopback-detection interval-time コマンドはデフォルトに戻します。

ループ検出が有効であるとき、装置は指定された間隔でループ検出フレームを送信します。検出間隔が短い場合、精度が高くなりますが、多くのリソースが消費されます。ループ検出間隔を設定する場合、システムの性能とループ検出速度を考慮してください。

🕮 **メモ：**

undo loopback-detection interval-time コマンドを実行しても、デフォルト設定には戻りません。**undo** コマンドを実行した場合、30 秒のループ検出間隔で動作する設定となります。デフォルト値に戻す場合、**loopback-detection interval-time 5** コマンドを実行してください。

例

ループ検出間隔を 10 秒に設定します。

<AC> system-view

[AC] loopback-detection interval-time 10

関連コマンド

display loopback-detection

目次

このセクションのページは **4-x-x** です。

6 章 LLDP 6-1
6.1 LLDP 設定コマンド 6-1
6.1.1 display lldp local-information 6-1
6.1.2 display lldp neighbor-information 6-8
6.1.3 display lldp statistics 6-16
6.1.4 display lldp status 6-23
6.1.5 display lldp tlv-config 6-30
6.1.6 lldp admin-status 6-33
6.1.7 lldp check-change-interval 6-35
6.1.8 lldp enable 6-36
6.1.9 lldp encapsulation snap 6-36
6.1.10 lldp fast-count 6-37
6.1.11 lldp global enable 6-38
6.1.12 lldp hold-multiplier 6-39
6.1.13 lldp management-address-format string 6-40
6.1.14 lldp notification remote-change enable 6-41
6.1.15 lldp timer notification-interval 6-42
6.1.16 lldp timer reinit-delay 6-42
6.1.17 lldp timer tx-interval 6-43
6.1.18 lldp tlv-enable 6-44

6章 LLDP

6.1 LLDP設定コマンド

デバイスモデルによってインタフェースのサポートは異なります。詳細は、オペレーションマニュアルのセクション 3 *インタフェース "Ethernet インタフェース"* を参照してください。

6.1.1 display lldp local-information

Syntax

display lldp local-information [**global** | **interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

global: グローバルのローカル LLDP 情報を表示します。

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

説明

display lldp local-information コマンドはローカル LLDP 情報を表示します。

パラメータを指定しない場合、以下が含まれるすべてのローカル LLDP 情報を表示します。

- グローバルの LLDP 情報
- up 状態の LLDP が有効なポートの LLDP 情報

例

すべてのローカル LLDP 情報を表示します。

<AC> display lldp local-information

```
Global LLDP local-information:
 Chassis ID         : ac74-096a-ded8
 System name        : AC
 System description  : Copyright (c) 2004-2018 New H3C Technologies Co., Ltd. Al
```

```
                  l rights reserved.
 System capabilities supported : Bridge, Router, Customer Bridge, Service Bridge
 System capabilities enabled   : Bridge, Router, Customer Bridge

 MED information:
 Device class             : Connectivity device
 MED inventory information of master board:
 HardwareRev              : Ver.B
 FirmwareRev              : 1.02
 SoftwareRev              : 7.1.2
 SerialNum                : 210235A3KYC17B000010
 Manufacturer name         : NEC
 Model name               : QX-W2230AC
 Asset tracking identifier  : Unknown

LLDP local-information of port 4[GigabitEthernet1/0/4]:
 Port ID type       : Interface name
 Port ID           : GigabitEthernet1/0/4
 Port description    : GigabitEthernet1/0/4 Interface
 LLDP agent nearest-bridge management address:
 Management address type          : IPv4
 Management address              : 192.168.1.101
 Management address interface type : IfIndex
 Management address interface ID   : 10
 Management address OID           : 0
 LLDP agent nearest-nontpmr management address:
 Management address type          : IPv4
 Management address              : 192.168.1.101
 Management address interface type : IfIndex
 Management address interface ID   : 10
 Management address OID           : 0
 LLDP agent nearest-customer management address:
 Management address type          : IPv4
 Management address              : 192.168.1.101
 Management address interface type : IfIndex
 Management address interface ID   : 10
 Management address OID           : 0
 Port VLAN ID(PVID)  : 1
 Port and protocol VLAN ID(PPVID)  : 0
 Port and protocol VLAN supported  : No
 Port and protocol VLAN enabled    : No
 VLAN name of VLAN 1       : VLAN 0001
 Management VLAN ID  : 0
```

```
Link aggregation supported : Yes
Link aggregation enabled   : No
Aggregation port ID        : 0
Auto-negotiation supported : Yes
Auto-negotiation enabled   : No
OperMau                  : Speed(1000)/Duplex(Full)
Power port class          : PD
PSE power supported       : No
PSE power enabled         : No
PSE pairs control ability  : No
Power pairs              : Signal
Port power classification  : Class 0
Maximum frame size        : 1600
Transmit Tw              : 0 us
Receive Tw               : 0 us
Fallback Tw              : 0 us
Echo Transmit Tw          : 0 us
Echo Receive Tw           : 0 us
PoE PSE power source      : Unknown
Port PSE priority         : Unknown
Port available power value : 0.0 w

<AC>
```

表 6-1 コマンド出力

フィールド	説明
Chassis ID	装置のBridge MACアドレスです。
System capabilities supported	サポートされる機能です。 • **Bridge**–スイッチングがサポートされます。 • **Router**–ルーティングがサポートされます。 • **WlamAccessPoint**—ローカル装置は無線APとして動作します。 • **Repeater**–信号リピートがサポートされます。 • **Telephone**—ローカル装置が電話として動作します。 • **DocsisCableDevice**–ローカル装置がDOCSIS準拠のケーブル装置として動作します。 • **StationOnly**–ローカル装置が基地局のみとして動作します。 • **Customer Bridge**–カスタマブリッジ機能がサポートされます。 • **Service Bridge**–サービスブリッジ機能がサポートされま

フィールド	説明
	す。 • **TPMR**–TPMR（The two-port MAC relay）機能がサポートされます。 • **Other**–上記で記載されている以外の機能がサポートされます。
System capabilities enabled	有効な機能です。 • **Bridge**–スイッチングが有効です。 • **Router**–ルーティングが有効です。 • **WlanAccessPoint**—ローカル装置は無線APとして動作します。 • **Repeater**–信号リピートが有効です。 • **Telephone**—ローカル装置が電話として動作しています。 • **DocsisCableDevice**–ローカル装置がDOCSIS準拠のケーブル装置として動作しています。 • **StationOnly**–ローカル装置が基地局のみとして動作しています。 • **Customer Bridge**–カスタマブリッジ機能が有効です。 • **Service Bridge**–サービスブリッジ機能が有効です。 • **TPMR**– TPMR（The two-port MAC relay）機能が有効です。 • **Other**–上記で記載されている以外の機能が有効です。
Device class	MED装置のクラスです。 • **Connectivity device**–ネットワーク装置です。 • **Class I**–通常の端末装置です。basic LLDP検出サービスが必要です。 • **Class II**–メディア端末装置です。通常の端末装置に加えて、メディアストリームをサポートします。 • **Class III**–通信端末装置です。通常の端末装置、メディアストリームに加えて、エンドユーザのIP通信システムをサポートします。
HardwareRev	ハードウェアバージョンです。
FirmwareRev	ファームウェアバージョンです。
SoftwareRev	ソフトウェアバージョンです。
SerialNum	シリアル番号です。
Manufacturer name	装置の製造メーカです。

フィールド	説明
Model name	装置モデルです。
Port ID type	ポートIDタイプです。 ● MACアドレスです。 ● インタフェース名です。
Port ID	ポートIDです。ポートIDタイプによって変わります。
Management address interface type	管理アドレスで識別されるインタフェースの番号タイプです。
Management address interface ID	管理アドレスで識別されるインタフェースのインデックスです。
Management address OID	管理アドレスのオブジェクトIDです。
DCBX control info	IEEE Std 802.1Qaz-2011のバージョン情報を表示します。 装置の現在のソフトウェアバージョンではこのフィールドをサポートしていません。
Oper version	DCBXのバージョン番号です。
P0- P1- P2- P3- P4- P5- P6- P7-	ローカルエンドで**priority-flow-control no-drop dot1p dot1p-list**コマンドを使用してサポートされる優先順位の数です。
Number of traffic classes supported	PFCでサポートされているトラフィッククラスの数です。 （Rev 1.01でのみ表示）
DCBX PFC info	装置の現在のソフトウェアバージョンではこのフィールドをサポートしていません。
Value of MBC	MBCは、MACsecをバイパスするパケットの能力を示します。これは1ビット長です。 ● **0**–MACsecが無効になっていると、パケットはMACsecをバイパスできます。 ● **1**–MACsecが無効になっていると、パケットはMACsecをバイパスできません。
Link aggregation supported	ポートのリンクアグリゲーションがサポートされているかどうかを示します。
Link aggregation enabled	ポートのリンクアグリゲーションが有効かどうかを示します。
Aggregation port ID	メンバポートIDです。リンクアグリゲーションが無効であるとき、0と表示されます。
Auto-negotiation supported	ポートのオートネゴシエーションがサポートされているかを示します。
Auto-negotiation enabled	ポートのオートネゴシエーションが有効かどうかを示します。
OperMau	ポートの通信速度、通信モードです。

フィールド	説明
Power port class	PoEポートのクラスです。 ● **PSE**–電力供給装置です。 ● **PD**–電力が供給された装置です。
PSE power supported	装置がPSEとして動作可能かどうかを示します。
PSE power enabled	装置がPSEとして動作しているかどうかを示します。
PSE pairs control ability	PSE-PD間のPoE電力管理機能が有効かどうかを示します。
Power pairs	電力供給モードです。 ● **Signal**–データ転送と同時に電力を供給します。 ● **Spare**–データ転送と別の信号線で電力を供給します。
Port power classification	PDのポート供給電力のクラスです。 この表示は、PSEが供給できるPDの供給電力のクラスを表しており、PSE装置でない場合は未対応です。PSE装置でない場合は ”Class 0” を表示します。 ● **Class 0**ークラス0です。 ● **Class 1**ークラス1です。 ● **Class 2**ークラス2です。 ● **Class 3**ークラス3です。 ● **Class 4**ークラス4です。
Power type	電源タイプ: ● Type 1 PD ● Type 2 PD ● Type 1 PSE ● Type 2 PSE
Power source	電源: ● 電源の種類がPSEの場合、オプションは次のとおりです。 • Unknown—不明な電源です。 • Primary—プライマリ電源です。 • Backup—バックアップ電源です。 • Reserved ● 電源の種類がPDの場合、オプションは次のとおりです。 • Unknown—不明な電源です。 • PSE—PSE電源です。 • Local—ローカル電源です。 • PSE and local—PSE電源とローカル電源です。

フィールド	説明
Power priority	• Unknown • Critical • High • Low
PD requested power value	PDが要求した電力です。（ワット）
PSE allocated power value	PSEが割り当てた電源です。（ワット）
PoE PSE power source	PSE電力供給タイプです。 • **Unknown**–不明な電力供給です。 • **Primary**–プライマリ電力供給です。 • **Backup**–バックアップ電力供給です。
Port PSE priority	PSEポートのPoE電力供給のプライオリティです。 • Unknown • Critical • High • Low
Port available power value	PSEポートのPoE電力あるいはPDポートで必要な電力です。単位はWです。
Transmit Tw	ローカルクライアントのスリープ時間です。単位はμsです。
Receive Tw	ローカルクライアントによって予期されたピアのクライアントのスリープ時間です。単位はμsです。
Fallback Tw	ローカルクライアントによって予期されたピアのクライアント候補のスリープ時間です。単位はμsです。
Echo Transmit Tw	ピアのクライアントのスリープ時間です。単位はμsです。 このフィールドは以下の場合、0と表示されます。 • ローカルクライアントがピアのクライアントのスリープ時間を受信していません。 • ピアのクライアントのスリープ時間が0μsです。
Echo Receive Tw	ピアのクライアントによって予期されたローカルクライアントのスリープ時間です。単位はμsです。 このフィールドは以下の場合、0と表示されます。 • ローカルクライアントがピアのクライアントから予期されたスリープ時間を受信していません。 • ピアのクライアントによって予期されたローカルクライアントのスリープ時間が0μsです。

6.1.2 display lldp neighbor-information

Syntax

display lldp neighbor-information [[[**interface** *interface-type interface-number*] [**verbose**]] | **list** [**system-name** *system-name*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、隣接装置から受信するすべてのポートの LLDP 情報を表示します。

verbose: ローカル装置が隣接装置から受信する LLDP の詳細情報を表示します。指定しない場合、ローカル装置が隣接装置から受信する LLDP の概要情報を表示します。

list: ローカル装置が隣接装置から受信する LLDP の情報をリスト形式で表示します。

system-name *system-name*: システム名で指定された隣接装置からローカル装置が受信する LLDP の情報を表示します。設定範囲は 1～255 です。指定しない場合、リストのすべての隣接装置からローカル装置が受信する LLDP の情報を表示します。

説明

display lldp neighbor-information コマンドはローカル装置が隣接装置から受信する LLDP 情報を表示します。LLDP 情報は LLDP TLV として受信します。

例

隣接装置からすべてのポートのすべての LLDP エージェントが受信した LLDP の概要情報を表示します。

<AC> display lldp neighbor-information verbose

```
LLDP neighbor-information of port 4[GigabitEthernet1/0/4]:
LLDP agent nearest-bridge:
 LLDP neighbor index : 1
 Update time         : 0 days, 0 hours, 1 minutes, 25 seconds
 Chassis type        : MAC address
 Chassis ID          : 487a-da85-b76c
 Port ID type        : Interface name
 Port ID             : GigabitEthernet1/0/17
 Time to live        : 121
 Port description    : GigabitEthernet1/0/17 Interface
```

```
 System name        : QX-L3-SW1
 System description  : Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. Al
                   l rights reserved.
 System capabilities supported : Bridge, Router, Customer Bridge, Service Bridge
 System capabilities enabled   : Bridge, Router, Customer Bridge
 Management address type          : IPv4
 Management address              : 192.168.1.254
 Management address interface type : IfIndex
 Management address interface ID   : 953
 Management address OID           : 0
 Port VLAN ID(PVID)  : 1
 Link aggregation supported : Yes
 Link aggregation enabled   : No
 Aggregation port ID       : 0
 Auto-negotiation supported : Yes
 Auto-negotiation enabled   : Yes
 OperMau                 : Speed(1000)/Duplex(Full)
 Power port class          : PSE
 PSE power supported       : No
 PSE power enabled         : No
 PSE pairs control ability  : No
 Power pairs              : Signal
 Port power classification  : Class 0
 Power type               : Type 2 PSE
 Power source             : Primary
 Power priority           : Unknown
 PD requested power value   : 0.0 w
 PSE allocated power value  : 0.0 w
 Maximum frame size        : 12288
```

隣接装置からすべてのポートのすべての LLDP エージェントが受信した LLDP の概要情報を表示します。

<AC> display lldp neighbor-information

```
LLDP neighbor-information of port 4[GigabitEthernet1/0/4]:
LLDP agent nearest-bridge:
 LLDP neighbor index : 1
 ChassisID/subtype   : 487a-da85-b76c/MAC address
 PortID/subtype     : GigabitEthernet1/0/17/Interface name
 Capabilities       : Bridge, Router, Customer Bridge
```

隣接装置からすべての LLDP エージェントが受信した LLDP の概要情報をリスト形式で表示します。

<AC> display lldp neighbor-information list

```
Chassis ID : * -- -- Nearest nontpmr bridge neighbor
           # -- -- Nearest customer bridge neighbor
           Default -- -- Nearest bridge neighbor
System Name         Local Interface Chassis ID     Port ID
QX-L3-SW1           GE1/0/4        487a-da85-b76c  GigabitEthernet1/0/17
```

表 6-2 コマンド出力

フィールド	説明
LLDP neighbor-information of port 1	LLDP情報がポート1から受信されました。
Update time	隣接情報のLLDP情報が最後にアップデートされた時間です。
Chassis type	装置IDタイプです。 ● **Chassis component**－装置構成です。 ● **Interface alias**－インタフェースの通称です。 ● **Port component**－ポート構成です。 ● **MAC address**－MACアドレスです。 ● **Network address (ipv4)**－ネットワークアドレスです。（IPv4） ● **Interface name**－インタフェース名です。 ● **Locally assigned**–上記にリストされたタイプ以外のローカルで定義された装置タイプです。
Chassis ID	LLDPが送信する装置を識別するIDです。 MACアドレス、ネットワークアドレス、インタフェース、あるいはそれ以外の値を使用することができ、隣接装置の装置タイプに依存します。
Port ID type	ポートIDタイプです。 ● **Interface alias**－インタフェースの通称です。 ● **Port component**－ポート構成です。 ● **MAC address**－MACアドレスです。 ● **Network address (ipv4)**－ネットワークアドレスです。（IPv4） ● **Interface name**－インタフェース名です。 ● **Agent circuit ID**－エージェントcircuit IDです。 ● **Locally assigned**–上記にリストされたタイプ以外のローカルで定義されたポートIDタイプです。
Port ID	ポートIDのタイプの値です。
System name	隣接装置のシステム名です。

フィールド	説明
System description	隣接装置のシステムの説明です。
System capabilities supported	隣接装置でサポートされる機能です。 • **Repeater**–信号のリピータがサポートされます。 • **Bridge**–スイッチングがサポートされます。 • **WlanAccessPoint**–隣接装置は、無線APとして機能します。 • **Router**–ルーティングがサポートされます。 • **Telephone**–隣接装置が電話として動作できます。 • **DocsisCableDevice**–隣接装置がDOCSIS準拠のケーブル装置として動作します。 • **StationOnly**–隣接装置が基地局のみとして動作します。 • **Customer Bridge**–カスタマブリッジ機能がサポートされます。 • **Service Bridge**–サービスブリッジ機能がサポートされます。 • **TPMR**– TPMR（The two-port MAC relay）機能がサポートされます。 • **Other**–上記で記載されている以外の機能がサポートされます。
System capabilities enabled	隣接装置で有効な機能です。 • **Repeater**–信号のリピータが有効です。 • **Bridge**–スイッチングが有効です。 • **WlanAccessPoint**–隣接装置は、無線APとして機能します。 • **Router**–ルーティングが有効です。 • **Telephone**–隣接装置が電話として動作できます。 • **DocsisCableDevice**–隣接装置がDOCSIS準拠のケーブル装置として動作しています。 • **StationOnly**–隣接装置が基地局のみとして動作しています。 • **Customer Bridge**–カスタマブリッジ機能が有効です。 • **Service Bridge**–サービスブリッジ機能が有効です。**TPMR**–TPMR（The two-port MAC relay）機能が有効です。 • **Other**–上記で記載されている以外の機能が有効です。
Management address OID	管理アドレスのオブジェクトIDです。
Port and protocol VLAN ID(PPVID)	ポートのプロトコルVLAN IDです。
Port and protocol VLAN supported	ポートのプロトコルVLANがサポートされているかどうかを示します。

フィールド	説明
Port and protocol VLAN enabled	ポートのプロトコルVLANが有効かどうかを示します。
VLAN name of VLAN 12	VLAN 12の名前です。
Auto-negotiation supported	ポートでネゴシエーションがサポートされているかを示します。
Auto-negotiation enabled	ポートでネゴシエーションが有効かどうかを示します。
OperMau	ポートの通信速度と通信モードの状態です。
Power port class	PoEポートのクラスです。 • **PSE**–電力供給装置です。 • **PD**–電力が供給された装置です。
PSE power supported	装置がPSEとして動作可能かどうかを示します。
PSE power enabled	装置がPSEとして動作しているかどうかを示します。
PSE pairs control ability	PSE-PD間のPoE電力管理機能が有効かどうかを示します。
Power pairs	電力供給モードです。 • **Signal**–データ転送と同時に電力を供給します。 • **Spare**–データ転送と別の信号線で電力を供給します。
Port power classification	PDのポート供給電力のクラスです。 • **Class 0**－クラス0です。 • **Class 1**－クラス1です。 • **Class 2**－クラス2です。 • **Class 3**－クラス3です。 • **Class 4**－クラス4です。
Power type	PoE装置タイプです。 • Type 1 PD • Type 2 PD • Type 1 PSE • Type 2 PSE

Power source	• PSE電力タイプです。
	  • **Unknown**–不明な電力供給です。
	  • **Primary**–プライマリ電力供給です。
	  • **Backup**–バックアップ電力供給です。
	  • **Reserved**－予備です。
	• PoE装置タイプがPDの場合、パラメータを示します。

フィールド	説明
	• **Unknown**–不明な電力供給です。 • **PSE**–PSE電力供給です。 • **Local**–ローカル電力供給です。 • **PSE and local**–PSE電力供給とローカル電力供給です。
Power priority	PSEポートのPoE電力供給のプライオリティです。 ● Unknown ● Critical ● High ● Low
PD requested power value	PDが要求する電力です。単位はWです。
PSE allocated power value	PSEがPDに供給する電力です。単位はWです。
Link aggregation supported	リンクアグリゲーションがサポートされているかどうかを示します。
Link aggregation enabled	リンクアグリゲーションが有効かどうかを示します。
Device class	MED装置クラスです。 ● **Connectivity device**－ネットワーク装置 ● **Class I**－通常の端末装置 基本的なLLDP検出サービスが必要です。 ● **Class II**－メディア端末装置 メディアストリームをサポートし、通常の端末装置としても機能します。 ● **Class III**－通信端末装置 エンドユーザのIP通信システムをサポートし、通常の端末装置またはメディア端末装置としても機能することができる。
Media policy type	メディアポリシータイプです。 ● unknown ● voice ● voiceSignaling ● guestVoice ● guestVoiceSignaling ● softPhoneVoice ● videoconferencing ● streamingVideo ● videoSignaling

フィールド	説明
Unknown policy	メディアポリシーが不明かどうかを示します。
VLAN tagged	メディアVLANのパケットにタグが付いているかどうかを示します。
Media policy VLAN ID	メディアVLANのIDを示します。
Media policy L2 priority	レイヤ2プライオリティを示します。
Media policy DSCP	DSCP値です。
Location format	位置情報の形式です。 ● **Invalid**－位置情報が無効です。 ● **Coordinate-based LCI**－座標ベースの位置情報です。 ● **Civic Address LCI**－典型的なアドレス情報です。 ● **ECS ELIN**－緊急の電話です。
PoE PSE power source	PSE電力供給タイプです。 ● **Unknown**–不明な電力供給です。 ● **Primary**–プライマリ電力供給です。 ● **Backup**–バックアップ電力供給です。
PoE PD power source	PD電力供給タイプです。 ● **Unknown**–不明な電力供給です。 ● **PSE**–PSE電力供給です。 ● **Local**–ローカル電力供給です。 ● **PSE and local**–PSE電力供給とローカル電力供給です。
Port PSE priority	PSEポートのPoE電力供給のプライオリティです。 ● Unknown ● Critical ● High ● Low
Port PD priority	PDポートのPoE電力を受信するプライオリティです。 ● Unknown ● Critical ● High ● Low
Port available power value	PSEポートのPoE電力あるいはPDポートで必要な電力です。単位はWです。
HardwareRev	ハードウェアバージョンです。
FirmwareRev	ファームウェアバージョンです。

フィールド	説明
SoftwareRev	ソフトウェアバージョンです。
SerialNum	シリアル番号です。
Manufacturer name	装置の製造メーカです。
Model name	装置モデルです。
TLV type	不明なbasic TLVタイプです。
TLV information	不明なbasic TLVタイプに含まれる情報です。
Unknown organizationally-defined TLV	不明な組織指定TLVです。
TLV OUI	不明な組織指定TLVのOUIです。
TLV subtype	不明な組織指定のTLVのサブタイプです。
Index	不明な組織指定のインデックスです。
Capabilities	隣接装置で有効な機能です。 ● **Repeater**–信号のリピータが有効です。 ● **Bridge**–スイッチングが有効です。 ● **WlanAccessPoint**–隣接装置はむせんAPとして動作します。 ● **Router**–ルーティングが有効です。 ● **Telephone**–隣接装置が電話として動作できます。 ● **DocsisCableDevice**–隣接装置がDOCSIS準拠のケーブル装置として動作しています。 ● **StationOnly**–隣接装置が基地局のみとして動作しています。 ● **Other**–上記で記載されている以外の機能が有効です。 ● **None**–隣接装置がTLVを通知しません。
Local Interface	LLDP情報を受信するローカルポートです。
Chassis ID : * -- -- Nearest nontpmr bridge neighbor #-- -- Nearest customer bridge neighbor	シャーシIDのフラグです。 ● （*）はnearest non-TPMR bridge neighborを示します。 ● （#）はnearest customer bridge neighborを示します。
Transmit Tw	ローカルクライアントのスリープ時間です。単位はμsです。
Receive Tw	ローカルクライアントによって予期されたピアのクライアントのスリープ時間です。単位はμsです。

フィールド	説明
Fallback Tw	ローカルクライアントによって予期されたピアのクライアント候補のスリープ時間です。単位はμsです。
Echo Transmit Tw	ピアのクライアントのスリープ時間です。単位はμsです。 このフィールドは以下の場合、0と表示されます。 • ローカルクライアントがピアのクライアントのスリープ時間を受信していません。 • ピアのクライアントのスリープ時間が0μsです。
Echo Receive Tw	ピアのクライアントによって予期されたローカルクライアントのスリープ時間です。単位はμsです。 このフィールドは以下の場合、0と表示されます。 • ローカルクライアントがピアのクライアントから予期されたスリープ時間を受信していません。 • ピアのクライアントによって予期されたローカルクライアントのスリープ時間が0μsです。

6.1.3 display lldp statistics

Syntax

display lldp statistics [**global** | [**interface** *interface-type interface-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

global: グローバルの LLDP の統計情報を表示します。

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

説明

display lldp statistics コマンドはグローバルあるいはポートの LLDP の統計情報を表示します。

キーワードを指定しない場合、グローバルの LLDP の統計情報とすべてのポートの LLDP の統計情報を表示します。

例

グローバルの LLDP の統計情報とすべてのポートの LLDP の統計情報を表示します。

<AC> display lldp statistics

```
LLDP statistics global information:
LLDP neighbor information last change time:0 days, 0 hours, 1 minutes, 25 seconds
The number of LLDP neighbor information inserted : 1
The number of LLDP neighbor information deleted  : 0
The number of LLDP neighbor information dropped  : 0
The number of LLDP neighbor information aged out : 0

LLDP statistics information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
The number of LLDP frames transmitted          : 0
The number of LLDP frames received             : 0
The number of LLDP frames discarded            : 0
The number of LLDP error frames                : 0
The number of LLDP TLVs discarded              : 0
The number of LLDP TLVs unrecognized           : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted           : 0
The number of CDP frames received              : 0
The number of CDP frames discarded             : 0
The number of CDP error frames                 : 0

LLDP agent nearest-nontpmr:
The number of LLDP frames transmitted          : 0
The number of LLDP frames received             : 0
The number of LLDP frames discarded            : 0
The number of LLDP error frames                : 0
The number of LLDP TLVs discarded              : 0
The number of LLDP TLVs unrecognized           : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted           : 0
The number of CDP frames received              : 0
The number of CDP frames discarded             : 0
The number of CDP error frames                 : 0

LLDP agent nearest-customer:
The number of LLDP frames transmitted          : 0
The number of LLDP frames received             : 0
The number of LLDP frames discarded            : 0
The number of LLDP error frames                : 0
The number of LLDP TLVs discarded              : 0
The number of LLDP TLVs unrecognized           : 0
The number of LLDP neighbor information aged out : 0
```

```
The number of CDP frames transmitted          : 0
The number of CDP frames received             : 0
The number of CDP frames discarded            : 0
The number of CDP error frames                : 0

LLDP statistics information of port 2 [GigabitEthernet1/0/2]:
LLDP agent nearest-bridge:
The number of LLDP frames transmitted         : 0
The number of LLDP frames received            : 0
The number of LLDP frames discarded           : 0
The number of LLDP error frames               : 0
The number of LLDP TLVs discarded             : 0
The number of LLDP TLVs unrecognized          : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted          : 0
The number of CDP frames received             : 0
The number of CDP frames discarded            : 0
The number of CDP error frames                : 0

LLDP agent nearest-nontpmr:
The number of LLDP frames transmitted         : 0
The number of LLDP frames received            : 0
The number of LLDP frames discarded           : 0
The number of LLDP error frames               : 0
The number of LLDP TLVs discarded             : 0
The number of LLDP TLVs unrecognized          : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted          : 0
The number of CDP frames received             : 0
The number of CDP frames discarded            : 0
The number of CDP error frames                : 0

LLDP agent nearest-customer:
The number of LLDP frames transmitted         : 0
The number of LLDP frames received            : 0
The number of LLDP frames discarded           : 0
The number of LLDP error frames               : 0
The number of LLDP TLVs discarded             : 0
The number of LLDP TLVs unrecognized          : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted          : 0
The number of CDP frames received             : 0
The number of CDP frames discarded            : 0
```

```
The number of CDP error frames                : 0

LLDP statistics information of port 3 [GigabitEthernet1/0/3]:
LLDP agent nearest-bridge:
The number of LLDP frames transmitted          : 0
The number of LLDP frames received             : 0
The number of LLDP frames discarded            : 0
The number of LLDP error frames                : 0
The number of LLDP TLVs discarded              : 0
The number of LLDP TLVs unrecognized           : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted           : 0
The number of CDP frames received              : 0
The number of CDP frames discarded             : 0
The number of CDP error frames                 : 0

LLDP agent nearest-nontpmr:
The number of LLDP frames transmitted          : 0
The number of LLDP frames received             : 0
The number of LLDP frames discarded            : 0
The number of LLDP error frames                : 0
The number of LLDP TLVs discarded              : 0
The number of LLDP TLVs unrecognized           : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted           : 0
The number of CDP frames received              : 0
The number of CDP frames discarded             : 0
The number of CDP error frames                 : 0

LLDP agent nearest-customer:
The number of LLDP frames transmitted          : 0
The number of LLDP frames received             : 0
The number of LLDP frames discarded            : 0
The number of LLDP error frames                : 0
The number of LLDP TLVs discarded              : 0
The number of LLDP TLVs unrecognized           : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted           : 0
The number of CDP frames received              : 0
The number of CDP frames discarded             : 0
The number of CDP error frames                 : 0

LLDP statistics information of port 4 [GigabitEthernet1/0/4]:
```

```
LLDP agent nearest-bridge:
The number of LLDP frames transmitted          : 54
The number of LLDP frames received             : 54
The number of LLDP frames discarded            : 0
The number of LLDP error frames                : 0
The number of LLDP TLVs discarded              : 0
The number of LLDP TLVs unrecognized           : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted           : 0
The number of CDP frames discarded             : 0
The number of CDP error frames                 : 0

LLDP agent nearest-nontpmr:
The number of LLDP frames transmitted          : 0
The number of LLDP frames received             : 0
The number of LLDP frames discarded            : 0
The number of LLDP error frames                : 0
The number of LLDP TLVs discarded              : 0
The number of LLDP TLVs unrecognized           : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted           : 0
The number of CDP frames received              : 0
The number of CDP frames discarded             : 0
The number of CDP error frames                 : 0

LLDP agent nearest-customer:
The number of LLDP frames transmitted          : 0
The number of LLDP frames received             : 0
The number of LLDP frames discarded            : 0
The number of LLDP error frames                : 0
The number of LLDP TLVs discarded              : 0
The number of LLDP TLVs unrecognized           : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted           : 0
The number of CDP frames received              : 0
The number of CDP frames discarded             : 0
The number of CDP error frames                 : 0

LLDP statistics information of port 5 [GigabitEthernet1/0/5]:
LLDP agent nearest-bridge:
The number of LLDP frames transmitted          : 0
The number of LLDP frames received             : 0
The number of LLDP frames discarded            : 0
```

```
The number of LLDP error frames               : 0
The number of LLDP TLVs discarded             : 0
The number of LLDP TLVs unrecognized          : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted          : 0
The number of CDP frames received             : 0
The number of CDP frames discarded            : 0
The number of CDP error frames                : 0

LLDP agent nearest-nontpmr:
The number of LLDP frames transmitted         : 0
The number of LLDP frames discarded           : 0
The number of LLDP error frames               : 0
The number of LLDP TLVs discarded             : 0
The number of LLDP TLVs unrecognized          : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted          : 0
The number of CDP frames received             : 0
The number of CDP frames discarded            : 0
The number of CDP error frames                : 0

LLDP agent nearest-customer:
The number of LLDP frames transmitted         : 0
The number of LLDP frames received            : 0
The number of LLDP frames discarded           : 0
The number of LLDP error frames               : 0
The number of LLDP TLVs discarded             : 0
The number of LLDP TLVs unrecognized          : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted          : 0
The number of CDP frames received             : 0
The number of CDP frames discarded            : 0
The number of CDP error frames                : 0

LLDP statistics information of port 6 [GigabitEthernet1/0/6]:
LLDP agent nearest-bridge:
The number of LLDP frames transmitted         : 0
The number of LLDP frames received            : 0
The number of LLDP frames discarded           : 0
The number of LLDP error frames               : 0
The number of LLDP TLVs discarded             : 0
The number of LLDP TLVs unrecognized          : 0
The number of LLDP neighbor information aged out : 0
```

```
The number of CDP frames transmitted          : 0
The number of CDP frames received             : 0
The number of CDP frames discarded            : 0
The number of CDP error frames                : 0

LLDP agent nearest-nontpmr:
The number of LLDP frames transmitted         : 0
The number of LLDP frames received            : 0
The number of LLDP frames discarded           : 0
The number of LLDP error frames               : 0
The number of LLDP TLVs discarded             : 0
The number of LLDP TLVs unrecognized          : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted          : 0
The number of CDP frames received             : 0
The number of CDP frames discarded            : 0
The number of CDP error frames                : 0

LLDP agent nearest-customer:
The number of LLDP frames transmitted         : 0
The number of LLDP frames received            : 0
The number of LLDP frames discarded           : 0
The number of LLDP error frames               : 0
The number of LLDP TLVs discarded             : 0
The number of LLDP TLVs unrecognized          : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted          : 0
The number of CDP frames received             : 0
The number of CDP frames discarded            : 0
The number of CDP error frames                : 0
```

表 6-3 コマンド出力

フィールド	説明
LLDP statistics global information	グローバルのLLDPの統計情報です。
LLDP neighbor information last change time	隣接情報が最後にアップデートした時間です。
The number of LLDP neighbor information inserted	隣接情報が追加された回数です。
The number of LLDP neighbor information deleted	隣接情報が削除された回数です。
The number of LLDP neighbor information dropped	メモリ空き容量が足りないために隣接情報が廃棄された回数です。

6.1.4 display lldp status

Syntax

display lldp status [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、グローバルの LLDP の状態とすべてのポートの LLDP の状態を表示します。

説明

display lldp status コマンドは LLDP の状態を表示します。

例

グローバルの LLDP の状態と各ポートの LLDP の状態を表示します。

<AC> display lldp status

```
Global status of LLDP: Enable
Bridge mode of LLDP: customer-bridge
The current number of LLDP neighbors: 1
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 1 minutes, 25 seconds
Transmit interval            : 30s
Fast transmit interval       : 1s
Transmit max credit          : 5
Hold multiplier              : 4
Reinit delay                 : 2s
Trap interval                : 30s
Fast start times             : 4

LLDP status information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
Port status of LLDP          : Enable
Admin status                 : TX_RX
Trap flag                    : No
```

```
MED trap flag              : No
Polling interval           : 0s
Number of LLDP neighbors     : 0
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV   : 0
Number of received unknown TLV : 0

LLDP agent nearest-nontpmr:
Port status of LLDP         : Enable
Admin status               : Disable
Trap flag                  : No
MED trap flag              : No
Polling interval           : 0s
Number of LLDP neighbors     : 0
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV   : 0
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP         : Enable
Admin status               : Disable
Trap flag                  : No
MED trap flag              : No
Polling interval           : 0s
Number of LLDP neighbors     : 0
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV   : 0
Number of received unknown TLV : 0

LLDP status information of port 2 [GigabitEthernet1/0/2]:
LLDP agent nearest-bridge:
Port status of LLDP         : Enable
Admin status               : TX_RX
Trap flag                  : No
MED trap flag              : No
Polling interval           : 0s
Number of LLDP neighbors     : 0
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV   : 0
```

```
Number of received unknown TLV : 0

LLDP agent nearest-nontpmr:
Port status of LLDP          : Enable
Admin status                 : Disable
Trap flag                    : No
MED trap flag                : No
Polling interval             : 0s
Number of LLDP neighbors     : 0
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV  : 0
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP          : Enable
Admin status                 : Disable
Trap flag                    : No
MED trap flag                : No
Polling interval             : 0s
Number of LLDP neighbors     : 0
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV  : 0
Number of received unknown TLV : 0

LLDP status information of port 3 [GigabitEthernet1/0/3]:
LLDP agent nearest-bridge:
Port status of LLDP          : Enable
Admin status                 : TX_RX
Trap flag                    : No
MED trap flag                : No
Polling interval             : 0s
Number of LLDP neighbors     : 0
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV  : 0
Number of received unknown TLV : 0

LLDP agent nearest-nontpmr:
Port status of LLDP          : Enable
Admin status                 : Disable
Trap flag                    : No
```

```
MED trap flag              : No
Polling interval           : 0s
Number of LLDP neighbors     : 0
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV   : 0
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP         : Enable
Admin status               : Disable
Trap flag                  : No
MED trap flag              : No
Polling interval           : 0s
Number of LLDP neighbors     : 0
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV   : 0
Number of received unknown TLV : 0

LLDP status information of port 4 [GigabitEthernet1/0/4]:
LLDP agent nearest-bridge:
Port status of LLDP         : Enable
Admin status               : TX_RX
Trap flag                  : No
MED trap flag              : No
Polling interval           : 0s
Number of LLDP neighbors     : 1
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV   : 11
Number of received unknown TLV : 0

LLDP agent nearest-nontpmr:
Port status of LLDP         : Enable
Admin status               : Disable
Trap flag                  : No
MED trap flag              : No
Polling interval           : 0s
Number of LLDP neighbors     : 0
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV   : 0
```

```
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP          : Enable
Admin status                 : Disable
Trap flag                    : No
MED trap flag                : No
Polling interval             : 0s
Number of LLDP neighbors     : 0
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV  : 0
Number of received unknown TLV : 0

LLDP status information of port 5 [GigabitEthernet1/0/5]:
LLDP agent nearest-bridge:
Port status of LLDP          : Enable
Admin status                 : TX_RX
Trap flag                    : No
MED trap flag                : No
Polling interval             : 0s
Number of LLDP neighbors     : 0
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV  : 0
Number of received unknown TLV : 0

LLDP agent nearest-nontpmr:
Port status of LLDP          : Enable
Admin status                 : Disable
Trap flag                    : No
MED trap flag                : No
Polling interval             : 0s
Number of LLDP neighbors     : 0
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV  : 0
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP          : Enable
Admin status                 : Disable
Trap flag                    : No
```

```
MED trap flag              : No
Polling interval           : 0s
Number of LLDP neighbors     : 0
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV   : 0
Number of received unknown TLV : 0

LLDP status information of port 6 [GigabitEthernet1/0/6]:
LLDP agent nearest-bridge:
Port status of LLDP         : Enable
Admin status               : TX_RX
Trap flag                  : No
MED trap flag              : No
Polling interval           : 0s
Number of LLDP neighbors     : 0
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV   : 0
Number of received unknown TLV : 0

LLDP agent nearest-nontpmr:
Port status of LLDP         : Enable
Admin status               : Disable
Trap flag                  : No
MED trap flag              : No
Polling interval           : 0s
Number of LLDP neighbors     : 0
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV   : 0
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP         : Enable
Admin status               : Disable
Trap flag                  : No
MED trap flag              : No
Polling interval           : 0s
Number of LLDP neighbors     : 0
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV   : 0
```

```
Number of received unknown TLV : 0
```

表 6-4 コマンド出力

フィールド	説明
Bridge mode of LLDP	LLDPブリッジモードです。サービスブリッジあるいはカスタマブリッジがあります。
Global status of LLDP	LLDPがグローバルで有効かどうかを示します。
LLDP neighbor information last changed time	隣接情報が最後にアップデートされた時間です。
Transmit interval	LLDPフレームの転送間隔です。
Hold multiplier	TTL乗数です。
Reinit delay	LLDPを再初期化の遅延時間です。
Transmit max credit	LLDPフレームを送信するトークンバケットサイズです。
Trap interval	トラップを転送する間隔です。
Fast start times	新しい隣接装置が検出された際、連続して送信されるLLDPフレームの回数です。
Port 1	ポート1のLLDPの状態です。
Port status of LLDP	ポートのLLDPが有効かどうかを示します。
Admin status	ポートのLLDP動作モードです。 • **Tx_Rx**–ポートはLLDPフレームの送受信ができます。 • **Rx_Only**–ポートはLLDPフレームの受信のみができます。 • **Tx_Only**–ポートはLLDPフレームの送信のみができます。 • **Disable**–ポートはLLDPフレームの送受信ができません。
Trap Flag	トラップが有効かどうかを示します。
Polling interval	LLDPのポーリング間隔です。0はLLDPのポーリングが無効であることを示します。
Number of neighbors	ポートに接続しているLLDPの隣接数です。
Number of MED neighbors	ポートに接続しているMEDの隣接数です。
Number of CDP neighbors	ポートに接続しているCDPの隣接数です。
Number of sent optional TLV	LLDPフレームに含まれるオプションTLVがポートに送信された数です。
Number of received unknown TLV	受信されたLLDPフレームに含まれる不明なTLVの数です。

6.1.5 display lldp tlv-config

Syntax

display lldp tlv-config [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、すべてのポートで通知可能なオプション LLDP TLV のタイプを表示します。

説明

display lldp tlv-config コマンドはポートで通知可能なオプション LLDP TLV のタイプを表示します。

例

GigabitEthernet 1/0/1 で通知可能なオプションの LLDP TLV のタイプを表示します。

<AC> display lldp tlv-config interface gigabitethernet 1/0/1

```
LLDP tlv-config of port 1[GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
NAME                          STATUS    DEFAULT
Basic optional TLV:
 Port Description TLV           YES      YES
 System Name TLV               YES      YES
 System Description TLV         YES      YES
 System Capabilities TLV        YES      YES
 Management Address TLV         YES      YES
IEEE 802.1 extend TLV:
 Port VLAN ID TLV              YES      YES
 Port And Protocol VLAN ID TLV   NO       NO
 VLAN Name TLV                 NO       NO
 DCBX TLV                      NO       NO
 Link Aggregation TLV           YES      YES
 Management VID TLV             NO       NO
IEEE 802.3 extend TLV:
```

```
 MAC-Physic TLV                YES      YES
 Power via MDI TLV             YES      YES
 Maximum Frame Size TLV        YES      YES
LLDP-MED extend TLV:
 Capabilities TLV              YES      YES
 Network Policy TLV            YES      YES
 Location Identification TLV    NO       NO
 Extended Power via MDI TLV     YES      YES
 Inventory TLV                 YES      YES

LLDP agent nearest-nontpmr:
NAME                          STATUS   DEFAULT
Basic optional TLV:
 Port Description TLV          NO       NO
 System Name TLV               NO       NO
 System Description TLV        NO       NO
 System Capabilities TLV       NO       NO
 Management Address TLV        NO       NO
IEEE 802.1 extend TLV:
 Port VLAN ID TLV              NO       NO
 Port And Protocol VLAN ID TLV  NO       NO
 VLAN Name TLV                 NO       NO
 DCBX TLV                      NO       NO
 Link Aggregation TLV          NO       NO
 Management VID TLV            NO       NO
IEEE 802.3 extend TLV:
 MAC-Physic TLV                NO       NO
 Power via MDI TLV             NO       NO
 Maximum Frame Size TLV        NO       NO
 LLDP-MED extend TLV:
 Capabilities TLV              NO       NO
 Network Policy TLV            NO       NO
 Location Identification TLV    NO       NO
 Extended Power via MDI TLV     NO       NO
 Inventory TLV                 NO       NO

LLDP agent nearest-customer:
NAME                          STATUS   DEFAULT
Basic optional TLV:
 Port Description TLV          YES      YES
 System Name TLV               YES      YES
 System Description TLV        YES      YES
 System Capabilities TLV       YES      YES
```

```
 Management Address TLV          YES      YES
IEEE 802.1 extend TLV:
 Port VLAN ID TLV               YES      YES
 Port And Protocol VLAN ID TLV    NO       NO
 VLAN Name TLV                 NO       NO
 DCBX TLV                     NO       NO
 Link Aggregation TLV           YES      YES
 Management VID TLV             NO       NO
IEEE 802.3 extend TLV:
 MAC-Physic TLV                NO       NO
 Power via MDI TLV              NO       NO
 Maximum Frame Size TLV          NO       NO
LLDP-MED extend TLV:
 Capabilities TLV              NO       NO
 Network Policy TLV             NO       NO
 Location Identification TLV     NO       NO
 Extended Power via MDI TLV      NO       NO
 Inventory TLV                 NO       NO
```

表 6-5 コマンド出力

フィールド	説明
LLDP tlv-config of port 1	ポート1の通知可能なオプションTLVです。
NAME	TLVのタイプです。
STATUS	TLVのタイプがポートに送信されたかどうかを示します。
DEFAULT	デフォルトでTLVのタイプがポートに送信されたかどうかを示します。
Basic optional TLV	basic TLVのオプションTLVです。 ● **Port description TL**V－ポート説明TLVです。 ● **System name TLV**－システム名TLVです。 ● **System description TLV**－システム説明TLVです。 ● **System capabilities TLV**－システム機能TLVです。 ● **Management address TLV**－管理アドレスTLVです。 ● **Congestion notification TLV**－輻輳通知TLVです。
IEEE 802.1 extended TLV	IEEE802.1組織指定TLVです。 ● **Port VLAN ID TLV**－ポートVLAN ID TLVです。 ● **Port and protocol VLAN ID TLV**－ポートのプロトコルVLAN TLVです。 ● **VLAN name TLV**－VLAN名TLVです。 ● **DCBX TLV**－DCBX TLVです。DCBX TLVはサポートしていま

フィールド	説明
	せん。 • **EVB TLV**－EVB TLVです。EVB TLVはサポートしていません。 • **Management VID TLV**－管理VID TLVです。
IEEE 802.3 extended TLV	IEEE802.3組織指定TLVです。 • **MAC-Physic TLV**－MAC物理TLVです。 • **Power via MDI TLV**－MDI経由の電力TLVです。 • **Link aggregation TLV**－リンクアグリゲーションTLVです。 • **Maximum frame size TLV**－最大フレームサイズTLVです。
LLDP-MED extend TLV	LLDP-MED TLVです。 • **Capabilities TLV**－機能TLVです。 • **Network Policy TLV**－ネットワークポリシーTLVです。 • **Extended Power-via-MDI TLV**－拡張MDI経由TLVです。 • **Location Identification TLV**－位置識別TLVです。 • **Inventory TLV**－インベントリTLVです。
Inventory TLV	インベントリTLVです。 • **Hardware Revision TLV**－ハードウェアレビジョンTLVです。 • **Firmware Revision TLV**－ファームウェアレビジョンTLVです。 • **Software Revision TLV**－ソフトウェアレビジョンTLVです。 • **Serial Number TLV**－シリアル番号TLVです。 • **Manufacturer Name TLV**－装置の製造メーカTLVです。 • **Model name TLV**－装置名TLVです。 • **Asset ID TLV**－Asset ID TLVです。

6.1.6 lldp admin-status

Syntax

Layer 2/Layer 3 Ethernet interface view：

lldp [**agent nearest-customer**] **admin-status** { **disable** | **rx** | **tx** | **txrx** }

undo lldp [**agent nearest-customer**] **admin-status**

Layer 2 aggregate interface view：

lldp agent nearest-customer admin-status { **disable** | **rx** | **tx** | **txrx** }

undo lldp agent nearest-customer admin-status

デフォルト

nearest bridge エージェントは txrx モード、nearest customer bridge エージェントは disable です。

View

Layer 2/Layer 3 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントタイプを指定します。指定しない場合、nearest bridge エージェントの動作モードを設定します。

nearest-customer: nearest customer bridge エージェントを指定します。

disable: Disable モードを指定します。Disable モードのポートは LLDP フレームの送受信ができません。

rx: Rx モードを指定します。Rx モードのポートは LLDP フレームの受信のみができます。

ポートは LLDP フレームの送受信ができます。

tx: Tx モードを指定します。Tx モードのポートは LLDP フレームの送信のみができます。

ポートは LLDP フレームの送受信ができます。

txrx: TxRx モードを指定します。TxRx モードのポートは LLDP フレームの送受信ができます。

説明

lldp admin-status コマンドは LLDP の動作モードを指定します。

undo lldp admin-status コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 の nearest customer bridge エージェントの LLDP 動作モードを Rx に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] lldp agent nearest-customer admin-status rx

6.1.7 lldp check-change-interval

Syntax

Layer 2/Layer 3 Ethernet interface view：

lldp [**agent nearest-customer**] **check-change-interval** *interval*

undo lldp [**agent nearest-customer**] **check-change-interval**

Layer 2 aggregate interface view：

lldp agent nearest-customer check-change-interval *interval*

undo lldp agent nearest-customer check-change-interval

デフォルト

無効

View

Layer 2/Layer 3 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントタイプを指定します。指定しない場合、nearest bridge エージェントの LLDP ポーリングを有効にし、ポーリング間隔を設定します。

nearest-customer: nearest customer bridge エージェントを指定します。

interval: LLDP ポーリング間隔を設定します。設定範囲は 1～30 秒です。

説明

lldp check-change-interval コマンドは LLDP ポーリングを有効にし、ポーリング間隔を設定します。

undo lldp check-change-interval コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 の nearest customer bridge エージェントの LLDP ポーリングを有効にし、ポーリング間隔を 30 秒に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] lldp agent nearest-customer check-change-interval 30

6.1.8 lldp enable

Syntax

lldp enable

undo lldp enable

デフォルト

有効

View

Layer 2/Layer 3 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

lldp enable コマンドはポートで LLDP を有効にします。

undo lldp enable コマンドはポートで LLDP を無効にします。

LLDP はグローバルとポートの両方で有効にしたときのみ適用されます。

例

GigabitEthernet 1/0/1 で LLDP を無効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] undo lldp enable

関連コマンド

lldp global enable

6.1.9 lldp encapsulation snap

Syntax

Layer 2/Layer 3 Ethernet interface view：

lldp [**agent nearest-customer**] **encapsulation snap**

undo lldp [**agent nearest-customer**] **encapsulation**

Layer 2 aggregate interface view：

lldp agent nearest-customer encapsulation snap

undo lldp agent nearest-customer encapsulation

デフォルト

Ethernet II

View

Layer 2/Layer 3 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントタイプを指定します。指定しない場合、nearest bridge エージェントの LLDP フレームのカプセル化フォーマットを設定します。

nearest-customer: nearest customer bridge エージェントを指定します。

説明

lldp encapsulation snap コマンドは LLDP フレームのカプセル化フォーマットを SNAP に設定します。

undo lldp encapsulation コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 の LLDP フレームのカプセル化フォーマットを SNAP に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] lldp encapsulation snap

6.1.10 lldp fast-count

Syntax

lldp fast-count *count*

undo lldp fast-count

デフォルト

高速 LLDP フレーム送信がトリガーされるたびに、4 つの LLDP フレームが送信されます。

View

System view

定義済みユーザロール

network-admin

パラメータ

count: 新しい隣接装置が検出される際に連続して送信される LLDP フレームの数を指定します。設定範囲は 1～8 です。

説明

lldp fast-count コマンドは新しい隣接装置が検出される際に連続して送信される LLDP フレームの数を指定します。

undo lldp fast-count コマンドはデフォルトに戻します。

例

新しい隣接装置が検出される際に連続して送信される LLDP フレームの数を 5 に設定します。

<AC> system-view

[AC] lldp fast-count 5

6.1.11 lldp global enable

Syntax

lldp global enable

undo lldp global enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

lldp global enable コマンドはグローバルで LLDP を有効にします。

undo lldp global enable コマンドはグローバルで LLDP を無効にします。

LLDP はグローバルとポートの両方で有効にしたときのみ適用されます。

例

グローバルで LLDP を無効にします。

<AC> system-view

[AC] undo lldp global enable

関連コマンド

lldp enable

6.1.12 lldp hold-multiplier

Syntax

lldp hold-multiplier *value*

undo lldp hold-multiplier

デフォルト

4

View

System view

定義済みユーザロール

network-admin

パラメータ

value: TTL の乗数を設定します。設定範囲は 2～10 です。

説明

lldp hold-multiplier コマンドは TTL の乗数を設定します。

undo lldp hold-multiplier コマンドはデフォルトに戻します。

LLDPDU で送信される TTL TLV は、受信装置で保存される装置情報の保存期間を決定します。

TTL の乗数を設定することにより、隣接装置に送信する TTL の設定を行うことができます。隣接装置についての情報の TTL は以下の式によって定義されます。

TTL ＝min（65535, （TTL の乗数 x LLDP フレームの送信間隔 ＋ 1））

TTL は最大 65535 秒です。65535 より大きい場合、65535 秒に丸められます。

例

TTL の乗数を 6 に設定します。

<AC> system-view

[AC] lldp hold-multiplier 6

関連コマンド

lldp timer tx-interval

6.1.13 lldp management-address-format string

Syntax

Layer 2/Layer 3 Ethernet interface view：

lldp [**agent nearest-customer**] **management-address-format string**

undo lldp [**agent nearest-customer**] **management-address-format**

Layer 2 aggregate interface view：

lldp agent nearest-customer management-address-format string

undo lldp agent nearest-customer management-address-format

デフォルト

numeric 形式

View

Layer 2/Layer 3 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントタイプを指定します。指定しない場合、nearest bridge エージェントの管理アドレスのカプセル化フォーマットを設定します。

nearest-customer: nearest customer bridge エージェントを指定します。

説明

lldp management-address-format string コマンドは管理アドレスの TLV のカプセル化フォーマットを string 形式に設定します。

undo lldp management-address-format コマンドはデフォルトに戻します。

管理アドレスの LLDP 隣接は同じカプセル化フォーマットを使用する必要があります。

例

GigabitEthernet 1/0/1 の nearest customer bridge エージェントで管理アドレスの TLV のカプセル化フォーマットを string 形式に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] lldp agent nearest-customer management-address-format string

6.1.14 lldp notification remote-change enable

Syntax

Layer 2/Layer 3 Ethernet interface view：

lldp [**agent nearest-customer**] **notification remote-change enable**

undo lldp [**agent nearest-customer**] **notification remote-change enable**

Layer 2 aggregate interface view：

lldp agent nearest-customer notification remote-change enable

undo lldp agent nearest-customer notification remote-change enable

デフォルト

無効

View

Layer 2/Layer 3 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントタイプを指定します。指定しない場合、nearest bridge エージェントの LLDP トラップを有効にします。

nearest-customer: nearest customer bridge エージェントを指定します。

説明

lldp notification remote-change enable コマンドは LLDP トラップを有効にします。

undo lldp notification remote-change enable コマンドは LLDP トラップを無効にします。

例

GigabitEthernet 1/0/1 の nearest customer bridge エージェントの LLDP トラップを有効にします。

<AC> system-view

[AC] interface GigabitEthernet 1/0/1

[AC-GigabitEthernet1/0/1] lldp agent nearest-customer notification remote-change enable

6.1.15 lldp timer notification-interval

Syntax

lldp timer notification-interval *interval*

undo lldp timer notification-interval

デフォルト

30 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: LLDP トラップと LLDP-MED トラップの送信間隔を指定します。設定範囲は 5～3600 秒です。

説明

lldp timer notification-interval コマンドはLLDP トラップと LLDP-MED トラップの送信間隔を設定します。

undo lldp timer notification-interval コマンドはデフォルトに戻します。

例

LLDP トラップと LLDP-MED トラップの送信間隔を 8 秒に設定します。

<AC> system-view

[AC] lldp timer notification-interval 8

6.1.16 lldp timer reinit-delay

Syntax

lldp timer reinit-delay *delay*

undo lldp timer reinit-delay

デフォルト

2 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

delay: LLDP の再初期化の遅延時間を設定します。設定範囲は 1～10 秒です。

説明

lldp timer reinit-delay コマンドは LLDP の再初期化の遅延時間を設定します。

undo lldp timer reinit-delay コマンドはデフォルトに戻します。

例

LLDP の再初期化の遅延時間を 4 秒に設定します。

<AC> system-view

[AC] lldp timer reinit-delay 4

6.1.17 lldp timer tx-interval

Syntax

lldp timer tx-interval *interval*

undo lldp timer tx-interval

デフォルト

30 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: LLDP フレームの送信間隔を設定します。設定範囲は 5～32768 秒です。

説明

lldp timer tx-interval コマンドは LLDP フレームの送信間隔を設定します。

undo lldp timer tx-interval コマンドはデフォルトに戻します。

例

LLDP フレームの送信間隔を 20 秒に設定します。

<AC> system-view

[AC] lldp timer tx-interval 20

6.1.18 lldp tlv-enable

Syntax

Layer 2 Ethernet interface view：

- nearest bridge エージェント

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all | port-vlan-id** | **link-aggregation** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all | port-vlan-id** | **link-aggregation** | **protocol-vlan-id** | **vlan-name** | **management-vid** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** } }

- nearest customer bridge エージェント

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all | port-vlan-id** | **link-aggregation** } }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all | port-vlan-id** | **link-aggregation** } }

Layer 2 aggregate interface view：

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

デフォルト

Ethernet インタフェースのデフォルトを以下に示します。

- nearest bridge エージェントは以下のタイプの LLDP TLV を除いたすべての LLDP TLV を送信します。
  - 位置識別 TLV
  - ポートのプロトコル VLAN ID TLV
  - VLAN 名 TLV
  - 管理 VLAN ID TLV
  - Energy-Efficient Ethernet TLV
- nearest customer bridge エージェントは basic TLV と IEEE802.1 組織指定 TLV を送信します。

レイヤ 3 Ethernet インタフェースのデフォルトを以下に示します。

- nearest bridge エージェントは、ネットワークポリシーTLV と Energy-Efficient Ethernet TLV を除いたすべての LLDP TLV（IEEE802.1 組織指定の TLV 中のリンクアグリゲーション TLV のみ）を送信します。
- nearest customer bridge エージェントは basic TLV と IEEE802.1 組織指定 TLV（リンクアグリゲーション TLV のみ）を送信します。

レイヤ 2 アグリゲートインタフェースのデフォルトを以下に示します。

- nearest bridge エージェントは存在しません。
- nearest customer bridge エージェントは basic TLV と IEEE802.1 組織指定 TLV（ポートのプロトコル VLAN ID TLV、VLAN 名 TLV、管理 VLAN ID TLV のみ）を送信します。

View

Layer 2/Layer 3 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントタイプを指定します。Ethernet インタフェースであるいはマネジメント Ethernet インタフェースでパラメータを指定しない場合、nearest bridge エージェントの通知可能な TLV のタイプを設定します。

nearest-customer: nearest customer bridge エージェントを指定します。

all: 指定したタイプのすべての TLV を送信します。

- 以下の TLV を送信するインタフェースを有効にします。
  - **basic-tlv** で **all** が指定された場合、すべての basic LLDP TLV を送信します。
  - **dot1-tlv** で **all** が指定された場合、すべての 802.1 組織指定 LLDP TLV を送信します。
  - **dot3-tlv** で **all** が指定された場合、すべての 802.3 組織指定 LLDP TLV を送信します。
- **med-tlv** で **all** が指定された場合、位置識別 TLV を除くすべての LLDP-MED TLV を送信します。

basic-tlv: basic LLDP TLV を送信します。

management-address-tlv [*ip-address* | **interface loopback** *interface-number*]:

管理アドレス TLV を送信します。*ip-address* は送信される管理アドレスを指定します。デフォルトを以下に示します。**loopback** *interface-number* パラメータはループバックインタフェースの IP アドレスを指定します。デフォルトを以下に示します。

- レイヤ 2 Ethernet インタフェースあるいはアグリゲートインタフェースで、管理アドレスは以下の要件に一致する VLAN インタフェースのプライマリ IP アドレスです。
  - up 状態のインタフェースです。
  - 一致する VLAN ID がポートで許可された VLAN でもっとも小さい値です。

  許可された VLAN の VLAN インタフェースに IP アドレスが設定されていない、あるいはすべての VLAN インタフェースが down している場合、ポートの MAC アドレスが送信されます。
- レイヤ 3 イーサネットインタフェースの場合、次の条件が満たされると、ポートの IPv4 アドレスが送信されます。
  - *ip-address* 引数が設定されていません。
  - 指定されたループバックインタフェースに IPv4 アドレスがないか、または指定されたループバックインタフェースが存在しません。

  ポートに IP アドレスがない場合、ポートの MAC アドレスが送信されます。

undo コマンドを実行するとき、以下の処理を行います。

- *ip-address*、および **interface loopback** *interface-number* を指定しない場合、ポートは管理アドレス TLV を送信しません。
- ip-address、または **interface loopback** *interface-number* を指定すると、ポートはデフォルトの管理アドレス TLV を送信します。

port-description: ポート説明 TLV を送信します。

system-capability: システム機能 TLV を送信します。

system-description: システム説明 TLV を送信します。

system-name: システム名 TLV を送信します。

dot1-tlv: IEEE 802.1 組織指定 LLDP TLV を送信します。

congestion-notification: QCN TLV を送信します。nearest bridge LLDP インタフェースだけが QCN TLV を送信できます。

port-vlan-id: ポート VLAN ID TLV を送信します。

protocol-vlan-id [*vlan-id*]: ポートとプロトコル VLAN ID TLV を送信します。*vlan-id* は送信される TLV の VLAN ID を指定します。VLAN ID の設定範囲は 1～4094 です。デフォルトはポートでもっとも小さい VLAN ID です。

vlan-name [*vlan-id*]: VLAN 名 TLV を送信します。*vlan-id* は送信される TLV の VLAN ID を指定します。VLAN ID の設定範囲は 1～4094 です。デフォルトはポートでもっとも小さい VLAN ID です。VLAN ID を指定せず、ポートが VLAN に割り当てられていない場合、ポートの PVID がアドバタイズされます。

management-vid [*mvlan-id*]: 管理 LAN ID TLV を送信します。*mvlan-id* は送信される TLV の管理 VLAN ID を指定します。管理 VLAN ID の設定範囲は 1～4094 です。管理 VLAN ID が指定されない場合、0 が送信されます。0 は LLDP エージェントが管理 VLAN ID で設定されないことを示します。

dot3-tlv: IEEE802.3 組織指定 LLDP TLV を送信します。

link-aggregation: リンクアグリゲーション TLV を送信します。

mac-physic: MAC/PHY の設定/状態 TLV（MAC/PHY configuration/status TLV）を送信します。

max-frame-size: 最大フレームサイズ TLV を送信します。

power: MDI TLV の電力と電力ステートフル制御 TLV を送信します。

med-tlv: LLDP-MED TLV を送信します。

capability: LLDP-MED 機能 TLV を送信します。

inventory: ハードウェアレビジョン、ファームウェアレビジョン、ソフトウェアレビジョン、シリアル番号、装置名、製品名、assert ID の TLV を送信します。

location-id: 位置識別 TLV を送信します。

civic-address: 位置識別 TLV のネットワーク装置に関する一般的なアドレス情報を挿入します。

device-type: 装置タイプを設定します。設定範囲は 0～2 です。

- 0 は DHCP サーバを指定します。
- 1 はスイッチを指定します。
- 2 は LLDP-MED エンドポイントを指定します。

country-code: ISO 3166 で定義された国別コードを設定します。

{ *ca-type ca-value* }&<1-10>: アドレス情報を設定します。*ca-type* はアドレス情報タイプを示します。設定範囲は 0～255 です。*ca-value* はアドレス情報を示します。設定範囲は 1～250 文字です。&<1-10>は *ca-type ca-value* を最大 10 まで指定できることを示します。

elin-address: 位置識別 TLV に緊急用電話番号を挿入します。

tel-number: 緊急用電話番号を設定します。設定範囲は 10～25 です。

network-policy [*vlan-id*]: ネットワークポリシーTLV を送信します。音声 VLAN ID の設定範囲は 1～4094 です。

power-over-ethernet: 拡張 MDI 経由の電力 TLV（power-via-MDI TLV）を送信します。

説明

lldp tlv-enable コマンドは通知可能な TLV のタイプを設定します。

undo lldp tlv-enable コマンドは TLV の指定されたタイプの送信を無効にします。

nearest bridge エージェントはアグリゲートインタフェースでサポートしていません。

all パラメータを指定しないで、TLV の複数のタイプを送信することができます。

MAC/PHY 設定/状態 TLV が送信されない場合、通知可能であるにも関わらず、LLDP-MED TLV が送信されません。LLDP-MEDTLV が送信されない場合、通知可能であるにも関わらず、他の LLDP-MED TLV が送信されません。

IEEE802.1 組織指定 LLDP TLV のプロトコル VLAN ID、VLAN 名 TLV、管理 VLAN ID TLV は nearest bridge エージェントでのみ設定できます。

例

GigabitEthernet 1/0/1 の IEEE802.1 組織指定 TLV のリンクアグリゲーション TLV を送信するため、GigabitEthernet 1/0/1 の nearest customer bridge エージェントを有効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] lldp agent nearest-customer tlv-enable dot1-tlv link-aggregation

目次

このセクションのページは **4-x-x** です。

7 章 レイヤ 2 フォワーディングの設定 7-1
7.1 標準レイヤ 2 フォワーディングの設定コマンド 7-1
7.1.1 display mac-forwarding statistics 7-1
7.1.2 reset mac-forwarding statistics 7-3
7.2 高速レイヤ 2 フォワーディングの設定コマンド 7-4
7.2.1 display mac-forwarding cache ip 7-4
7.2.2 display mac-forwarding cache ip fragment 7-5

7章 レイヤ 2 フォワーディングの設定

7.1 標準レイヤ2フォワーディングの設定コマンド

7.1.1 display mac-forwarding statistics

Syntax

display mac-forwarding statistics [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 種別と数字でインタフェースを指定します。本オプションを指定しない場合、コマンドは全インタフェースのフォワーディング統計情報を表示します。

説明

レイヤ 2 フォワーディング統計情報を表示するには、**display mac-forwarding statistics** コマンドを使用します。

例

全インタフェースのレイヤ 2 フォワーディング統計情報を表示します。

<AC> display mac-forwarding statistics

```
Input:
  Sum:             888       Unknown Unicast:   0
  Broadcast:        0         Multicast:        0
  Filtered:         0         STP discarded:    0
  Service dropped:  0          Source dropped:   0
  Unknown dropped:  0          Learning dropped: 0
  Attack dropped:   0          Suppress dropped: 0
Deliver:
  Sum:             111       L2 protocol:      11
  Local MAC address: 100
Output:
  Sum:             666       Filtered:         0
```

```
  Blackhole dropped: 0          STP discarded:     0
  Service dropped:   0          Dest MAC dropped:  0
```

GigabitEthernet 1/0/1 インタフェースのレイヤ 2 フォワーディング統計情報を表示します。

<AC> display mac-forwarding statistics interface gigabitethernet 1/0/1

```
GigabitEthernet 1/0/1:
Input frames: 100    Output frames:100
Filtered:     0
```

表 7-1 コマンド出力

フィールド	説明
Input	インバウンドイーサネットフレームの統計情報
Sum	受信したイーサネットフレームの総数
Filtered	802.1Q VLANインバウンドフィルタリングルールによってフィルタリングされたイーサネットフレームの数
STP discarded	STPでブロックされたポートにおける破棄されたインバウンドイーサネットフレームの数
Service dropped	インバウンドサービス機能によって破棄されたイーサネットフレームの数
Source dropped	送信元MACアドレスがAll 0、マルチキャスト、ブロードキャストMACアドレスであるために破棄されたイーサネットフレームの数
Unknown dropped	不明な送信元MACアドレスのフレームのフォワーディングが装置で無効になっているために破棄されたイーサネットフレームの数
Learning dropped	MACアドレス学習数が上限に達した後に、不明な送信元MACアドレスのフレームのフォワーディングが装置で無効になっているために破棄されたイーサネットフレームの数
Attack dropped	送信元MACアドレスに基づいて機能によって破棄されたアタックイーサネットフレームの数
Suppress dropped	ストーム抑止によって破棄されたイーサネットフレームの数
Broadcast	受信したブロードキャストイーサネットフレームの数
Multicast	受信したマルチキャストイーサネットフレームの数
Unknown Unicast	受信した不明なユニキャストイーサネットフレームの数
Deliver	CPUに送出したイーサネットフレームの統計情報
Sum	CPUに送出したイーサネットフレームの総数

フィールド	説明
L2 protocol	CPUに送出したレイヤ2プロトコルイーサネットフレームの数
Local MAC address	宛先MACアドレスがローカルレイヤ3 VLANインタフェースのMACアドレスであるイーサネットフレームの数
Output	アウトバウンドイーサネットフレームの統計情報
Sum	イーサネットフレームの総数
Blackhole dropped	ブラックホールMACアドレス宛てのために破棄されたイーサネットフレームの数
Filtered	802.1Q VLANアウトバウンドフィルタリングルールによってフィルタリングされたイーサネットフレームの数
STP discarded	STPでブロックされたポートにおける破棄されたアウトバウンドイーサネットフレームの数
Service dropped	アウトバウンドサービス機能によって破棄されたイーサネットフレームの数
Dest MAC dropped	宛先MACアドレスに基づいて機能によって破棄されたイーサネットフレームの数
Input frames	インタフェースで受信したイーサネットフレームの数
Output frames	インタフェースで送信したイーサネットフレームの数
Filtered	他VLANからのものであるためにフィルタリングされたイーサネットフレームの数

7.1.2 reset mac-forwarding statistics

Syntax

reset mac-forwarding statistics

View

User view

定義済みユーザロール

network-admin

network-operator

説明

レイヤ 2 フォワーディング統計情報をクリアするには、**reset mac-forwarding statistics** コマンドを使用します。

例

レイヤ 2 フォワーディング統計情報をクリアします。

<AC> reset mac-forwarding statistics

7.2 高速レイヤ2フォワーディングの設定コマンド

7.2.1 display mac-forwarding cache ip

Syntax

display mac-forwarding cache ip [*ip-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip-address: IPv4 アドレスを指定します。指定しない場合、本コマンドはすべての IPv4 高速フォワーディングエントリを表示します。

説明

IPv4 高速フォワーディングエントリを表示するには、**display mac-forwarding cache ip** コマンドを使用します。

例

すべての IPv4 高速フォワーディングエントリを表示します。

<AC> display mac-forwarding cache ip

```
Total number of mac-forwarding entries: 2
SIP           SPort DIP           DPort Pro Input_If    Output_If   VLAN
1.1.1.2        99    1.1.1.1        2048  1   GE1/0/1     GE1/0/1     2
1.1.1.1        98    1.1.1.2        2012  1   GE1/0/2     GE1/0/2     2
```

表 7-2 コマンド出力

フィールド	説明
Total number of mac-forwarding entries	IPv4高速フォワーディングエントリの総数
SIP	送信元IPv4アドレス

フィールド	説明
SPort	送信元ポート番号
DIP	宛先IPv4アドレス
DPort	宛先ポート番号
Pro	プロトコル番号
Input_If	入力インタフェースのタイプと番号 高速フォワーディングに関係する入力インタフェ―スがない場合、本フィールドはN/Aと表示されます。 利用可能な入力インタフェースがない場合、本フィールドはハイフン（-）が表示されます。
Output_If	出力インタフェースのタイプと番号 高速フォワーディングに関係する出力インタフェ―スがない場合、本フィールドはN/Aと表示されます。 利用可能な出力インタフェースがない場合、本フィールドはハイフン（-）が表示されます。
VLAN	VLAN ID

7.2.2 display mac-forwarding cache ip fragment

Syntax

display mac-forwarding cache ip fragment [*ip-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip-address: IPv4 アドレスを指定します。指定しない場合、本コマンドはすべての IPv4 フラグメント高速フォワーディングエントリを表示します。

説明

IPv4 フラグメント高速フォワーディングエントリを表示するには、**display mac-forwarding cache ip fragment** コマンドを使用します。

例

すべての IPv4 フラグメント高速フォワーディングエントリを表示します。

<AC> display mac-forwarding cache ip fragment

```
Total number of fragment mac-forwarding entries: 2
SIP           SPort DIP           DPort Pro Input_If    ID     VLAN
1.1.1.1        117  1.1.1.2        0    1   GE1/0/1     2828   1
1.1.1.2        110  1.1.1.1        67   17  GE1/0/2     2322   1
```

表 7-3 コマンド出力

フィールド	説明
Total number of fragment mac-forwarding entries	IPv4フラグメント高速フォワーディングエントリの総数
SIP	送信元IPv4アドレス
SPort	送信元ポート番号
DIP	宛先IPv4アドレス
DPort	宛先ポート番号
Pro	プロトコル番号
Input_If	入力インタフェースのタイプと番号 高速フォワーディングに関係する入力インタフェ―スがない場合、本フィールドはN/Aと表示されます。 利用可能な入力インタフェースがない場合、本フィールドはハイフン（-）が表示されます。
ID	フラグメンテーションID
VLAN	VLAN ID

QX-W2230AC アクセスコントローラ

コマンドマニュアル

5. IP サービス

本マニュアルは以下に示す章で構成されています。

01-ARP
02-gratuitous ARP
03-proxy ARP
04-IP アドレス
05-DHCP の概要
06-DHCP サーバ
07-DHCP リレー
08-DHCP クライアント
09-DHCP スヌーピング
10-BOOTP
11-DNS
12-IP パフォーマンスの最適化
13-NAT

目次

このセクションのページは **5-x-x** です。

1 章 ARP 1-1
1.1 ARP 設定コマンド 1-1
1.1.1 arp check enable 1-1
1.1.2 arp check log enable 1-2
1.1.3 arp max-learning-num 1-3
1.1.4 arp static 1-4
1.1.5 arp timer aging 1-5
1.1.6 display arp 1-6
1.1.7 display arp ip-address 1-9
1.1.8 display arp timer aging 1-10
1.1.9 reset arp 1-10

1章 ARP

1.1 ARP設定コマンド

1.1.1 arp check enable

Syntax

arp check enable

undo arp check enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

arp check enable コマンドはダイナミック ARP エントリチェックを有効にします。

undo arp check enable コマンドはダイナミック ARP エントリチェックを無効にします。

ダイナミック ARP エントリチェック機能は、マルチキャスト MAC アドレスを含むダイナミック ARP エントリのサポート状態にある装置を無効にします。その装置は、マルチキャストMACアドレスを含むダイナミックARPエントリを学習することができません。マルチキャスト MAC アドレスを含むスタティック ARP エントリを手動で追加する事は出来ません。

ダイナミック ARP エントリチェック機能が無効の場合、マルチキャスト MAC アドレスを含む ARP エントリがサポートされます。その装置は、ユニキャスト MAC アドレスをソースとする ARP パケットより供給されるマルチキャスト MAC アドレスを含むダイナミック ARP エントリを学習できます。また、マルチキャスト MAC アドレスを含むスタティック ARP エントリを手動で追加できます。

例

ダイナミック ARP エントリチェックを有効にします。

<AC> system-view

[AC] arp check enable

1.1.2 arp check log enable

Syntax

arp check log enable

undo arp check log enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

arp check log enable コマンドは ARP ロギング機能を有効にします。

undo arp check log enable コマンドは ARP ロギング機能を無効にします。

ARP が IP アドレスを正常に解決できないとき、装置で ARP イベントをロギングします。以下の ARP イベントをロギングできます。

- インタフェースで proxy ARP が無効な場合、受信した ARP パケットの宛先 IP アドレスが、受信インタフェースの IP アドレス、あるいは NAT 後のパブリック IP アドレスのいずれでもない時。
- 受信した ARP エントリの送信元 IP アドレスが、受信インタフェースの IP アドレス、あるいは NAT 後のパブリック IP アドレスと重複している時。

装置は Information Center に ARP ログメッセージを送信します。Information Center のログ出力ルールを設定するため、**info-center source** コマンドを使用します。Information Center の詳細はオペレーションマニュアルのセクション 11 *システム管理* の *"Information Center"* を参照してください。

装置は非常に多くの ARP ログを作成することができます。システムリソースを保護するため、ARP イベントの調査、トラブルシューティングを行っているときのみ、ARP ロギング機能を有効にしてください。

例

ARP ロギング機能を有効にします。

<AC> system-view

[AC] arp check log enable

1.1.3 arp max-learning-num

Syntax

arp max-learning-num *max-number*

undo arp max-learning-num

デフォルト

3072

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

max-number: インタフェースが学習できるダイナミック ARP エントリの最大数を指定します。範囲は 0～3072 です。

説明

arp max-learning-num コマンドはインタフェースが学習できるダイナミック ARP エントリの最大数を設定します。

undo arp max-learning-num コマンドはデフォルトに戻します。

インタフェースはダイナミックに ARP エントリを学習可能です。多すぎる ARP エントリを保持することを防ぐため、インタフェースが学習できるダイナミック ARP エントリの最大数を設定することができます。設定した最大数に到達すると、インタフェースは ARP エントリの学習を停止します。

0 に設定した場合、ダイナミック ARP エントリの学習を無効にします。

例

VLAN インタフェース 40 が学習できるダイナミック ARP エントリの最大数を 500 に設定します。

<AC> system-view

[AC] interface vlan-interface 40

[AC-Vlan-interface40] arp max-learning-num 500

GigabitEthernet 1/0/1 が学習できるダイナミック ARP エントリの最大数を 1000 に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] arp max-learning-num 1000

レイヤ 2 アグリゲートインタフェース Bridge-aggregation 1 が学習できるダイナミック ARP エントリの最大数を 1000 に設定します。

<AC> system-view

[AC] interface bridge-aggregation 1

[AC-Bridge-Aggregation1] arp max-learning-num 1000

1.1.4 arp static

Syntax

arp static *ip-address mac-address* [*vlan-id interface-type interface-number*]

undo arp *ip-address*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: スタティック ARP エントリの IP アドレスを指定します。

mac-address: スタティック ARP エントリの MAC アドレスを指定します。形式は H-H-H です。

vlan-id: ARP エントリが所属する VLAN の ID を指定します。設定範囲は 1～4094 です。

interface-type interface-number: インタフェースのタイプと番号を指定します。インタフェースは Ethernet インタフェースかアグリゲートインタフェースが選択できます。

説明

arp static コマンドはスタティック ARP エントリを設定します。

undo arp コマンドはスタティック ARP エントリを削除します。

スタティック ARP エントリは手動で設定し維持します。スタティック ARP エントリはエージアウトしません。またダイナミック ARP エントリに上書きされることはありません。

スタティック ARP エントリはロングスタティック ARP エントリとショートスタティック ARP エントリに分類されます。

解決済みのショートスタティック ARP エントリは特定のイベントで未解決になります。たとえば、出力インタフェースがダウンしたとき、あるいは対応する VLAN や VLAN インタフェースが削除されたとき、未解決になります。

ロングスタティック ARP エントリは解決の場合と未解決の場合に分類されます。未解決のロングスタティック ARP エントリの場合、パケットの転送は行われません。ロングスタティック ARP エントリは以下の状態で未解決となり、パケットの転送に使用することができません。

- 対応する VLAN インタフェースあるいは出力インタフェースがダウンしている時。
- エントリの IP アドレスがローカル IP アドレスと競合している時。
- ローカルインタフェースに、ARP エントリの IP アドレスと同一のサブネットの IP アドレスがない時。

vlan-id interface-type interface-number を指定した場合、以下の制限とガイドラインに従ってください。

- インタフェースは Ethernet インタフェースにする必要があります。
- VLAN、VLAN インタフェースはすでに作成されている必要があります。Ethernet インタフェースは VLAN に属している必要があります。
- VLAN インタフェースの IP アドレスと *ip-address* パラメータで指定された IP アドレスは同一ネットワークにする必要があります。
- VLAN あるいは VLAN インタフェースが削除された場合、VLAN のロングスタティック ARP エントリは削除されます。

例

IP アドレスが 202.38.10.2、MAC アドレスが 0000-0001-0000、出力インタフェースが VLAN10 の GigabitEthernet 1/01 であるロングスタティック ARP エントリを設定します。

<AC> system-view

[AC] arp static 202.38.10.2 0000-0001-0000 10 gigabitethernet 1/0/1

関連コマンド

- **display arp**
- **reset arp**

1.1.5 arp timer aging

Syntax

arp timer aging *aging-time*

undo arp timer aging

デフォルト

20 分

View

System view

定義済みユーザロール

network-admin

パラメータ

aging-time: ダイナミック ARP エントリのエージングタイマを設定します。設定範囲は 1～1440 分です。

説明

arp timer aging コマンドはダイナミック ARP エントリのエージングタイマを設定します。

undo arp timer aging コマンドはデフォルトに戻します。

ARP テーブル上の各ダイナミック ARP エントリは有効期限を持っています。有効期限はエージングタイマと呼ばれ、有効期限内にダイナミック ARP エントリがアップデートされるたびに、エージングタイマはリセットされます。有効期限切れになる前に更新されなかったダイナミック ARP エントリは、ARP テーブルから削除されます。

必要に応じてダイナミック ARP エントリのエージングタイマを設定してください。たとえば proxy ARP を設定するとき、不正なダイナミック ARP エントリが時間内に削除されるようにエージングタイマを短い値に設定してください。

例

ダイナミック ARP エントリのエージングタイマを 10 分に設定します。

<AC> system-view

[AC] arp timer aging 10

関連コマンド

display arp timer aging

1.1.6 display arp

Syntax

display arp [[**all** | **dynamic** | **static**] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count** | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての ARP エントリを表示します。

dynamic: ダイナミック ARP エントリを表示します。

static: スタティック ARP エントリを表示します。

vlan *vlan-id*: 指定した VLAN の ARP エントリを表示します。設定範囲は 1～4094 です。

interface *interface-type interface-number*: *interface-type interface-number* で指定されたインタフェースの ARP エントリを表示します。

count: ARP エントリ数を表示します。

verbose: ARP エントリの詳細情報を表示します。

説明

display arp コマンドは ARP エントリを表示します。

このコマンドは IP アドレス、MAC アドレス、VLAN ID、出力インタフェース、エントリタイプ、エージングタイマを含む ARP エントリの情報を表示します。

パラメータを指定しない場合、すべての ARP エントリを表示します。

例

すべての ARP エントリを表示します。

<AC> display arp all

```
Type: S-Static   D-Dynamic   O-Openflow   R-Rule   I-Invalid
IP address      MAC address    SVID    Interface             Aging Type
192.168.100.1   5cdd-7081-2a2d 1       GE1/0/1               11    D
192.168.100.3   6805-ca17-4a5e 1       GE1/0/1               14    D
192.168.100.4   a036-9f42-b774 1       GE1/0/1               17    D
192.168.100.8   7446-a08f-0ca2 1       GE1/0/1               16    D
192.168.100.18  f092-1cef-677f 1       GE1/0/1               10    D
192.168.100.40  2c41-389f-9b97 1       GE1/0/1               2     D
192.168.100.66  000f-e212-510e 1       GE1/0/1               2     D
192.168.100.197 3ce5-a618-e6a8 1       GE1/0/1               11    D
192.168.100.199 2222-1111-baaa 1       GE1/0/1               11    D
192.168.100.201 000f-1e2e-0a11 1       GE1/0/1               11    D
```

すべての ARP エントリの詳細情報を表示します。

<AC> display arp all verbose

```
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP Address      : 1.1.1.1         SVID/CVID: 1/--         Aging   : --
```

```
MAC Address     : 02e0-f102-0023   Type     : S          Nickname: 0x0000
Interface       : GE1/0/1
VPN Instance    : [No Vrf]
```

すべての ARP エントリの数を表示します。

<AC> display arp all count

```
 Total number of entries : 10
```

表 1-1 コマンド出力

フィールド	説明
IP Address	ARPエントリのIPアドレスです。
MAC Address	ARPエントリのMACアドレスです。
SVLAN/VSI	ARPエントリが所属するVSIのインデックス、あるいはSVLANのIDです。以下のどちらかの状態である場合、--と表示されます。 ● ARPエントリが未解決のショートスタティックARPエントリです。 ARPエントリの出力インタフェースがSVLANやVSIに所属していません。
SVLAN/CVLAN	ARPエントリが所属するCVLAN、あるいはSVLANのIDです。以下のどちらかの状態である場合、--と表示されます。 ● ARPエントリが未解決のショートスタティックARPエントリです。 ● ARPエントリの出力インタフェースがSVLANやCVLANに所属していません。
Interface	● ARPエントリの出力インタフェースです。ARPエントリが未解決のショートスタティックARPエントリである場合、--と表示されます。
Aging	ダイナミックARPエントリのエージングタイマです。単位は分です。--はエージングタイマが不明、あるいはエージングタイマが有効期限切れであることを示します。
Type	ARPエントリのタイプです。 ● **D**–ダイナミックARPエントリです。 ● **S**–スタティックARPエントリです。 ● **O**–オープンフロー。通常のソフトウェアでは未搭載。 ● **R**–ロール。 ● **I**–無効なARPエントリです。
NickName	ARPエントリのニックネームです。ニックネームは４ケタの16進数です。例えば、0x012a。

フィールド	説明
Total number of entries	ARPエントリ数です。
IP Address	ARPエントリのIPアドレスです。

関連コマンド

- **arp static**
- **reset arp**

1.1.7 display arp ip-address

Syntax

display arp *ip-address* [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip-address: 指定した IP アドレスの ARP エントリを表示します。

verbose: ARP エントリの詳細情報を表示します。

説明

display arp ip-address コマンドは IP アドレスの ARP エントリを表示します。

ARP エントリの情報は IP アドレス、MAC アドレス、VLAN ID、出力インタフェース、エントリタイプ、エージングタイマを含みます。

例

IP アドレス 192.168.100.1 の ARP エントリを表示します。

<AC> display arp 192.168.100.1

```
  Type: S-Static    D-Dynamic    O-Openflow   R-Rule   I-Invalid
IP address      MAC address    SVID    Interface             Aging Type
192.168.100.1   5cdd-7081-2a2d 1       GE1/0/1               3     D
```

関連コマンド

- **arp static**

- **reset arp**

1.1.8 display arp timer aging

Syntax

display arp timer aging

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display arp timer aging コマンドはダイナミック ARP エントリのエージングタイマを表示します。

例

ダイナミック ARP エントリのエージングタイマを表示します。

<AC> display arp timer aging

```
Current ARP aging time is 10 minute(s)
```

関連コマンド

arp timer aging

1.1.9 reset arp

Syntax

reset arp { **all** | **dynamic** | **interface** *interface-type interface-number* | **static** }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべての ARP エントリを削除します。

dynamic: すべてのダイナミック ARP エントリを削除します。

static: すべてのスタティック ARP エントリを削除します。

interface *interface-type interface-number*: *interface-type interface-number* で指定されたインタフェースの ARP エントリを削除します。指定しない場合、すべてのインタフェースの ARP エントリを削除します。

説明

reset arp コマンドは ARP テーブルから ARP エントリを削除します。

例

すべてのスタティック ARP エントリを削除します。

<AC> reset arp static

関連コマンド

- **arp static**
- **display arp**

目次

このセクションのページは **5-x-x** です。

2 章 Gratuitous ARP 2-1
2.1 Gratuitous ARP 設定コマンド 2-1
2.1.1 arp ip-conflict log prompt.....2-1
2.1.2 arp send-gratuitous-arp.....2-1
2.1.3 gratuitous-arp mac-change retransmit.....2-3
2.1.4 gratuitous-arp-learning enable 2-4
2.1.5 gratuitous-arp-sending enable.....2-4

2章 Gratuitous ARP

2.1 Gratuitous ARP設定コマンド

2.1.1 arp ip-conflict log prompt

Syntax

arp ip-conflict log prompt

undo arp ip-conflict log prompt

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

arp ip-conflict log prompt コマンドは、IP 重複の通知を有効にします。

undo arp ip-conflict log prompt コマンドはデフォルトに戻します。

受信した ARP パケットの送信元 IP アドレスを使用する場合、装置は以下のように動作します。

- gratuitous ARP 要求を送信します。
- 重複に関する ARP 応答を装置が受信した後に、エラーメッセージを表示します。

例

装置で IP 重複の通知を有効にします。

<AC> system-view

[AC] arp ip-conflict log prompt

2.1.2 arp send-gratuitous-arp

Syntax

arp send-gratuitous-arp [**interval** *interval*]

undo arp send-gratuitous-arp

デフォルト

無効

View

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

interval *interval*: gratuitous ARP パケットを送信する送信間隔を設定します。設定範囲は 200～200000 ミリ秒です。なお、ARP パケットを送信する送信間隔のデフォルト値は、2000 ミリ秒です。

説明

arp send-gratuitous-arp コマンドはインタフェースで gratuitous ARP パケットの定期送信を有効にし、送信間隔を設定します。

undo arp send-gratuitous-arp コマンドはインタフェースで gratuitous ARP パケットを定期的に送信することを無効にします。

このコマンドは有効にしたインタフェースのデータリンクレイヤの状態が up で、且つ IP アドレスが設定されているときのみ、適用されます。

この機能はインタフェースのプライマリ IP アドレス、あるいは手動で設定されたセカンダリ IP アドレスの gratuitous ARP 要求のみ送信することができます。プライマリ IP アドレスは手動または自動で設定することができますが、セカンダリ IP アドレスは手動で設定する必要があります。

gratuitous ARP パケットの送信間隔を変更すると、次の送信間隔から設定が適用されます。

gratuitous ARP パケットの送信間隔は以下の状況によって、設定した値よりも長くなります。

- 複数のインタフェースで有効にされた場合
- 各インタフェースで複数のセカンダリ IP アドレスが設定された場合
- 優先する状況で短い送信間隔を設定した場合

例

VLAN インタフェース 2 で gratuitous ARP パケットの定期送信を有効にし、送信間隔を 300 ミリ秒に設定します。

<AC> system-view

[AC] interface vlan-interface 2

[AC-Vlan-interface2] arp send-gratuitous-arp interval 300

2.1.3 gratuitous-arp mac-change retransmit

Syntax

gratuitous-arp mac-change retransmit *times* **interval** *seconds*

undo gratuitous-arp mac-change retransmit

デフォルト

装置は MAC アドレス変更を通知するための gratuitous ARP パケットを 1 回だけ送信します。

View

System view

定義済みユーザロール

network-admin

パラメータ

times: gratuitous ARP パケットを再送信する回数を設定します。設定範囲は 1～10 です。

interval *seconds*: gratuitous ARP パケットを再送信する間隔を設定します。設定範囲は 1～10 秒です。

説明

gratuitous-arp mac-change retransmit コマンドは装置の MAC アドレスのために gratuitous ARP パケットを再送信する回数、送信間隔を設定します。

undo gratuitous-arp mac-change retransmit コマンドはデフォルトに戻します。

装置は、MAC アドレスの変更を他のデバイスに通知するために、gratuitous ARP パケットを送信します。ただし、装置はデフォルトで 1 回だけ gratuitous ARP パケットを送信するため、他の装置はパケットの受信に失敗する可能性があります。このコマンドを使用して、他の装置がパケットを受信できるように、gratuitous ARP 再送信パラメータを設定します。

このコマンドを実行すると、装置は MAC アドレス変更を通知するための gratuitous ARP パケットを、指定された回数、指定された間隔で再送信します。

例

MAC アドレス変更を通知するための gratuitous ARP パケットを 5 秒間隔で 3 回再送信するように設定します。

<AC> system-view

[AC] gratuitous-arp mac-change retransmit 3 interval 5

2.1.4 gratuitous-arp-learning enable

Syntax

gratuitous-arp-learning enable

undo gratuitous-arp-learning enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

gratuitous-arp-learning enable コマンドは gratuitous ARP パケットの学習機能を有効にします。

undo gratuitous-arp-learning enable コマンドは gratuitous ARP パケットの学習機能を無効にします。

gratuitous ARP パケットの学習機能は、装置が受信した gratuitous ARP パケットをもとに ARP エントリを作成あるいはアップデートすることで ARP テーブルを維持することができます。

学習機能が無効であるとき、装置は既存の ARP エントリのみをアップデートするため受信した gratuitous ARP パケットを使用します。ARP エントリは受信した gratuitous ARP パケットをもとに作成されません。これは ARP テーブルの空き容量を節約します。

例

gratuitous ARP パケットの学習機能を有効にします。

<AC> system-view

[AC] gratuitous-arp-learning enable

2.1.5 gratuitous-arp-sending enable

Syntax

gratuitous-arp-sending enable

undo gratuitous-arp-sending enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

gratuitous-arp-sending enable コマンドは異なるサブネットから ARP 要求を受信した際に、gratuitous ARP パケットの送信を有効にします。

undo gratuitous-arp-sending enable コマンドはデフォルトに戻します。

例

異なるサブネットから ARP 要求を受信した際に、gratuitous ARP パケットの送信を無効にします。

<AC> system-view

[AC] undo gratuitous-arp-sending enable

目次

このセクションのページは **5-x-x** です。

3 章 proxy ARP 3-1
3.1 proxy ARP 設定コマンド.....3-1
3.1.1 display local-proxy-arp.....3-1
3.1.2 display proxy-arp 3-2
3.1.3 local-proxy-arp enable 3-2
3.1.4 proxy-arp enable.....3-4

3章 proxy ARP

3.1 proxy ARP設定コマンド

3.1.1 display local-proxy-arp

Syntax

display local-proxy-arp [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定したインタフェースのローカル Proxy ARP のタイプとナンバーを表示します。

説明

display local-proxy-arp コマンドはローカル Proxy ARP の状態を表示します。

ローカル Proxy ARP の状態は有効あるいは無効にすることができます。

インタフェースを指定した場合、指定したインタフェースのローカル Proxy ARP の状態を表示します。

インタフェースを指定しない場合、すべてのインタフェースのローカル Proxy ARP の状態を表示します。

例

VLAN インタフェース 2 のローカル Proxy ARP の状態を表示します。

<AC> display local-proxy-arp interface vlan-interface 2

```
Interface Vlan-interface2
 Local Proxy ARP status: enabled
```

関連コマンド

local-proxy-arp enable

3.1.2 display proxy-arp

Syntax

display proxy-arp [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定したインタフェースの Proxy ARP のタイプとナンバーを表示します。

説明

display proxy-arp コマンドは Proxy ARP の状態を表示します。

Proxy ARP の状態は有効あるいは無効にすることができます。

インタフェースを指定した場合、指定したインタフェースの Proxy ARP の状態を表示します。

インタフェースを指定しない場合、すべてのインタフェースの Proxy ARP の状態を表示します。

例

VLAN インタフェース 1 の Proxy ARP の状態を表示します。

<AC> display proxy-arp interface vlan-interface 2

```
Interface Vlan-interface2
 Proxy ARP status: disabled
```

関連コマンド

proxy-arp enable

3.1.3 local-proxy-arp enable

Syntax

local-proxy-arp enable [**ip-range** *start-ip-address* **to** *end-ip-address*]

undo local-proxy-arp enable

デフォルト

無効.

View

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

ip-range *start-ip-address* **to** *end-ip-addrerss*: ローカル Proxy ARP を有効にする IP アドレスの範囲を指定します。*start-ip-address* は *end-ip-address* 以下の値にしてください。

説明

local-proxy-arp enable コマンドはローカル Proxy ARP を有効にします。

undo local-proxy-arp enable コマンドはローカル Proxy ARP を無効にします。

Proxy ARP は異なるネットワークの IP アドレスの ARP 要求に応答するため、ネットワークの装置で有効にします。Proxy ARP を有効にすることで、異なるブロードキャストドメインのホストが同一のブロードキャストドメインにいるように互いに通信できるようにします。

Proxy ARP は一般的な Proxy ARP とローカル Proxy ARP があります。

一般的な Proxy ARP は異なるレイヤ 3 インタフェースに接続され、異なるブロードキャストドメインに存在するホスト間で通信することができます。

ローカル Proxy ARP は同一のレイヤ 3 インタフェースに接続され、異なるブロードキャストドメインに存在するホスト間で通信することができます。

ip-range パラメータによって範囲の設定を複数実行した場合、最後に行った設定が適用されます。

例

VLAN インタフェース 2 でローカル Proxy ARP を有効にします。

<AC> system-view

[AC] interface vlan-interface 2

[AC-Vlan-interface2] local-proxy-arp enable

VLAN インタフェース 2 で IP アドレス範囲 1.1.1.1～1.1.1.20 のローカル Proxy ARP を有効にします。

<AC> system-view

[AC] interface vlan-interface 2

[AC-Vlan-interface2] local-proxy-arp enable ip-range 1.1.1.1 to 1.1.1.20

関連コマンド

display local-proxy-arp

3.1.4 proxy-arp enable

Syntax

proxy-arp enable

undo proxy-arp enable

デフォルト

無効

View

VLAN interface view

定義済みユーザロール

network-admin

説明

proxy-arp enable コマンドは Proxy ARP を有効にします。

undo proxy-arp enable コマンドは Proxy ARP を無効にします。

Proxy ARP は異なるネットワークの IP アドレスの ARP 要求に応答するため、ネットワークの装置で有効にします。Proxy ARP を有効にすることで、異なるブロードキャストドメインのホストが同一のブロードキャストドメインにいるように互いに通信できるようにします。

Proxy ARP は一般的な Proxy ARP とローカル Proxy ARP があります。

一般的な Proxy ARP は異なるレイヤ 3 インタフェースに接続され、異なるブロードキャストドメインに存在するホスト間で通信することができます。

ローカル Proxy ARP は同一のレイヤ 3 インタフェースに接続され、異なるブロードキャストドメインに存在するホスト間で通信することができます。

例

VLAN インタフェース 2 で Proxy ARP を有効にします。

<AC> system-view

[AC] interface vlan-interface 2

[AC-Vlan-interface2] proxy-arp enable

関連コマンド

display proxy-arp

目次

このセクションのページは **5-x-x** です。

4 章 IP アドレス 4-1
4.1 IP アドレス設定コマンド 4-1
4.1.1 display ip interface 4-1
4.1.2 display ip interface brief 4-4
4.1.3 ip address 4-6

4章 IP アドレス

4.1 IPアドレス設定コマンド

4.1.1 display ip interface

Syntax

display ip interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、すべてのレイヤ 3 インタフェースの IP の設定と統計情報を表示します。

説明

display ip interface コマンドは指定したレイヤ 3 インタフェースの IP の設定と統計情報を表示します。

統計情報には以下の情報が含まれます。

- ユニキャストパケットの数、バイト、インタフェースが送受信したマルチキャストパケットが含まれます。
- TTL 無効のパケットの数、インタフェースが受信した ICMP パケットの数が含まれます。

例

VLAN インタフェース 10 の IP の設定と統計情報を表示します。

<AC> display ip interface vlan-interface 10

```
Vlan-interface10 current state : DOWN
Line protocol current state : DOWN
Internet Address is 1.1.1.1/8 Primary
Broadcast address : 1.255.255.255
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
```

```
TTL invalid packet number:        0
ICMP packet input number:         0
  Echo reply:                    0
  Unreachable:                   0
  Source quench:                 0
  Routing redirect:              0
  Echo request:                  0
  Router advert:                 0
  Router solicit:                0
  Time exceed:                   0
  IP header bad:                 0
  Timestamp request:             0
  Timestamp reply:               0
  Information request:           0
  Information reply:             0
  Netmask request:               0
  Netmask reply:                 0
  Unknown type:                  0
```

表 4-1 コマンド出力

フィールド	説明
current state	インタフェースの現在の物理状態です。 ● **Administrative DOWN**—インタフェースが**shutdown**コマンドでシャットダウンしています。 ● **DOWN**—インタフェースが管理上upとなっていますが、物理的にdownしています。ケーブル接続あるいはリンク障害によって引き起こされる可能性があります。 ● **UP**—インタフェースが管理上および物理的にupとなっています。
Line protocol current state	リンクレイヤプロトコルの現在の状態です。 ● **DOWN**—インタフェースのプロトコル状態がdownしています。 ● **UP**—インタフェースのプロトコル状態がupしています。 ● **UP (spoofing)**—インタフェースのプロトコル状態がUpしているように見せかけていることを示します。対応するリンクが存在しない、あるいはリンクがオンデマンドでのみ設定されることを示します。

フィールド	説明
Internet Address	インタフェースのIPアドレスです。 ● **Primary**—プライマリIPアドレスです。 ● **Sub**—セカンダリIPアドレスです。 ● **DHCP-Allocated**—DHCPによって取得したIPアドレスです。 ● **BOOTP-Allocated**—BOOTPによって取得したIPアドレスです。
Broadcast address	インタフェースに接続されたサブネットのブロードキャストアドレスです。
The Maximum Transmit Unit	インタフェースのMTU（最大転送ユニット）です。単位はバイトです。
input packets, bytes, multicasts output packets, bytes, multicasts	インタフェースで受信したユニキャストパケット、バイト、マルチキャストパケットです。（装置起動時に統計情報の取得が開始されます。）
TTL invalid packet number	インタフェースで受信したTTL無効のパケット数です。（装置起動時に統計情報の取得が開始されます。）
ICMP packet input number: Echo reply: Unreachable: Source quench: Routing redirect: Echo request: Router advert: Router solicit: Time exceed: IP header bad: Timestamp request: Timestamp reply: Information request: Information reply: Netmask request: Netmask reply: Unknown type:	インタフェースで受信したICMPパケットの総数です。（装置起動時に統計情報の取得が開始されます。） ● **Echo reply packets**－エコー応答パケットです。 ● **Unreachable packets**－到達不能パケットです。 ● **Source quench packets**－送信元抑制パケットです。 ● **Routing redirect packets**－ルーティングリダイレクトパケットです。 ● **Echo request packets**－エコー要求パケットです。 ● **Router advertisement packets**－ルータ通知パケットです。 ● **Router solicitation packets**－ルータ選択要求パケットです。 ● **Time exceeded packets**－時間超過パケットです。 ● **IP header bad packets**－IPヘッダ不良パケットです。 ● **Timestamp request packets**－タイムスタンプ要求パケットです。 ● **Timestamp reply packets**－タイムスタンプ応答パケットです。 ● **Information request packets**－情報要求パケットです。 ● **Information reply packets**－情報応答パケットです。 ● **Netmask request packets**－ネットマスク要求パケットです。 ● **Netmask reply packets**－ネットマスク応答パケットです。 ● **Unknown type packets**－不明なタイプのパケットです。

関連コマンド

- **display ip interface brief**
- **ip address**

4.1.2 display ip interface brief

Syntax

display ip interface [*interface-type* [*interface-number*]] **brief**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type: インタフェースタイプを指定します。指定しない場合、すべてのレイヤ 3 インタフェースの IP 設定の概要情報を表示します。

interface-number: インタフェース番号を指定します。指定しない場合、指定したタイプのすべてのレイヤ 3 インタフェースの IP 設定の概要情報を表示します。

説明

display ip interface brief コマンドはレイヤ 3 インタフェースの IP 設定の概要情報を表示します。物理リンクの状態、リンクレイヤプロトコルの状態、IP アドレス、インタフェースの説明が含まれます。

例

VLAN インタフェースの IP 設定の概要情報を表示します。

<AC> display ip interface vlan-interface brief

```
*down: administratively down
(s): spoofing  (l): loopback
Interface          Physical Protocol IP address             Description
Vlan10             down     down     6.6.6.1        --       Link to Co...
```

表 4-2 コマンド出力

フィールド	説明
*down: administratively down	インタフェースが**shutdown**コマンドでシャットダウンしています。
(s) : spoofing	インタフェースのスプーフィング属性です。リンクレイヤプロトコルがUp表示されているインタフェースにリンクがない、あるいはリンクがオンデマンドでのみ設定されることを示します。
Interface	インタフェース名です。
Physical	インタフェースの物理状態です。 ● ***down**—インタフェースが**shutdown**コマンドでシャットダウンしています。 ● **down**—インタフェースが管理上upとなっていますが、物理的にdownしています。ケーブル接続あるいはリンク障害によって引き起こされる可能性があります。 ● **up**—インタフェースが管理上および物理的にupとなっています。
Protocol	インタフェースのリンクレイヤプロトコルの状態です。 ● **down**—インタフェースのプロトコル状態がdownしています。 ● **down(l)**—ループバックインタフェースのプロトコル状態がdownしています。 ● **up**—インタフェースのリンクレイヤプロトコルがupです。 ● **up(l)**—ループバックインタフェースのリンクレイヤプロトコルがupです。 ● **up(s)**—インタフェースのプロトコル状態がup（spoofing）です。
IP Address	インタフェースのIPアドレスです。設定されていない場合、（--）と表示されます。
Description	インタフェースの説明の情報です。 説明が設定されていない場合、（--）と表示されます。

関連コマンド

- **display ip interface**
- **ip address**

4.1.3 ip address

Syntax

ip address *ip-address* { *mask-length* | *mask* } [**sub**]

undo ip address [*ip-address* { *mask-length* | *mask* } [**sub**]

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: インタフェースの IP アドレスを指定します。ドットで区切り、10 進数で指定します。

mask-length: サブネットマスクの長さを指定します。設定範囲は 1～31 です。ループバックインタフェースの設定範囲は 1～32 です。

mask: サブネットマスクを指定します。ドットで区切り、10 進数で指定します。

sub: インタフェースにセカンダリ IP アドレスを割り当てます。

説明

ip address コマンドはインタフェースに IP アドレスを割り当てます。

undo ip address コマンドはインタフェースから IP アドレスを削除します。

インタフェースのプライマリ IP アドレスあるいはセカンダリ IP アドレスを設定するために、このコマンドを使用します。

インタフェースは 1 つのプライマリ IP アドレスのみ設定することができます。新しく設定されたプライマリ IP アドレスは、古いアドレスを上書きします。インタフェースが複数のサブネットに接続されている場合、サブネットがインタフェースを通して通信できるように、プライマリ IP アドレスとサブネットを設定します。

BOOTP、DHCP、PPP を通して IP アドレスを取得するインタフェースはセカンダリ IP アドレスを設定することができません。

undo ip address コマンドはインタフェースからすべての IP アドレスを削除します。

undo ip address *ip-address* { *mask* | *mask-length* }コマンドはプライマリ IP アドレスを削除します。**undo ip address** *ip-address* { *mask* | *mask-length* } **sub** コマンドはセカンダリ IP アドレスを削除します。

インタフェースに割り当てたプライマリ IP アドレスとセカンダリ IP アドレスは同一ネットワークセグメント上に設定することができますが、装置の異なるインタフェースは異なるネットワークセグメント上に存在する必要があります。

例

VLAN インタフェース 10 にプライマリ IP アドレスを 129.12.0.1、セカンダリ IP アドレスを 202.38.160.1、サブネットマスクを 255.255.255.0 に設定します。

<AC> system-view

[AC] interface vlan-interface 10

[AC-Vlan-interface10] ip address 129.12.0.1 255.255.255.0

[AC-Vlan-interface10] ip address 202.38.160.1 255.255.255.0 sub

関連コマンド

- **display ip interface**
- **display ip interface brief**

目次

このセクションのページは **5-x-x** です。

5 章 DHCP の概要 5-1
5.1 DHCP 設定コマンド 5-1
5.1.1 dhcp dscp 5-1
5.1.2 dhcp enable 5-2
5.1.3 dhcp select 5-2

5章 DHCP の概要

5.1 DHCP設定コマンド

5.1.1 dhcp dscp

Syntax

dhcp dscp *dscp-value*

undo dhcp dscp

デフォルト

56

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: DHCP パケットの DSCP を設定します。設定範囲は 0～63 です。

説明

dhcp dscp コマンドは DHCP サーバあるいは DHCP リレーエージェントに送信される DHCP パケットの DSCP を設定します。

undo dhcp dscp コマンドはデフォルトに戻します。

DHCP パケットの DSCP の値はパケットのプライオリティを指定します。パケットを送信するプライオリティに影響します。DSCP の値が大きくなると、プライオリティが高くなります。

例

DHCP パケットの DSCP を 30 に設定します。

<AC> system-view

[AC] dhcp dscp 30

5.1.2 dhcp enable

Syntax

dhcp enable

undo dhcp enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

dhcp enable コマンドは DHCP を有効にします。

undo dhcp enable コマンドは DHCP を無効にします。

DHCP に関する設定は DHCP を有効にしたのち適用されます。

DHCP サーバあるいは DHCP リレーエージェントの設定を実行する前に、DHCP を有効にしてください。

例

DHCP を有効にします。

<AC> system-view

[AC] dhcp enable

5.1.3 dhcp select

Syntax

dhcp select { **relay** | **server** }

undo dhcp select { **relay** | **server** }

デフォルト

インタフェースは DHCP サーバモードで動作し、設定パラメータの DHCP 要求に応答します。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

relay: インタフェースで DHCP リレーエージェントを有効にします。

server: インタフェースで DHCP サーバを有効にします。

説明

dhcp select コマンドはインタフェースで DHCP サーバあるいは DHCP リレーエージェントを有効にします。

undo dhcp select コマンドはインタフェースで DHCP サーバあるいは DHCP リレーエージェントを無効にします。無効にした場合、インタフェースは受信した DHCP パケットを廃棄します。

インタフェースで DHCP サーバモードを DHCP リレーエージェントモードに変更する前に、**reset dhcp server ip-in-use** コマンドでアドレスの割り当てと許可された ARP エントリを削除してください。これらの割り当ては、DHCP リレーエージェントが有効になったのち、作成される ARP エントリと重複する可能性があります。

例

VLAN インタフェース 2 で DHCP リレーエージェントを有効にします。

<AC> system-view

[AC] interface vlan-interface 2

[AC-Vlan-interface2] dhcp select relay

目次

このセクションのページは **5-x-x** です。

6 章 DHCP サーバ 6-1
6.1 DHCP サーバ設定コマンド 6-1
6.1.1 address range 6-1
6.1.2 bims-server 6-2
6.1.3 bootfile-name 6-3
6.1.4 class option-group 6-4
6.1.5 dhcp class 6-5
6.1.6 dhcp option group 6-6
6.1.7 dhcp server apply ip-pool 6-7
6.1.8 dhcp server forbidden-ip 6-8
6.1.9 dhcp server ip-pool 6-9
6.1.10 dhcp server ping packets 6-10
6.1.11 dhcp server ping timeout 6-11
6.1.12 dhcp server relay information enable 6-12
6.1.13 display dhcp server conflict 6-13
6.1.14 display dhcp server expired 6-14
6.1.15 display dhcp server free-ip 6-15
6.1.16 display dhcp server ip-in-use 6-17
6.1.17 display dhcp server pool 6-18
6.1.18 display dhcp server statistics 6-21
6.1.19 dns-list 6-23
6.1.20 domain-name 6-24
6.1.21 expired 6-25
6.1.22 forbidden-ip 6-26
6.1.23 gateway-list 6-27
6.1.24 if-match 6-28
6.1.25 nbns-list 6-31
6.1.26 netbios-type 6-32
6.1.27 network 6-33
6.1.28 next-server 6-34
6.1.29 option 6-35
6.1.30 reset dhcp server conflict 6-37
6.1.31 reset dhcp server expired 6-37
6.1.32 reset dhcp server ip-in-use 6-38
6.1.33 reset dhcp server statistics 6-39
6.1.34 static-bind 6-39

6.1.35 tftp-server domain-name 6-41
6.1.36 tftp-server ip-address 6-42
6.1.37 voice-config 6-43

6章 DHCP サーバ

6.1 DHCPサーバ設定コマンド

6.1.1 address range

Syntax

address range *start-ip-address end-ip-address*

undo address range

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

start-ip-address: 開始 IP アドレスを指定します。

end-ip-address: 終了 IP アドレスを指定します。

説明

address range コマンドはダイナミックの割り当てを行うため DHCP アドレスプールの IP アドレス範囲を設定します。

undo address range コマンドは DHCP アドレスプールの IP アドレス範囲を削除します。

IP アドレス範囲が指定されていない場合、address pool view で **network** コマンドを使用してサブネットのすべての IP アドレスを割り当てることができます。IP アドレス範囲が指定されている場合、IP アドレス範囲の IP アドレスのみを割り当てることができます。

address range コマンドを使用した後、アドレスプールのセカンダリサブネットを指定するため、**network secondary** コマンドを使用することができません。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

address range で指定されたアドレス範囲は **network** コマンドで指定されたサブネット内にある必要があります。範囲外のアドレスを割り当てることはできません。

例

アドレスプール 1 の 192.168.8.1～192.168.8.150 のアドレス範囲を指定します。

<AC> system-view

[AC] dhcp server ip-pool 1

[AC-dhcp-pool-1] address range 192.168.8.1 192.168.8.150

関連コマンド

- **display dhcp server pool**
- **network**

6.1.2 bims-server

Syntax

bims-server ip *ip-address* [**port** *port-number*] **sharekey** { **cipher** | **simple** } *string*

undo bims-server

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: BIMS サーバの IP アドレスを指定します。

port *port-number*: BIMS サーバのポート番号を指定します。設定範囲は 1～65534 です。
cipher: 暗号テキストキーを設定します。

simple: プレーンテキストキーを設定します。

string: キーの文字列を設定します。大文字小文字を区別します。**simple** を指定した場合、プレーンテキストで 1～16 の文字列でなくてはなりません。**cipher** を設定した場合、1～53 文字の暗号テキストでなければなりません。BIMS サーバに送られたパケットを暗号化するために DHCP クライアントは共有キーを使用します。

説明

bims-server コマンドは、DHCP アドレスプールの BIMS サーバの IP アドレス、ポート番号、共有キーを指定します。

undo bims-server コマンドは、指定された BIMS サーバ情報を削除します。

コマンドを複数回、設定した場合、最後に行った設定が適用されます。

セキュリティ目的のため、プレーンテキストで設定されたパスワードも含め、すべてのパスワードは暗号テキストで保存されます。

例

BIMS サーバの IP アドレス 1.1.1.1、ポート番号 80、共有キーaabbcc アドレスプール 0 に指定します。

<AC> system-view

[AC] dhcp server ip-pool 0

[AC-dhcp-pool-0] bims-server ip 1.1.1.1 port 80 sharekey simple aabbcc

関連コマンド

display dhcp server pool

6.1.3 bootfile-name

Syntax

bootfile-name *bootfile-name*

undo bootfile-name

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

bootfile-name: コンフィグレーションファイル名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

説明

bootfile-name コマンドはコンフィグレーションファイル名を指定します。

undo bootfile-name コマンドはコンフィグレーションファイル名を削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

コンフィグレーションファイルが TFTP サーバにある場合、TFTP サーバのコンフィグレーションファイル名を指定します。

例

DHCP アドレスプール 0 のブートファイル名 boot.cfg を指定します。

<AC> system-view

[AC] dhcp server ip-pool 0

[AC-dhcp-pool-0] bootfile-name boot.cfg

関連コマンド

- **display dhcp server pool**
- **next-server**
- **tftp-server domain-name**
- **tftp-server ip-address**

6.1.4 class option-group

Syntax

class *class-name* **option-group** *option-group-number*

undo class *class-name* **option-group**

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

class-name: DHCP ユーザクラスの名前を指定します。設定範囲は 1～63 文字で、大文字と小文字は区別しません。

option-group-number: DHCP オプショングループに 1 から 32768 までの番号を割り当てます。

説明

class option-group コマンドは DHCP ユーザクラスの DHCP オプショングループを指定します。

undo class option-group コマンドは DHCP ユーザクラスの DHCP オプショングループ設定を削除します。

DHCP-DISCOVER メッセージを受信すると、サーバはこのコマンドで指定された順序で DHCP クライアントと DHCP ユーザクラスを比較します。一致する DHCP ユーザクラスが見つかった場合、サーバはクライアントにオプショングループの DHCP オプションを割り当てます。複数の DHCP ユーザクラスと一致した場合、サーバは次のようにオプショングループを選択します。

· オプショングループに共通のオプションがある場合、サーバは最初に一致したユーザクラスに指定されたオプショングループを選択します。

· オプショングループのオプションが異なる場合、サーバは一致するオプショングループをすべて選択します。

DHCP アドレスプール内の DHCP ユーザクラスに指定できるオプショングループは 1 つだけです。ユーザクラスに対してこのコマンドを複数回実行すると、最新の設定が有効になります。

例

DHCP アドレスプール 0 の DHCP ユーザクラス user に、DHCP オプショングループ 1 を指定します。

<AC> system-view

[AC] dhcp server ip-pool 0

[AC-dhcp-pool-0] class user option-group 1

関連コマンド

dhcp option-group

6.1.5 dhcp class

Syntax

dhcp class *class-name*

undo dhcp class *class-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

class-name: DHCP ユーザクラスの名前を指定します。設定範囲は 1～63 文字で、大文字と小文字は区別しません。

説明

dhcp class コマンドは DHCP ユーザクラスを作成し、その view に移行します。

undo dhcp class コマンドは指定した DHCP ユーザクラスを削除します。

またコマンドを使用して既存の DHCP ユーザクラス View に移行することができます。

DHCP ユーザクラス View では、if-match コマンドを使用して、DHCP クライアントを DHCP ユーザクラスに紐付ける一致ルールを設定できます。

例

DHCP ユーザクラス test を作成し、その View に移行します。

<AC> system-view

[AC] dhcp class test

[AC-dhcp-class-test]

関連コマンド

- **class option-group**
- **if-match**

6.1.6 dhcp option group

Syntax

dhcp option-group *option-group-number*

undo dhcp option-group *option-group-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

option-group-number: DHCP オプショングループに 1 から 32768 までの番号を割り当てます。

説明

dhcp option group コマンドは DHCP オプショングループを作成し、その view に移行します。

undo dhcp option group コマンドは指定した DHCP オプショングループを削除します。

またコマンドを使用して既存の DHCP オプショングループ View に移行することができます。

例

DHCP オプショングループ 1 を作成し、その View に移行します。

<AC> system-view

[AC] dhcp option-group 1

[AC-dhcp-option-group-1]

関連コマンド

- **class option-group**
- **option**

6.1.7 dhcp server apply ip-pool

Syntax

dhcp server apply ip-pool *pool-name*

undo dhcp server apply ip-pool

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

pool-name: DHCP アドレスプールの名前を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

説明

dhcp server apply ip-pool コマンドはインタフェースにアドレスプールを適用します。

undo dhcp server apply ip-pool コマンドは設定を削除します。

インタフェースから DHCP 要求を受信すると、DHCP サーバはすべてのアドレスプールから、割り当て可能な DHCP クライアントの IP アドレスを検索します。
このコマンドが設定されている場合は、サーバはインタフェースに適用されたアドレスプールから、DHCP クライアントに IP アドレスを割り当てます。アドレスプールに割り当て可能な IP アドレスがない、または、アドレスプール自体が存在しない場合は、DHCP クライアントは IP アドレスを取得することができません。
コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

VLAN インタフェース 2 に DHCP アドレスプール 0 を適用します。

<AC> system-view

[AC] interface vlan-interface 2

[AC-Vlan-interface2] dhcp server apply ip-pool 0

関連コマンド

dhcp server ip-pool

6.1.8 dhcp server forbidden-ip

Syntax

dhcp server forbidden-ip *start-ip-address* [*end-ip-address*]

undo dhcp server forbidden-ip *start-ip-address* [*end-ip-address*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

start-ip-address: 開始 IP アドレスを指定します。

end-ip-address: 終了 IP アドレスを指定します。*end-ip-address* は *start-ip-address* より小さい値にすることができません。指定されない場合、*start-ip-address* のみがダイナミック割り当てから除外されます。

説明

dhcp server forbidden-ip コマンドはダイナミック割り当てから指定した IP アドレスを除外します。

undo dhcp server forbidden-ip コマンドは設定を削除します。

ゲートウェイとFTPサーバのような装置のIPアドレスはクライアントに割り当てることができません。このコマンドはダイナミック割り当てからそのようなアドレスを除外します。

除外された IP アドレスがスタティックの割り当てにある場合、クライアントに割り当てることができます。

undo dhcp server forbidden-ip コマンドでアドレスあるいはアドレス範囲を削除する場合、**dhcp server forbidden-ip** コマンドで指定したアドレスあるいはアドレス範囲と同一にしてください。

アドレス範囲の一部の IP アドレスを削除する場合、アドレス範囲全体を削除する必要があります。

ダイナミック割り当てから複数の IP アドレス範囲を除外することができます。

例

ダイナミック割り当てから IP アドレス 10.110.1.1～10.110.1.63 を除外します。

<AC> system-view

[AC] dhcp server forbidden-ip 10.110.1.1 10.110.1.63

関連コマンド

- **forbidden-ip**
- **static-bind**

6.1.9 dhcp server ip-pool

Syntax

dhcp server ip-pool *pool-name*

undo dhcp server ip-pool *pool-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

pool-name: アドレスプールを固有に識別するため DHCP アドレスプールの名前を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

説明

dhcp server ip-pool コマンドは DHCP アドレスプールを作成し、その view に移行します。

undo dhcp server ip-pool コマンドは指定した DHCP アドレスプールを削除します。

またコマンドを使用して既存の DHCP アドレスプールに移行することができます。

DHCP アドレスプールは DHCP クライアントに割り当てられる設定パラメータを記録するために使用されます。

例

DHCP アドレスプール pool1 を作成します。

<AC> system-view

[AC] dhcp server ip-pool pool1

[AC-dhcp-pool-pool1]

関連コマンド

- **dhcp server apply ip-pool**
- **display dhcp server pool**

6.1.10 dhcp server ping packets

Syntax

dhcp server ping packets *number*

undo dhcp server ping packets

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

number: ping パケットの最大数を指定します。設定範囲は 0～10 です。0 は DHCP サーバがアドレス競合の検出を行わないことを示します。

説明

dhcp server ping packets コマンドは ping パケットの最大数を指定します。

undo dhcp server ping packets コマンドはデフォルトに戻します。

IP アドレスの競合を防ぐため、DHCP サーバは DHCP クライアントに IP アドレスを割り当てる前に IP アドレス宛に ping を実行します。

ping が成功した場合、サーバは IP アドレスが競合していると認識し、新しい IP アドレスを選択します。すべての ping が失敗すると、サーバは DHCP クライアントに IP アドレスを割り当てます。

例

ping パケットの最大数を 10 に指定します。

<AC> system-view

[AC] dhcp server ping packets 10

関連コマンド

- **dhcp server ping timeout**
- **display dhcp server conflict**
- **reset dhcp server conflict**

6.1.11 dhcp server ping timeout

Syntax

dhcp server ping timeout *milliseconds*

undo dhcp server ping timeout

デフォルト

500 ミリ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

milliseconds: ping 応答に対するタイムアウト時間を指定します。設定範囲は 0～10000 ミリ秒です。アドレス競合の検出を無効にする場合、0 を指定します。

説明

dhcp server ping timeout コマンドは DHCP サーバで ping 応答に対するタイムアウト時間を設定します。

undo dhcp server ping timeout コマンドはデフォルトに戻します。

IP アドレスの競合を防ぐため、DHCP サーバは DHCP クライアントに IP アドレスを割り当てる前に IP アドレス宛に ping を実行します。

ping が成功した場合、サーバは IP アドレスが競合していると認識し、新しい IP アドレスを選択します。すべての ping が失敗すると、サーバは DHCP クライアントに IP アドレスを割り当てます。

例

ping 応答に対するタイムアウト時間を 1000 ミリ秒に設定します。

<AC> system-view

[AC] dhcp server ping timeout 1000

関連コマンド

- **dhcp server ping packets**
- **display dhcp server conflict**
- **reset dhcp server conflict**

6.1.12 dhcp server relay information enable

Syntax

dhcp server relay information enable

undo dhcp server relay information enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

dhcp server relay information enable コマンドは DHCP サーバのオプション 82 を有効にします。

undo dhcp server relay information enable コマンドは DHCP サーバのオプション 82 を無効にします。

DHCP サーバがオプション 82 を処理するように設定されている場合、オプション 82 のメッセージを受信すると、DHCP サーバはオプション 82 を DHCP 応答メッセージに追加します。DHCP サーバがオプション 82 を無効するように設定されている場合、DHCP 応答メッセージにオプション 82 を追加しません。

例

DHCP サーバのオプション 82 を無効にします。

<AC> system-view

[AC] undo dhcp server relay information enable

6.1.13 display dhcp server conflict

Syntax

display dhcp server conflict [**ip** *ip-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip *ip-address*: 指定した IP アドレスの競合情報を表示します。指定しない場合、すべての IP アドレスの競合情報を表示します。

説明

display dhcp server conflict コマンドは IP アドレス競合の情報を表示します。

DHCP サーバは以下の状況で IP アドレス競合の情報を作成します。

- DHCP クライアントに IP アドレスを割り当てる前、DHCP サーバは ping を行い、が他のホストで IP アドレスを使用しているかどうかを検出します。
- DHCP クライアントは IP アドレス競合をサーバに通知するため、DHCP サーバに DECLINE パケットを送信します。

- DHCP サーバはアドレスプールの割り当て可能なアドレスが自身の IP アドレスであることを検出します。

例

すべての IP アドレスの競合情報を表示します。

<AC> display dhcp server conflict

```
IP address         Detect time
4.4.4.1            Apr 25 16:57:20 2007
4.4.4.2            Apr 25 17:00:10 2007
```

表 6-1 コマンド出力

フィールド	説明
IP address	競合したIPアドレスです。
Detect time	競合が検出された時間です。

関連コマンド

reset dhcp server conflict

6.1.14 display dhcp server expired

Syntax

display dhcp server expired [**ip** *ip-address* | **pool** *pool-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip *ip-address*: 指定した IP アドレスのリース期限の終了に関する情報を表示します。指定しない場合、すべての IP アドレスのリース期限の終了に関する情報を表示します。

pool *pool-name*: 指定したアドレスプールのリース期限の終了に関する情報を表示します。設定範囲は 1～63 です。大文字、小文字を区別しません。指定しない場合、すべてのアドレスプールのリース期限の終了に関する情報を表示します。

説明

display dhcp server expired コマンドはリース期限の終了に関する情報を表示します。

有効なアドレスがすべて割り当てられてとき、DHCP サーバは DHCP クライアントにリース期限が終了した IP アドレスを割り当てます。

例

すべてのリース期限の終了に関する情報を表示します。

<AC> display dhcp server expired

```
IP address      Client-identifier/Hardware address   Lease expiration
4.4.4.6         3030-3066-2e65-3230-302e-3130-3234   Apr 25 17:10:47 2007
                -2d45-7468-6572-6e65-7430-2f31
```

表 6-2 コマンド出力

フィールド	説明
IP address	リース期限が終了するIPアドレスです。
Client-identifier/Hardware address	クライアントIDあるいはMACアドレスです。 DHCP client ID • クライアントIDの値がASCII形式である場合、タイプは00です。 • クライアントIDの値が指定したインタフェースのMACアドレスを使用している場合、タイプは01です。 • クライアントIDの値が16進数形式である場合、タイプは文字列の最初の2桁の文字です。
Lease expiration	リース期限が終了する時間です。

関連コマンド

reset dhcp server expired

6.1.15 display dhcp server free-ip

Syntax

display dhcp server free-ip [**pool** *pool-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pool *pool-name*: 指定したアドレスプールの割り当て可能な IP アドレスを表示します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。指定しない場合、すべてのアドレスプールの割り当て可能なすべての IP アドレスを表示します。

説明

display dhcp server free-ip コマンドは割り当て可能な IP アドレスを表示します。

例

すべてのアドレスプールの割り当て可能な IP アドレスを表示します。

<AC> display dhcp server free-ip

```
Pool name: 1
  Network: 10.0.0.0 mask 255.0.0.0
    IP ranges from 10.0.0.10 to 10.0.0.100
    IP ranges from 10.0.0.105 to 10.0.0.255
  Secondary networks:
    10.1.0.0 mask 255.255.0.0
      IP ranges from 10.1.0.0 to 10.1.0.255
    10.2.0.0 mask 255.255.0.0
      IP Ranges from 10.2.0.0 to 10.2.0.255

Pool name: 2
  Network: 20.1.1.0 mask 255.255.255.0
    IP ranges from 20.1.1.0 to 20.1.1.255
```

表 6-3 コマンド出力

フィールド	説明
Pool name	アドレスプールの名前です。
Network	割り当て可能なネットワークです。
IP ranges	割り当て可能なIPアドレス範囲です。
Secondary networks	割り当て可能なセカンダリネットワークです。

関連コマンド

- **address range**
- **dhcp server ip-pool**
- **network**

6.1.16 display dhcp server ip-in-use

Syntax

display dhcp server ip-in-use [**ip** *ip-address* | **pool** *pool-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip *ip-address*: 指定した IP アドレスの割り当て情報を表示します。指定しない場合、すべての割り当てられた IP アドレスの情報を表示します。

pool *pool-name*: 指定した IP アドレスプールの割り当て情報を表示します。設定範囲は 1～63 です。大文字、小文字を区別しません。指定しない場合、すべての割り当てられた IP アドレスプールの IP アドレスの情報を表示します。

説明

display dhcp server ip-in-use コマンドは割り当てられた IP アドレスの情報を表示します。

クライアントの割り当て情報は、DHCP サーバに DHCP クライアントのゲートウェイが設定されているときのみ、IP ソースガードのような他のセキュリティモジュールで使用することができます。

リース期限が 2100 年を超過する場合、リース期限は After 2100 と表示されます。

例

すべての割り当てられた DHCP アドレスの情報を表示します。

<AC> display dhcp server ip-in-use

```
IP address      Client identifier/    Lease expiration      Type
                Hardware address
10.1.1.1        4444-4444-4444        Not used              Static(F)
10.1.1.2        3030-3030-2e30-3030-  May 1 14:02:49 2015   Auto(C)
                662e-3030-3033-2d45-
```

```
                7468-6572-6e65-74
10.1.1.3        1111-1111-1111        After 2100            Static(C)
```

表 6-4 コマンド出力

フィールド	説明
IP address	割り当てられたIPアドレスです。
Client identifier/Hardware address	クライアントIDあるいはハードウェアアドレスです。
Lease expiration	リース期間です。 • **Exact time (May 1 14:02:49 2015)**—リース期間が終了する時間です。 • **Not used**—スタティック割り当てのIPアドレスがクライアントに割り当てられていません。 • **Unlimited**—期限なしのリースです。 • **After 2100**—リース期間の終了が2100年以降です。
Type	割り当てタイプです。 • **Static(F)**— IPアドレスが割り当てられていない空きのスタティック割り当てです。 • **Static(O)**—IPアドレスが選択され、提供されたスタティック割り当てです。DHCPサーバによってDHCP-OFFERパケットにIPアドレスが記載されDHCPクライアントに送信されます。 • **Static(C)**—IPアドレスがDHCPクライアントに割り当てられ、コミットされたスタティック割り当てです。 • **Auto(O)**—IPアドレスが選択され、一時的に提供されたダイナミック割り当てです。DHCPサーバによってDHCP-OFFERパケットにIPアドレスが記載されDHCPクライアントに送信されます。 • **Auto(C)**— IPアドレスがDHCPクライアントに割り当てられ、コミットされたダイナミック割り当てです。

関連コマンド

reset dhcp server ip-in-use

6.1.17 display dhcp server pool

Syntax

display dhcp server pool [*pool-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pool-name: 指定したアドレスプールの情報を表示します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。指定しない場合、すべてのアドレスプールの情報を表示します。

説明

display dhcp server pool コマンドは DHCP アドレスプールの情報を表示します。

例

すべての DHCP アドレスプールの情報を表示します。

<AC> display dhcp server pool

```
Pool name: 0
  Network 20.1.1.0 mask 255.255.255.0
  class a range 20.1.1.50 20.1.1.60
  bootfile-name abc.cfg
  dns-list 20.1.1.66 20.1.1.67 20.1.1.68
  domain-name www.aabbcc.com
  bims-server ip 192.168.0.51 sharekey cipher $c$3$K13OmQPi791YvQoF2Gs1E+65LOU=
  option 2 ip-address 1.1.1.1
  expired 1 2 3 0

Pool name: 1
  Network 20.1.1.0 mask 255.255.255.0
  secondary networks:
    20.1.2.0 mask 255.255.255.0
    20.1.3.0 mask 255.255.255.0
  bims-server     ip     192.168.0.51     port     50     sharekey     cipher
$c$3$K13OmQPi791YvQoF2Gs1E+65LOU=
  forbidden-ip 20.1.1.22 20.1.1.36 20.1.1.37
  forbidden-ip 20.1.1.22 20.1.1.23 20.1.1.24
  gateway-list 1.1.1.1 2.2.2.2 4.4.4.4
  nbns-list 5.5.5.5 6.6.6.6 7.7.7.7
  netbios-type m-node
  option 2 ip-address 1.1.1.1
  expired 1 0 0 0
```

```
Pool name: 2
  Network 20.1.1.0 mask 255.255.255.0
  address range 20.1.1.1 to 20.1.1.15
  class departmentA range 20.1.1.20 to 20.1.1.29
  class departmentB range 20.1.1.30 to 20.1.1.40
  next-server 20.1.1.33
  tftp-server domain-name www.dian.org.cn
  tftp-server ip-address 192.168.0.120
  voice-config ncp-ip 10.1.1.2
  voice-config as-ip 10.1.1.5
  voice-config fail-over 10.1.1.1 123*
  option 2 ip-address 1.1.1.3
  expired 1 0 0 0

Pool name: 3
  static bindings:
    ip-address 10.10.1.2 mask 255.0.0.0
      hardware-address 00e0-00fc-0001 ethernet
    ip-address 10.10.1.3 mask 255.0.0.0
      client-identifier aaaa-bbbb
  expired unlimited
```

表 6-5 コマンド出力

フィールド	説明
Pool name	アドレスプールの名前です。
Network	割り当て可能なネットワークです。
secondary networks	割り当て可能なセカンダリネットワークです。
address range	割り当て可能なアドレス範囲です。
class *class-name* range	DHCPユーザクラスとアドレス範囲です。
static bindings	スタティックIP-MAC/クライアントIDバインディングです。
option	カスタマイズされたDHCPオプションです。
expired	リース期限です。この例の1 2 3 4は1日2時間3分4秒を示します。
bootfile-name	ブートファイル名です。
dns-list	DNSサーバのIPアドレスです。

フィールド	説明
domain-name	ドメイン名サフィックスです。
bims-server	BIMSサーバの情報です。
forbidden-ip	ダイナミックの割り当てから除外されたIPアドレスです。
gateway-list	ゲートウェイアドレスです。
nbns-list	WINSサーバのアドレスです。
netbios-type	NetBIOSノードタイプです。
next-server	次のサーバのIPアドレスです。
tftp-server domain-name	TFTPサーバ名です。
tftp-server ip-address	TFTPサーバのアドレスです。
voice-config ncp-ip	プライマリのネットワークコーリングプロセッサのアドレスです。
voice-config as-ip	バックアップのネットワークコーリングプロセッサのアドレスです。
voice-config fail-over	フェイルオーバルートです。

6.1.18 display dhcp server statistics

Syntax

display dhcp server statistics [**pool** *pool-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pool *pool-name*: アドレスプールを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。指定しない場合、すべてのアドレスプールの情報を表示します。

説明

display dhcp server statistics コマンドは DHCP サーバの統計情報を表示します。

例

DHCP サーバの統計情報を表示します。

<AC> display dhcp server statistics

```
Pool number:                  1
Pool utilization:             0.39%
Bindings:
  Automatic:                   1
  Manual:                     0
  Expired:                     0
Conflict:                      1
Messages received:            10
  DHCPDISCOVER:               5
  DHCPREQUEST:                3
  DHCPDECLINE:                0
  DHCPRELEASE:                2
  DHCPINFORM:                 0
  BOOTPREQUEST:                0
Messages sent:                6
  DHCPOFFER:                  3
  DHCPACK:                     3
  DHCPNAK:                     0
  BOOTPREPLY:                 0
Bad Messages:                  0
```

表 6-6 コマンド出力

フィールド	説明
Pool number	アドレスプールの総数です。このフィールドは指定したアドレスプールの統計情報を表示する場合、表示されません。
Pool utilization	プール使用率です。 ● すべてのアドレスプールの統計情報を表示する場合、すべてのアドレスプールの使用率を表示します。 ● アドレスプールの統計情報を表示する場合、指定したアドレスプールの使用率を表示します。
Bindings	以下のタイプの割り当てです。 ● **Automatic**—ダイナミック割り当て数です。 ● **Manual**—スタティック割り当て数です。 ● **Expired**—除外された割り当て数です。

フィールド	説明
Conflict	競合アドレスの総数です。このフィールドは指定したアドレスプールの統計情報を表示する場合、表示されません。
Messages received	クライアントから受信されたDHCPパケットです。 • DHCPDISCOVER • DHCPREQUEST • DHCPDECLINE • DHCPRELEASE • DHCPINFORM • BOOTPREQUEST このフィールドは指定したアドレスプールの統計情報を表示する場合、表示されません。
Messages sent	クライアントに送信されたDHCPパケットです。 • DHCPOFFER • DHCPACK • DHCPNAK • BOOTPREPLY このフィールドは指定したアドレスプールの統計情報を表示する場合、表示されません。
Bad Messages	BADメッセージ数です。 このフィールドは指定したアドレスプールの統計情報を表示する場合、表示されません。

関連コマンド

reset dhcp server statistics

6.1.19 dns-list

Syntax

dns-list *ip-address*&<1-8>

undo dns-list [*ip-address*&<1-8>]

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-8>: DNS サーバを指定します。&<1-8>は DNS サーバのアドレスを半角スペースで区切り最大 8 つまで指定できることを示します。

説明

dns-list コマンドは DHCP アドレスプールの DNS サーバアドレスを指定します。

undo dns-list コマンドは DHCP アドレスプールの DNS サーバアドレスを削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

パラメータを指定しない場合、**undo dns-list** コマンドは DHCP アドレスプールのすべての DNS サーバのアドレスを削除します。

例

DHCP アドレスプール 0 の DNS サーバアドレス 10.1.1.254 を指定します。

<AC> system-view

[AC] dhcp server ip-pool 0

[AC-dhcp-pool-0] dns-list 10.1.1.254

関連コマンド

display dhcp server pool

6.1.20 domain-name

Syntax

domain-name *domain-name*

undo domain-name

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

domain-name: ドメイン名を指定します。設定範囲は 1～50 です。大文字、小文字を区別します。

説明

domain-name コマンドは DHCP アドレスプールのドメイン名を指定します。

undo domain-name コマンドは DHCP アドレスプールのドメイン名を削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

DHCP アドレスプール 0 のドメイン名 company.com を指定します。

<AC> system-view

[AC] dhcp server ip-pool 0

[AC-dhcp-pool-0] domain-name company.com

関連コマンド

display dhcp server pool

6.1.21 expired

Syntax

expired { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }

undo expired

デフォルト

1 日

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

day *day*: 日数を指定します。設定範囲は 0～365 日です。

hour *hour*: 時間を指定します。設定範囲は 0～23 時間です。デフォルトは 0 時間です。

minute *minute*: 分を指定します。設定範囲は 0～59 分です。デフォルトは 0 分です。

second *second*: 秒を指定します。設定範囲は 0～59 秒です。デフォルトは 0 秒です。

unlimited: リース期間を指定しません。正確には 136 年のリース期間です。

説明

expired コマンドは DHCP アドレスプールのリース期間を指定します。

undo expired コマンドは DHCP アドレスプールのリース期間をデフォルトに戻します。

DHCP サーバは DHCP クライアントにリース期間と共に IP アドレスを割り当てます。リース期間が終了する前に、DHCP クライアントはリース期間を延長する必要があります。

- リース期間の延長が成功した場合、DHCP クライアントは IP アドレスを使用し続けることができます。
- リース期間の延長が失敗したとき、以下のイベントの両方が発生します。
  - □ リース期間が終了した後 DHCP クライアントは IP アドレスを使用することができません。
  - □ DHCP サーバは終了したアドレスとして IP アドレスにラベルをつけます。

例

DHCP アドレスプール 0 のリース期間を 1 日、2 時間、3 分、4 秒に指定します。

<AC> system-view

[AC] dhcp server ip-pool 0

[AC-dhcp-pool-0] expired day 1 hour 2 minute 3 second 4

関連コマンド

- **display dhcp server expired**
- **display dhcp server pool**
- **reset dhcp server expired**

6.1.22 forbidden-ip

Syntax

forbidden-ip *ip-address*&<1-8>

undo forbidden-ip [*ip-address*&<1-8>]

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-8>: 除外する IP アドレスを指定します。&<1-8>は IP アドレスを半角スペースで区切り最大 8 つまで指定できることを示します。

説明

forbidden-ip コマンドはアドレスプールのダイナミック割り当てから IP アドレスを除外します。

undo forbidden-ip コマンドは設定を削除します。

アドレスプールの除外された IP アドレスは他のアドレスプールで割り当て可能です。

アドレスプールで最大 4096 の IP アドレスを除外することができます。

パラメータを指定しない場合、**undo forbidden-ip** コマンドはすべての除外した IP アドレスを削除します。

例

DHCP アドレスプール 0 のダイナミック割り当てから 192.168.1.3 と 192.168.1.10 を除外します。

<AC> system-view

[AC] dhcp server ip-pool 0

[AC-dhcp-pool-0] forbidden-ip 192.168.1.3 192.168.1.10

関連コマンド

- **dhcp server forbidden-ip**
- **display dhcp server pool**

6.1.23 gateway-list

Syntax

gateway-list *ip-address*&<1-64>

undo gateway-list [*ip-address*&<1-64>]

デフォルト

設定なし

View

DHCP address pool view

DHCP secondary subnet view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-64>: ゲートウェイを指定します。&<1-64>はゲートウェイアドレスを半角スペースで区切り最大 64 つまで指定できることを示します。ゲートウェイアドレスは割り当て可能な IP アドレスと同一のサブネットに存在する必要があります。

説明

gateway-list コマンドは DHCP アドレスプールあるいは DHCP セカンダリサブネットのゲートウェイアドレスを指定します。

undo gateway-list コマンドは DHCP アドレスプールあるいは DHCP セカンダリサブネットからゲートウェイアドレスを削除します。

DHCP サーバは以下の方法でセカンダリサブネットのクライアントにゲートウェイアドレスを割り当てます。

- address pool view と secondary subnet view の両方でゲートウェイを指定する場合、DHCP は secondary subnet view のゲートウェイアドレスをセカンダリサブネットのクライアントに割り当てます。
- address pool view でゲートウェイを指定し、secondary subnet view でゲートウェイを指定しない場合、DHCP は address pool view のゲートウェイアドレスをセカンダリサブネットのクライアントに割り当てます。

パラメータを指定しない場合、**undo gateway-list** コマンドはすべてのゲートウェイアドレスを削除します。

例

DHCP アドレスプール 0 のゲートウェイアドレス 10.1.1.1 を指定します。

<AC> system-view

[AC] dhcp server ip-pool 0

[AC-dhcp-pool-0] gateway-list 10.1.1.1

関連コマンド

display dhcp server pool

6.1.24 if-match

Syntax

if-match rule *rule-number* **{ hardware-address** *hardware-address* **mask** *hardware-address-mask* **| option** *option-code* **[ascii** *ascii-string* **[offset** *offset* **| partial] | hex** *hex-string* **[mask** *mask* **| offset** *offset* **length** *length* **| partial]] | relay-agent** *gateway-address* **}**

undo if-match rule *rule-number*

デフォルト

設定なし

View

DHCP user class view

定義済みユーザロール

network-admin

パラメータ

rule *rule-number*: ルールに割り当てる ID を指定します。値の範囲は 1～128 までで、ID が小さいほど、一致の優先度が高くなります。

hardware-address *hardware-address*: ハードウェアアドレスをハイフンで区切られた 16 進数の文字列で指定します。値の範囲は 4～39 文字です。最後の 16 進数は 2 桁または 4 桁で、その他の 16 進数は 4 桁である必要があります。たとえば、aabb-ccdd-ee は有効で、aabb-c-dddd または aabb-cc-dddd は無効です。

mask *hardware-address-mask*: *hardware-address* と AND 演算するマスクを指定します。マスクの長さはハードウェアアドレスと同じである必要があります。

option *option-code*: DHCP オプションの番号を指定します。1～254 の数値で指定します。

ascii *ascii-string*: ASCII 文字列を指定します。1～128 文字の文字列で指定します。

offset *offset*: 一致操作が開始されるまでのオフセットをバイト単位で指定します。値の範囲は 0～254 です。オフセット値を指定しない場合は、オプション内容の先頭バイトから照合が開始されます。ASCII 文字列を指定した場合、オフセット後のオプションの内容が ASCII 文字列と同じであれば、パケットはルールに一致します。16 進数を指定した場合、オフセット後の指定した長さのオプション内容が 16 進数と同じであれば、パケットはルールに一致します。

partial: 部分一致を有効にします。パケット内の指定されたオプションに、ルールで指定された ASCII 文字列または 16 進数が含まれている場合、パケットはルールに一致します。たとえば、ルールで abc を指定した場合、オプションの内容 xabc、xyzabca、xabcyz、および abcxyz はすべてルールに一致します。

hex *hex-string*: 16 進数の文字列を指定します。16 進数の文字列の長さは 2～256 までの偶数である必要があります。

mask *mask*: 一致操作の 16 進数マスクを指定します。マスク長は 2～256 までの偶数で、*hex-string* の文字列長と同じである必要があります。DHCP サーバは、マスク長のオプション内容を先頭から選択し、選択したオプション内容と指定した 16 進数をマスクと AND 演算します。2 つの AND 演算結果が同じ場合、パケットはルールと一致します。

length *length*: 照合するオプション内容の長さをバイト単位で指定します。値の範囲は 1～128 です。長さは、16 進文字列の長さと同じである必要があります。

relay-agent *gateway-address*: giaddr フィールドの値を指定します。値はドット付き 10 進表記の IPv 4 アドレスです。パケットの giaddr フィールド値がルールの値と同じ場合、パケットはルールに一致します。

説明

if-match コマンドは DHCP ユーザクラスの一致ルールを設定します。

undo if-match コマンドは DHCP ユーザクラスの一致ルールを削除します。

DHCP クライアントから送信された DHCP-DISCOVER パケットが DHCP ユーザクラスのルールと一致する場合、DHCP クライアントはユーザクラスと一致します。

1 つの DHCP ユーザクラスに対して複数の一致ルールを設定できます。

各一致ルールは、そのタイプ内のルール ID によって一意に識別されます(ハードウェアアドレス、オプション、またはリレーエージェントアドレス)。

- 設定しているルールの ID とタイプが既存のルールと同じ場合、新しいルールによって既存のルールが上書きされます。
- 設定するルールの ID が既存のルールと同じで、タイプが異なる場合は、新しいルールが有効になり、既存のルールと共存します。ベストプラクティスとして、異なるタイプのルールに同じ ID を割り当てないでください。
- 異なる ID のルールが同じルール内容を持つことはできません。

if-match hardware-address ルールを設定する場合は、次の注意事項に従ってください。

- ハードウェアアドレスタイプは、MAC アドレスのみをサポートします。他のタイプのハードウェアアドレスを持つクライアントでは、ルール一致となりません。
- 指定されたハードウェアアドレスは、クライアントハードウェアアドレスと同じ長さである必要があります。MAC アドレスと一致させるには、指定するハードウェアアドレスの長さを 6 バイトにする必要があります。
- ハードウェアアドレスのマスク内の、f と 0 は不連続にすることができます。たとえば、if-match rule 1 hardware-address 0094-0000-1100 mask ffff-0000-ff00 は、最初の 2 バイトが 0094 で、5 バイトが 11 のハードウェアアドレスと一致します。

if-match オプションルールを設定する場合は、次の注意事項に従ってください。

- オプションを含むパケットを照合するには、*option-code* の引数だけを指定します。
- AND 演算で 16 進数を一致させるには、option-code hex-string mask オプションを指定します。
- 16 進数を直接照合するには、オプション *option-code hex-string* [**offset** *offset* **length** *length* [**partial**] オプションを指定します。offset、length、または partial パラメータを指定しない場合、オプションの内容が 16 進数で始まると、パケットはルールに一致します。
- ASCII 文字列と一致させるには、*option-code* **ascii** *ascii-string* [**offset** *offset* [partial] オプションを指定します。offset または partial パラメータを指定しない場合、オプションの内容が ASCII 文字列で始まると、パケットはルールに一致します。

例

DHCP ユーザクラス test を作成し、その View に移行します。

<AC> system-view

[AC] dhcp class test

[AC-dhcp-class-test]

関連コマンド

- **class option-group**

if-match

6.1.25 nbns-list

Syntax

nbns-list *ip-address*&<1-8>

undo nbns-list [*ip-address*&<1-8>]

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-8>: WINS サーバの IP アドレスを指定します。&<1-8>は WINS サーバアドレスを半角スペースで区切り最大 8 つまで指定できることを示します。

説明

nbns-list コマンドは DHCP アドレスプールの WINS サーバアドレスを指定します。

undo nbns-list コマンドは指定した WINS サーバアドレスを削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

パラメータを指定しない場合、**undo nbns-list** コマンドはすべての WINS サーバアドレスを削除します。

例

DHCP アドレスプール 0 の WINS サーバアドレス 10.1.1.1 を指定します。

<AC> system-view

[AC] dhcp server ip-pool 0

[AC-dhcp-pool-0] nbns-list 10.1.1.1

関連コマンド

- **display dhcp server pool**
- **netbios-type**

6.1.26 netbios-type

Syntax

netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo netbios-type

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

b-node: ブロードキャストノードを指定します。b-node クライアントはサーバから名前-IP マッピングを取得するため、ブロードキャストメッセージで宛先名を送信します。

h-node: ハイブリッドノードを指定します。h-node クライアントは WINS サーバに宛先名をユニキャストします。応答を受信しない場合、h-node クライアントはサーバからマッピングを取得するため宛先名をブロードキャストします。

m-node: ミックスノードを指定します。m-node クライアントは宛先名をブロードキャストします。応答を受信しない場合、m-node クライアントはサーバからマッピングを取得するため宛先名をユニキャストします。

p-node: ピアツーピアノードを指定します。p-node クライアントは WINS サーバから WINS サーバを取得するため、ユニキャストメッセージの宛先アドレスを送信します。

説明

netbios-type コマンドは DHCP アドレスプールの NetBIOS ノードタイプを指定します。

undo netbios-type コマンドは指定した NetBIOS ノードタイプを削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

DHCP アドレスプール 0 の NetBIOS ノードタイプを p-node に指定します。

<AC> system-view

[AC] dhcp server ip-pool 0

[AC-dhcp-pool-0] netbios-type p-node

関連コマンド

- **display dhcp server pool**
- **nbns-list**

6.1.27 network

Syntax

network *network-address* [*mask-length* | **mask** *mask*] [**secondary**]

undo network *network-address* [*mask-length* | **mask** *mask*] [**secondary**]

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

network-address: ダイナミック割り当てのサブネットを指定します。マスク長やマスクが指定されない場合、ナチュラルマスクが使用されます。

mask-length: マスク長を指定します。設定範囲は 1～30 です。

mask *mask*: ドットで区切られた形式でマスクを指定します。

secondary: セカンダリサブネットを指定します。指定しない場合、プライマリサブネットを指定します。プライマリサブネットのアドレスが使い果たされている場合、DHCP サーバはクライアントのためにセカンダリサブネットからアドレスを選択します。

説明

network コマンドは DHCP アドレスプールのダイナミック割り当てのサブネットを指定します。

undo network コマンドは指定されたサブネットを削除します。

セカンダリサブネットを指定し、その view に移行するため、**secondary** を使用することができます。**gateway-list** コマンドを使用して DHCP クライアントのためにセカンダリサブネットのゲートウェイを指定することができます。

DHCP アドレスプールで 1 つのプライマリサブネットのみを指定することができます。コマンドを複数回設定した場合、最後に行った設定が適用されます。

DHCP アドレスプールで最大 32 のセカンダリサブネットを指定することができます。

DHCP アドレスプールのプライマリサブネットとセカンダリサブネットは同一ネットワークアドレス、マスクにすることができません。

アドレスプールで **address range** コマンドを使用した場合、同一のアドレスプールのセカンダリサブネットを指定することができません。

ネットワークの設定の変更あるいは削除を行うと現在のアドレスプールから割り当てられたアドレスを削除します。

例

DHCP アドレスプール 0 のプライマリサブネット 192.168.8.0/24 とセカンダリサブネット 192.168.10.0/24 を指定します。

<AC> system-view

[AC] dhcp server ip-pool 0

[AC-dhcp-pool-0] network 192.168.8.0 mask 255.255.255.0

[AC-dhcp-pool-0] network 192.168.10.0 mask 255.255.255.0 secondary

[AC-dhcp-pool-0-secondary]

関連コマンド

- **display dhcp server pool**
- **gateway-list**

6.1.28 next-server

Syntax

next-server *ip-address*

undo next-server

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address: サーバの IP アドレスを指定します。

説明

next-server コマンドは DHCP アドレスプールのサーバの IP アドレスを指定します。

undo next-server コマンドは DHCP アドレスプールからサーバの IP アドレスを削除します。

起動時、DHCP クライアントは IP アドレス、指定されたサーバの IP アドレスを取得します。他のブート情報を取得するため TFTP サーバのような指定されたサーバと連絡をとります。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

DHCP アドレスプール 0 のサーバの IP アドレス 10.1.1.254 を指定します。

<AC> system-view

[AC] dhcp server ip-pool 0

[AC-dhcp-pool-0] next-server 10.1.1.254

関連コマンド

display dhcp server pool

6.1.29 option

Syntax

option *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address*&<1-8> }

undo option *code*

デフォルト

設定なし

View

DHCP address pool view

DHCP option group view

定義済みユーザロール

network-admin

パラメータ

code: 自己定義されたオプション数を指定します。設定範囲は 2～254 です。50～54、56、58、59、61、62、82 を除きます。

ascii *ascii-string*: ASCII の文字列を指定します。設定範囲は 1～255 です。

hex *hex-string*: 16 進数の偶数番号を指定します。設定範囲は 2～256 です。

ip-address *ip-address*&<1-8>: 自己定義されたオプションの IP アドレスを指定します。&<1-8>は IP アドレスを半角スペースで区切り最大 8 つまで指定できることを示します。

説明

option コマンドは自己定義された DHCP オプションを設定します。

undo option コマンドは自己定義された DHCP オプションを削除します。

DHCP サーバは ASCII 文字列、16 進数文字列、IP アドレスで自己定義されたオプションを記載し、DHCP 応答の自己定義されたオプションをクライアントに送信します。

以下の目的のためにオプションを定義することができます。

- 新しくリリースされたオプションを追加します。
- オプション 43 のようなベンダ指定のオプションを追加します。
- CLI によって設定できない、専用の設定コマンドのオプションを追加します。たとえば **option** *4* **ip-address** *1.1.1.1* コマンドで DHCP クライアントにタイムサーバアドレス 1.1.1.1 を定義することができます。
- DHCP オプションでは正確な要件を満たすことができない場合、既存の DHCP オプションを拡張します。たとえば、**dns-list** コマンドは 8 つの DNS サーバアドレスを設定することができます。8 つを超える DNS サーバを指定する場合、すべての DNS サーバで **option** *6* コマンドを使用する必要があります。

専用のコマンドと **option** コマンドの両方を使用して DHCP オプションを指定する場合、DHCP サーバは専用のコマンドで指定された内容を割り当てます。たとえば、DHCP サーバのアドレスが **dns-list** コマンドと **option** *6* コマンドで指定された場合、サーバは **dns-list** コマンドで指定されたアドレスを使用します。

DHCP オプショングループで設定された DHCP オプションは DHCP アドレスプールで設定された DHCP オプションより優先されます。

option コマンドで同じコードが指定された場合、最後に行った設定が適用されます。

例

アドレスプール 0 のログサーバアドレス 2.2.2.2 を指定するためオプション 7 を設定します。

<AC> system-view

[AC] dhcp server ip-pool 0

[AC-dhcp-pool-0] option 7 ip-address 2.2.2.2

関連コマンド

display dhcp server pool

6.1.30 reset dhcp server conflict

Syntax

reset dhcp server conflict [**ip** *ip-address*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: 指定された IP アドレスの競合に関する情報を削除します。指定しない場合、すべてのアドレスの競合に関する情報を削除します。

説明

reset dhcp server conflict コマンドは IP アドレスの競合に関する情報を削除します。

ダイナミックに割り当てられた IP アドレスが他のホストでスタティックに設定されたとき、アドレスの競合が発生します。アドレスプールの設定を修正した後、競合したアドレスは割り当て可能になります。これらのアドレスを割り当てるため、最初に競合に関する情報を削除するため、**reset dhcp server conflict** コマンドを使用します。

例

すべてのアドレスの競合に関する情報を削除します。

<AC> reset dhcp server conflict

関連コマンド

display dhcp server conflict

6.1.31 reset dhcp server expired

Syntax

reset dhcp server expired [**ip** *ip-address* | **pool** *pool-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: 期限が終了した IP アドレスを指定し、IP アドレスに関する割り当て情報を削除します。指定しない場合、すべてのアドレスの競合に関する情報を削除します。

pool *pool-name*: 指定したアドレスプールの期限が終了した IP アドレスの割り当て情報を削除します。設定範囲は 1～63 です。大文字、小文字は区別しません。指定しない場合､すべてのアドレスプールの期限が終了した IP アドレスの割り当て情報を削除します。

説明

reset dhcp server expired コマンドは期限が終了した IP アドレスの割り当て情報を削除します。

例

すべての期限が終了した IP アドレスの割り当て情報を削除します。

<AC> reset dhcp server expired

関連コマンド

display dhcp server expired

6.1.32 reset dhcp server ip-in-use

Syntax

reset dhcp server ip-in-use [**ip** *ip-address* | **pool** *pool-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: 指定した IP アドレスの割り当て情報を削除します。指定しない場合、すべての IP アドレスの割り当て情報を削除します。

pool *pool-name*: 指定したアドレスプールの割り当て情報を削除します。設定範囲は 1～63 です。大文字、小文字を区別しません。指定しない場合、すべてのアドレスプールの割り当て情報を削除します。

説明

reset dhcp server ip-in-use コマンドは IP アドレス、アドレスプールの割り当て情報を削除します。

reset dhcp server ip-in-use コマンドで割り当てられたスタティック割り当て情報を削除すると、スタティック割り当て情報は未割り当てのスタティック割り当て情報となります。

例

IP アドレス 10.110.1.1 の割り当て情報を削除します。

<AC> reset dhcp server ip-in-use ip 10.110.1.1

関連コマンド

display dhcp server ip-in-use

6.1.33 reset dhcp server statistics

Syntax

reset dhcp server statistics

View

User view

定義済みユーザロール

network-admin

説明

reset dhcp server statistics コマンドは DHCP サーバの統計情報を削除します。

例

DHCP サーバの統計情報を削除します。

<AC> reset dhcp server statistics

関連コマンド

display dhcp server statistics

6.1.34 static-bind

Syntax

static-bind ip-address *ip-address* [*mask-length* | **mask** *mask*] { **client-identifier** *client-identifier* | **hardware-address** *hardware-address* [**ethernet** | **token-ring**] }

undo static-bind ip-address *ip-address*

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address *ip-address*: スタティック割り当ての IP アドレスを指定します。マスク長あるいはマスクが指定されない場合、ナチュラルマスクが使用されます。

mask-length: マスク長を指定します。設定範囲は 1〜30 です。

mask *mask*: ドットで区切られた形式でマスクを指定します。

client-identifier *client-identifier*: スタティック割り当てのクライアント ID を指定します。設定範囲は 4〜254 文字です。形式は H-H-H で、16 進数の数字とハイフン（-）で構成されます。最後の H は 2 桁あるいは 4 桁の 16 進数にすることができますが、それ以外の H は 4 桁の 16 進数の文字にする必要があります。たとえば、aabb-cccc-dd は有効な ID ですが、aabb-c-dddd や aabb-cc-dddd は無効な ID です。

hardware-address *hardware-address*: スタティック割り当てのクライアントのハードウェアアドレスを指定します。設定範囲は 4〜39 文字です。形式は H-H-H で、16 進数の数字とハイフン（-）で構成されます。最後の H は 2 桁あるいは 4 桁の 16 進数にすることができますが、それ以外の H は 4 桁の 16 進数の文字にする必要があります。たとえば、aabb-cccc-dd は有効なハードウェアアドレスですが、aabb-c-dddd や aabb-cc-dddd は無効なハードウェアアドレスです。

ethernet: クライアントのハードウェアアドレスのタイプを Ethernet に指定します。デフォルトタイプは Ethernet です。

token-ring: クライアントのハードウェアアドレスのタイプを Token Ring に指定します。

説明

static-bind コマンドはクライアント ID あるいは MAC アドレスを IP アドレスにスタティックに割り当てます。

undo static-bind コマンドはスタティックの割り当てを削除します。

スタティック割り当ての IP アドレスは DHCP サーバのインタフェースのアドレスにすることはできません。そうでなければ、IP アドレスの競合が発生すると、境界のクライアントは IP アドレスを取得することができません。

アドレスプールのスタティック割り当てを複数指定することができます。アドレスプールのスタティック割り当ては最大 8192 です。

スタティックの割り当てを修正することはできません。DHCP クライアントの割り当てを変更する場合、最初に既存の割り当てを削除し、新しい割り当てを作成してください。

例

DHCP アドレスプール 0 の IP アドレス 10.1.1.1/24 をクライアント ID が 00aa-aabb のクライアント ID に割り当てます。

<AC> system-view

[AC] dhcp server ip-pool 0

[AC-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0 client-identifier 00aa-aabb

関連コマンド

display dhcp server pool

6.1.35 tftp-server domain-name

Syntax

tftp-server domain-name *domain-name*

undo tftp-server domain-name

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

domain-name: TFTP サーバ名を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。

説明

tftp-server domain-name コマンドは DHCP アドレスプールの TFTP サーバ名を指定します。

undo tftp-server domain-name コマンドは DHCP アドレスプールの TFTP サーバ名を削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

DHCP アドレスプール 0 の TFTP サーバ aaa を指定します。

<AC> system-view

[AC] dhcp server ip-pool 0

[AC-dhcp-pool-0] tftp-server domain-name aaa

関連コマンド

- **display dhcp server pool**
- **tftp-server ip-address**

6.1.36 tftp-server ip-address

Syntax

tftp-server ip-address *ip-address*

undo tftp-server ip-address

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address: TFTP サーバの IP アドレスを指定します。

説明

tftp-server ip-address コマンドは DHCP アドレスプールの TFTP サーバアドレスを指定します。

undo tftp-server ip-address コマンドは DHCP アドレスプールの TFTP サーバアドレスを削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

DHCP アドレスプール 0 の TFTP サーバアドレス 10.1.1.1 を指定します。

<AC> system-view

[AC] dhcp server ip-pool 0

[AC-dhcp-pool-0] tftp-server ip-address 10.1.1.1

関連コマンド

- **display dhcp server pool**
- **tftp-server domain-name**

6.1.37 voice-config

Syntax

voice-config { **as-ip** *ip-address* | **fail-over** *ip-address dialer-string* | **ncp-ip** *ip-address* }

undo voice-config [**as-ip** | **fail-over** | **ncp-ip** | **voice-vlan**]

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

as-ip *ip-address*: バックアップのネットワークコーリングプロセッサの IP アドレスを指定します。

fail-over *ip-address dialer-string*: フェイルオーバ IP アドレスとダイヤル文字列を指定します。設定範囲は 1～39 です。0～9 の数字、アスタリスク（*）が含まれます。

ncp-ip *ip-address*: プライマリのネットワークコーリングプロセッサの IP アドレスを指定します。

説明

voice-config コマンドは DHCP アドレスプールのオプション 184 の内容を設定します。

undo voice-config コマンドは DHCP アドレスプールのオプション 184 の内容を削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

DHCP アドレスプール 0 のオプション 184 を設定します。プライマリのネットワークコーリングプロセッサの IP アドレスを 10.1.1.1、セカンダリのネットワークコーリングプロセッサの IP アドレスを 10.2.2.2 に設定します。フェイルオーバ IP アドレスは 10.3.3.3 です。ダイヤル文字列は 99*です。

<AC> system-view

[AC] dhcp server ip-pool 0

[AC-dhcp-pool-0] voice-config ncp-ip 10.1.1.1

[AC-dhcp-pool-0] voice-config as-ip 10.2.2.2

[AC-dhcp-pool-0] voice-config fail-over 10.3.3.3 99*

関連コマンド

display dhcp server pool

目次

このセクションのページは **5-x-x** です。

7 章 DHCP リレー 7-1
7.1 DHCP リレーエージェント設定コマンド 7-1
7.1.1 dhcp relay client-information record 7-1
7.1.2 dhcp relay client-information refresh enable 7-2
7.1.3 dhcp relay information circuit-id 7-3
7.1.4 dhcp relay information enable 7-5
7.1.5 dhcp relay information remote-id 7-6
7.1.6 dhcp relay information strategy 7-8
7.1.7 dhcp relay release ip 7-9
7.1.8 dhcp relay server-address 7-10
7.1.9 display dhcp relay client-information 7-11
7.1.10 display dhcp relay information 7-12
7.1.11 display dhcp relay server-address 7-14
7.1.12 display dhcp relay statistics 7-15
7.1.13 reset dhcp relay client-information 7-17
7.1.14 reset dhcp relay statistics 7-17

7章 DHCP リレー

7.1 DHCPリレーエージェント設定コマンド

7.1.1 dhcp relay client-information record

Syntax

dhcp relay client-information record

undo dhcp relay client-information record

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

dhcp relay client-information record コマンドはリレーエントリのクライアント情報の記録を有効にします。

undo dhcp relay client-information コマンドはリレーエントリのクライアント情報の記録を無効にします。

DHCP リレーエージェントが DHCP クライアントのゲートウェイで設定されたときのみクライアント情報が記録されます。

リレーエントリはクライアントの IP アドレス、MAC アドレスのようなクライアントの情報が含まれます。

リレーエントリのクライアント情報の記録を無効にすると、記録されたすべてのリレーエントリを削除します。

例

リレーエントリのクライアント情報の記録を有効にします。

<AC> system-view

[AC] dhcp relay client-information record

関連コマンド

- **dhcp relay client-information refresh enable**

7.1.2 dhcp relay client-information refresh enable

Syntax

dhcp relay client-information refresh enable

undo dhcp relay client-information refresh enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

dhcp relay client-information refresh enable コマンドは DHCP リレーエージェントでダイナミックリレーエントリの定期的な更新を有効にします。

undo dhcp relay client-information refresh enable コマンドは DHCP リレーエージェントでダイナミックリレーエントリの定期的な更新を無効にします。

DHCP クライアントは DHCP サーバに IP アドレスをリリースするため、DHCP-RELEASE メッセージをユニキャストします。

DHCP リレーエージェントは DHCP サーバにメッセージを送信し、クライアントの IP-MAC アドレスエントリを削除しません。

この機能で、DHCP リレーエージェントは DHCP サーバに DHCP-REQUEST メッセージを定期的に送信するため、クライアントの IP アドレス、リレーインタフェースの MAC アドレスを使用します。

- サーバが DHCP-ACK メッセージを送信する、あるいは時間以内にメッセージを返信しない場合、DHCP リレーエージェントは以下の処理を行います。
  - □ リレーエントリを削除します。
  - □ IP アドレスをリリースするため、DHCP サーバに DHCP-RELEASE メッセージを送信します。
- サーバが DHCP-NAK メッセージを返信する場合、リレーエージェントはエントリを保持します。

この機能が無効である場合、DHCP リレーエージェントは自動でリレーエントリを削除しません。DHCP クライアントが IP アドレスをリリースしたのち、対応するリレーエントリを削除するため、リレーエージェントで **reset dhcp relay client-information** コマンドを使用する必要があります。

例

DHCP リレーエージェントでダイナミックリレーエントリの定期的な更新を無効にします。

<AC> system-view

[AC] undo dhcp relay client-information refresh enable

関連コマンド

- **dhcp relay client-information record**
- **reset dhcp relay client-information**

7.1.3 dhcp relay information circuit-id

Syntax

dhcp relay information circuit-id { **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] } [**format** { **ascii** | **hex** }] }

undo dhcp relay information circuit-id

デフォルト

コードモードは normal で、パディング形式は hex です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

string *circuit-id*: circuit ID サブオプションの内容を指定します。設定範囲は 3～63 です。大文字、小文字を区別します。

normal: コードモードを normal モードに指定します。このパディングの内容は VLAN ID とポート番号から構成されます。

verbose: コードモードを verbose モードに指定します。このパディングの内容はノード識別子、インタフェース情報、VLAN ID が含まれます。デフォルトのノード識別子はアクセスノードの MAC アドレスです。デフォルトのインタフェース情報は Ethernet タイプ（eth で固定です）、シャーシ番号、サブスロット番号、インタフェース番号が含まれます。

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: アクセスノードの識別子を指定します。

- **mac**: ノード識別子として MAC アドレスを使用します。デフォルトのノード識別子です。
- **sysname**: ノード識別子として装置名を使用します。装置名は system view の **sysname** コマンドを使用して設定することができます。装置名のパディング形式は指定したパディング形式に関わらず、常に ASCII です。

🕮 **メモ：**

ノード識別子として **sysname** を指定した場合、装置名を設定するときに半角スペースを含むことができません。そうでなければ、DHCP リレーエージェントはオプション 82 の追加あるいは置き換えに失敗します。

- **user-defined** *node-identifier*: ユーザ定義のノード識別子を使用します。設定範囲は 1～50 です。大文字、小文字を区別します。指定された文字列のパディング形式は指定したパディング形式に関われず、常に ASCII になります。

format: circuit ID サブオプションのコードタイプを指定します。

ascii: ASCII コードタイプを指定します。

hex: hex のコードタイプを指定します。

説明

dhcp relay information circuit-id コマンドはオプション 82 の circuit ID サブオプションのパディング内容とパディング形式を設定します。

undo dhcp relay information circuit-id コマンドはデフォルトに戻します。

Circuit ID サブオプションでは、インタフェース分割やサブインタフェースに関する情報を伝達することはできません。インタフェース分割やサブインタフェースの追加情報は、オペレーションマニュアルのセクション 3 *インタフェース “Ethernet インタフェース”* を参照ください。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

ユーザ定義、normal モード、verbose モードのパディング形式はコマンドの設定によって変わります。表 7-1 に異なるモードのパディング形式を示します。

表 7-1 異なるモードのパディング形式

キーワード（モード）	パディング形式が指定されていない場合	パディング形式が ASCII	パディング形式が hex
string *circuit-id*	パディング形式を指定できません。常にASCIIになります。	–	–
normal	hex	ASCII	hex

キーワード（モード）	パディング形式が指定されていない場合	パディング形式がASCII	パディング形式が hex
verbose	VLAN IDはhexです。 ノード識別子、Ethernetタイプ、インタフェース番号はASCIIです。	ASCII	ノード識別子とEthernetタイプはASCIIです。 インタフェース番号とVLAN IDはhexです。

例

circuit ID サブオプションのコードモードが verbose、ノード識別子が装置名、パディング形式が ASCII に指定します。

<AC> system-view

[AC] interface vlan-interface 10

[AC-Vlan-interface10] dhcp relay information enable

[AC-Vlan-interface10] dhcp relay information strategy replace

[AC-Vlan-interface10] dhcp relay information circuit-id verbose node-identifier sysname format ascii

関連コマンド

- **dhcp relay information enable**
- **dhcp relay information strategy**
- **display dhcp relay information**

7.1.4 dhcp relay information enable

Syntax

dhcp relay information enable

undo dhcp relay information enable

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

説明

dhcp relay information enable コマンドはリレーエージェントでオプション 82 のサポートを有効にします。

undo dhcp relay information enable コマンドはオプション 82 のサポートを無効にします。

本コマンドによって DHCP リレーエージェントが DHCP サーバに要求を転送する前に、オプション 82 が含まれない DHCP 要求にオプション 82 を追加します。オプション 82 の内容は **dhcp relay information circuit-id** コマンド、**dhcp relay information remote-id** コマンドによって決まります。DHCP 要求にオプション 82 が含まれる場合、リレーエージェントは **dhcp relay information strategy** コマンドで設定された方法にしたがって DHCP 要求を処理します。

本機能が無効である場合、リレーエージェントはオプション 82 を含む DHCP 要求とオプション 82 を含まない DHCP 要求を DHCP サーバに転送します。

例

オプション 82 のサポートを有効にします。

<AC> system-view

[AC] interface vlan-interface 10

[AC-Vlan-interface10] dhcp relay information enable

関連コマンド

- **dhcp relay information circuit-id**
- **dhcp relay information remote-id**
- **dhcp relay information strategy**
- **display dhcp relay information**

7.1.5 dhcp relay information remote-id

Syntax

dhcp relay information remote-id { { **ap-mac** | **ap-mac-ssid** | **normal** } [**format** { **ascii** | **hex** }] | **ap-name** | **ap-name-ssid** | **string** *remote-id* | **sysname** }

undo dhcp relay information remote-id

デフォルト

コードモードは normal で、パディング形式は hex です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ap-mac：リモート ID のサブオプションを AP の MAC アドレスで埋め込むよう指定します。

ap-mac-ssid：リモート ID サブオプションにコロン（:）で区切られた AP の MAC アドレスと SSID を埋め込むよう指定します。SSID の詳細については、オペレーションマニュアルのセクション 2 *WLAN “WLAN アクセスの設定”* を参照してください。

normal: コードモードを normal モードに指定します。このパディングの内容は受信インタフェースの MAC アドレスです。

format: remote ID サブオプションのコードタイプを指定します。デフォルトのコードタイプは hex です。

ascii: ASCII コードタイプを指定します。

hex: hex のコードタイプを指定します。

ap-name：リモート ID サブオプションに AP の名前を埋め込むよう指定します。AP 名の詳細については、オペレーションマニュアルのセクション 2 *WLAN “AP 管理”* を参照してください。

ap-name-ssid：リモート ID のサブオプションに、コロン（:）で区切られた AP の名前と SSID を埋め込むよう指定します。

string *remote-id*: remote ID サブオプションの内容を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。

sysname: リモート ID サブオプションの内容として装置名を指定します。装置名は **sysname** コマンドを使用して設定することができます。

説明

dhcp relay information remote-id コマンドはオプション 82 の remote ID サブオプションのパディング内容とパディング形式を設定します。

undo dhcp relay information remote-id コマンドはデフォルトに戻します。

パディング形式は、AP 名（**ap-name**）、AP 名と SSID（**ap-name-ssid**）、指定された文字列（**string**）、およびデバイス名（**sysname**）の ASCII 形式です。

AP MAC アドレス（**ap-mac**）、AP MAC アドレスと SSID（**ap-mac-ssid**）、および **normal** モードのパディング形式は、コマンドによって決まります。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

オプション 82 の remote ID サブオプションのパディング内容を device001 に指定します。

<AC> system-view

[AC] interface vlan-interface 10

[AC-Vlan-interface10] dhcp relay information enable

[AC-Vlan-interface10] dhcp relay information strategy replace

[AC-Vlan-interface10] dhcp relay information remote-id string device001

関連コマンド

- **dhcp relay information enable**
- **dhcp relay information strategy**
- **display dhcp relay information**

7.1.6 dhcp relay information strategy

Syntax

dhcp relay information strategy { **drop** | **keep** | **replace** }

undo dhcp relay information strategy

デフォルト

replace

View

Interface view

定義済みユーザロール

network-admin

パラメータ

drop: オプション 82 メッセージが含まれる DHCP メッセージを廃棄します。

keep: オプション 82 を含むメッセージをそのまま転送するよう指定します。

replace: 元のオプション 82 のメッセージを設定されたオプション 82 のメッセージに置き換えます。

説明

dhcp relay information strategy コマンドはDHCP リレーエージェントでオプション82が含まれるメッセージの処理方法を設定します。

undo dhcp relay information strategy コマンドはデフォルトに戻します。

本コマンドは DHCP 要求にオプション 82 が含まれる場合のみ適用されます。

DHCP 要求にオプション 82 が含まれない場合、DHCP リレーエージェントは DHCP サーバに DHCP 要求を転送する前、常に DHCP 要求にオプション 82 を追加します。

replace パラメータを指定した場合、オプション 82 のパディングモード、パディング形式を設定してください。**keep** パラメータあるいは **drop** パラメータを指定した場合、オプション 82 のパディングモード、パディング形式を設定する必要はありません。設定しても適用されません。

例

DHCP リレーエージェントでオプション 82 が含まれるメッセージの処理方法を keep に設定します。

<AC> system-view

[AC] interface vlan-interface 10

[AC-Vlan-interface10] dhcp relay information enable

[AC-Vlan-interface10] dhcp relay information strategy keep

関連コマンド

- **dhcp relay information enable**
- **display dhcp relay information**

7.1.7 dhcp relay release ip

Syntax

dhcp relay release ip *ip-address*

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: リリースされる IP アドレスを指定します。

説明

dhcp relay release ip コマンドは指定したクライアントの IP アドレスをリリースします。

本コマンドを実行した後、リレーエージェントは DHCP サーバに DHCP-RELEASE パケットを送信し、IP アドレスのリレーエントリを削除します。パケットを受信するとサーバは、IP アドレスをリリースするため、指定された IP アドレスの割り当て情報を削除します。

例

IP アドレス 1.1.1.1 をリリースします。

<AC> system-view

[AC] dhcp relay release ip 1.1.1.1

7.1.8 dhcp relay server-address

Syntax

dhcp relay server-address *ip-address*

undo dhcp relay server-address [*ip-address*]

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: DHCP サーバの IP アドレスを指定します。DHCP リレーエージェントは DHCP クライアントから受信した DHCP パケットを DHCP サーバに転送します。

説明

dhcp relay server-address コマンドは DHCP リレーエージェントの DHCP サーバを指定します。

undo dhcp relay server-address コマンドは DHCP サーバを削除します。

DHCP サーバを指定する IP アドレスは、DHCP リレーエージェントインタフェースの IP アドレスと同一のサブネット上に置くことはできません。その場合、DHCP クライアントは IP アドレスの取得に失敗します。

インタフェースで最大 8 つの DHCP サーバを指定することができます。DHCP リレーエージェントはクライアントからのパケットをすべての指定された DHCP サーバに転送します。

IP アドレスを指定しない場合、**undo dhcp relay server-address** コマンドはインタフェースのすべての DHCP サーバを削除します。

例

リレーエージェントの VLAN インタフェース 10 で DHCP サーバ 1.1.1.1 を指定します。

<AC> system-view

[AC] interface vlan-interface 10

[AC-Vlan-interface10] dhcp relay server-address 1.1.1.1

関連コマンド

- **dhcp select relay**
- **display dhcp relay interface**

7.1.9 display dhcp relay client-information

Syntax

display dhcp relay client-information [**interface** *interface-type interface-number* | **ip** *ip-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定されたインタフェースのリレーエントリを表示します。

ip *ip-address*: 指定された IP アドレスのリレーエントリを表示します。

説明

display dhcp relay client-information コマンドはリレーエージェントのリレーエントリを表示します。

dhcp relay client-information record コマンドが設定されているときのみ、DHCP リレーエージェントはリレーエントリを記録します。

パラメータを指定しなかった場合、本コマンドはリレーエージェントのすべてのインタフェースのリレーエントリを表示します。

例

リレーエージェントのすべてのリレーエントリを表示します。

<AC> display dhcp relay client-information

```
Total number of client-information items: 2
Total number of dynamic items: 1
Total number of temporary items: 1
IP address      MAC address     Type       Interface          VPN name
10.1.1.1        00e0-0000-0001  Dynamic    GE1/0/1            N/A
```

```
10.1.1.5        00e0-0000-0000   Temporary   Vlan2            N/A
```

表 7-2 コマンド出力

フィールド	説明
Total number of client-information items	リレーエントリの総数
Total number of dynamic items	ダイナミックリレーエントリの総数
Total number of temporary items	一時的リレーエントリの総数
IP address	DHCPクライアントのIPアドレス
MAC address	DHCPクライアントのMACアドレス
Type	リレーエントリタイプ • **Dynamic**—リレーエージェントはDHCPサーバからAck応答を受信した際にダイナミックリレーエントリを作成します。 • **Temporary**—リレーエージェントはDHCPクライアントらREQUESTパケットを受信した際に一時的なリレーエントリを作成します。
Interface	DHCPクライアントに接続されたレイヤ3インタフェース リレーエージェントにインタフェース情報がない場合、**N/A**と表示されます。
VPN name	DHCPクライアントが所属しているVPNインスタンス名 DHCPクライアントがVPNに所属していない場合、**N/A**と表示されます。 本フィールドは現在のソフトウェアバージョンでサポートしていません。

関連コマンド

- **dhcp relay client-information record**
- **reset dhcp relay client-information**

7.1.10 display dhcp relay information

Syntax

display dhcp relay information [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定したインタフェースのオプション 82 の設定情報を表示します。インタフェースを指定しない場合、すべてのインタフェースのオプション 82 の設定情報を表示します。

説明

display dhcp relay information コマンドは DHCP リレーエージェントのオプション 82 の設定情報を表示します。

例

すべてのインタフェースのオプション 82 の設定情報を表示します。

<AC> display dhcp relay information

```
Interface: Vlan-interface100
  Status: Enable
  Strategy: Replace
  Circuit ID Pattern: Verbose
  Remote ID Pattern: Sysname
  Circuit ID format-type: Undefined
  Remote ID format-type: ASCII
  Node identifier: aabbcc
Interface: Vlan-interface200
  Status: Enable
  Strategy: Replace
  Circuit ID Pattern: User Defined
  Remote ID Pattern: User Defined
  Circuit ID format-type: ASCII
  Remote ID format-type: ASCII
  User defined:
  Circuit ID: vlan100
  Remote ID: device001
```

表 7-3 コマンド出力

フィールド	説明
Interface	インタフェース名

フィールド	説明
Status	オプション82の状態 • **Enable**—DHCPリレーエージェントはオプション82のサポートが有効です。 • **Disable**—DHCPリレーエージェントはオプション82のサポートが無効です。
Strategy	要求メッセージの処理方法 **Option 82**、**Drop**、**Keep**、**Replace**が含まれます。
Circuit ID Pattern	circuit IDサブオプションのパディングモード **Verbose**、**Normal**、**User Defined**があります。
Remote ID Pattern	remote IDサブオプションのパディングモード **Sysname**、**Normal**、**User Defined**があります。
Circuit ID format-type	circuit IDサブオプションのパディング形式 **ASCII**、**Hex**、**Undefined**があります。
Remote ID format-type	remote IDサブオプションのパディング形式 **ASCII**、**Hex**、**Undefined**があります。
Node identifier	アクセスノード識別子
User defined	ユーザ定義サブオプションの内容
Circuit ID	circuit IDサブオプションのユーザ定義の内容
Remote ID	remote IDサブオプションのユーザ定義の内容

7.1.11 display dhcp relay server-address

Syntax

display dhcp relay server-address [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定されたインタフェースの DHCP サーバのアドレスを表示します。指定しない場合、DHCP リレーエージェントで動作するすべてのインタフェースの DHCP サーバのアドレスを表示します。

説明

display dhcp relay server-address コマンドはインタフェースに設定された DHCP サーバのアドレスを表示します。

例

すべてのインタフェースの DHCP サーバのアドレスを表示します。

<AC> display dhcp relay server-address

```
Interface name              Server IP address
GE1/0/1                     2.2.2.2
```

表 7-4 コマンド出力

フィールド	説明
Interface name	インタフェース名
Server IP address	DHCPサーバのIPアドレス

関連コマンド

dhcp relay server-address

7.1.12 display dhcp relay statistics

Syntax

display dhcp relay statistics [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定したインタフェースの DHCP パケットの統計情報を表示します。指定しない場合、DHCP リレーエージェントのすべての DHCP パケットの統計情報を表示します。

説明

display dhcp relay statistics コマンドは DHCP リレーエージェントの DHCP パケットの統計情報を表示します。

例

DHCP リレーエージェントのすべての DHCP パケットの統計情報を表示します。

<AC> display dhcp relay statistics

```
DHCP packets dropped:               0
DHCP packets received from clients:    0
   DHCPDISCOVER:                    0
   DHCPREQUEST:                     0
   DHCPINFORM:                      0
   DHCPRELEASE:                     0
   DHCPDECLINE:                     0
   BOOTPREQUEST:                    0
DHCP packets received from servers:    0
   DHCPOFFER:                       0
   DHCPACK:                         0
   DHCPNAK:                         0
   BOOTPREPLY:                      0
DHCP packets relayed to servers:       0
   DHCPDISCOVER:                    0
   DHCPREQUEST:                     0
   DHCPINFORM:                      0
   DHCPRELEASE:                     0
   DHCPDECLINE:                     0
   BOOTPREQUEST:                    0
DHCP packets relayed to clients:       0
   DHCPOFFER:                       0
   DHCPACK:                         0
   DHCPNAK:                         0
   BOOTPREPLY:                      0
DHCP packets sent to servers:          0
   DHCPDISCOVER:                    0
   DHCPREQUEST:                     0
   DHCPINFORM:                      0
   DHCPRELEASE:                     0
   DHCPDECLINE:                     0
   BOOTPREQUEST:                    0
DHCP packets sent to clients:          0
   DHCPOFFER:                       0
   DHCPACK:                         0
```

```
DHCPNAK:                        0
BOOTPREPLY:                     0
```

関連コマンド

reset dhcp relay statistics

7.1.13 reset dhcp relay client-information

Syntax

reset dhcp relay client-information [**interface** *interface-type interface-number* | **ip** *ip-address*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 指定されたインタフェースのリレーエントリを削除します。

ip *ip-address*: 指定された IP アドレスのリレーエントリを削除します。

説明

reset dhcp relay client-information コマンドは DHCP リレーエージェントのリレーエントリを削除します。

パラメータを指定しない場合、DHCP リレーエージェント上のすべてのリレーエントリを削除します。

例

DHCP リレーエージェントのすべてのリレーエントリを削除します。

<AC> reset dhcp relay client-information

関連コマンド

display dhcp relay client-information

7.1.14 reset dhcp relay statistics

Syntax

reset dhcp relay statistics [**interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 指定されたインタフェースの DHCP リレーエージェントの統計情報を削除します。指定しない場合、すべての DHCP リレーエージェントの統計情報を削除します。

説明

reset dhcp relay statistics コマンドは DHCP リレーエージェントの統計情報を削除します。

例

すべての DHCP リレーエージェントの統計情報を削除します。

<AC> reset dhcp relay statistics

関連コマンド

display dhcp relay statistics

目次

このセクションのページは **5-x-x** です。

8 章 DHCP クライアント 8-1
8.1 DHCP クライアント設定コマンド 8-1
8.1.1 dhcp client dad enable 8-1
8.1.2 dhcp client dscp 8-1
8.1.3 dhcp client user-defined request-list exclude 8-2
8.1.4 display dhcp client 8-3
8.1.5 ip address dhcp-alloc 8-7

8章 DHCP クライアント

8.1 DHCPクライアント設定コマンド

8.1.1 dhcp client dad enable

Syntax

dhcp client dad enable

undo dhcp client dad enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

dhcp client dad enable コマンドはアドレス重複の検出を有効にします。

undo dhcp client dad enable コマンドはアドレス重複の検出を無効にします。

DHCP クライアントは、ARP パケットを使用して IP アドレスの重複があるかどうかを検出します。攻撃者は、サーバが割り当てた IP アドレスを使用できなくさせるため、ARP 応答を送信し、IP アドレスの所有者として動作します。ARP 攻撃がネットワークに存在する場合、アドレス重複検出機能を無効にすることを推奨します。

例

アドレス重複の検出を無効にします。

<AC> system-view

[AC] undo dhcp client dad enable

8.1.2 dhcp client dscp

Syntax

dhcp client dscp *dscp-value*

undo dhcp client dscp

デフォルト

56

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: DHCP パケットの DSCP を設定します。設定範囲は 0～63 です。

説明

dhcp client dscp コマンドは DHCP クライアントによって送信される DHCP パケットの DSCP 値を設定します。

undo dhcp client dscp コマンドはデフォルトに戻します。

パケットの DSCP 値はパケットのプライオリティを指定し、パケットを送信するプライオリティに影響します。DSCP 値が大きくなると優先度が高くなります。

例

DHCP クライアントによって送信される DHCP パケットの DSCP 値を 30 に設定します。

<AC> system-view

[AC] dhcp client dscp 30

8.1.3 dhcp client user-defined request-list exclude

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.85a を含む以降のソフトウェアからサポートしています。

Syntax

dhcp client user-defined request-list exclude *option-code*&<1-n>

undo client user-defined request-list exclude

デフォルト

Option55 は全てのデフォルトオプションが含まれています

View

Interface view

定義済みユーザロール

network-admin

パラメータ

option-code&<1-n>: Option55 から削除するデフォルトオプションを指定します。&<1-n> はスペース区切りで複数のオプションを指定できることを示します。指定できる最大数は装置により異なります。

説明

dhcp client dscp コマンドはDHCP クライアントによって送信されるDHCP パケットのOption55 のデフォルトオプションから指定したデフォルトオプションを削除します。

undo dhcp client dscp コマンドはデフォルトに戻します。

オプション 55（パラメータリクエストリスト）は、クライアントが DHCP サーバから取得したいネットワーク構成パラメータを指定するために使用されます。

このオプションには、クライアントが必要とするパラメータのオプション値が含まれています。 デフォルトでは、クライアントリクエストのオプション 55 にはデフォルトのオプションセットが含まれています。

しかし、これらのデフォルトのオプションセットには、運用上不要なパラメータが含まれている場合があります。

この機能を利用すると、オプション 55 から指定したデフォルトオプションを削除し、DHCP サーバに必要なパラメータだけを要求することが出来ます。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

VLAN インタフェース 10 で、DHCP クライアントによって送信される DHCP パケットのオプション 55 からデフォルトオプション 150 を削除します。

<AC> system-view

[AC] interface vlan-interface 10

[AC-Vlan-interface10] dhcp client user-defined request-list exclude 150

8.1.4 display dhcp client

Syntax

display dhcp client [**verbose**] [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose: DHCP クライアントの詳細情報を表示します。

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

説明

display dhcp client コマンドは DHCP クライアントの情報を表示します。

インタフェースを指定しなかった場合、すべてのインタフェースの DHCP クライアントの情報を表示します。

例

すべてのインタフェースの DHCP クライアントの情報を表示します。

<AC> display dhcp client

```
Vlan-interface10 DHCP client information:
 Current state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 DHCP server: 40.1.1.2
```

DHCP クライアントの詳細情報を表示します。

<AC> display dhcp client verbose

```
Vlan-interface10 DHCP client information:
 Current state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 Lease from May 21 19:00:29 2012   to   May 24 19:00:29 2012
 DHCP server: 40.1.1.2
 Transaction ID: 0x1c09322d
 Default router: 40.1.1.2
 Classless static routes:
   Destination: 1.1.0.1, Mask: 255.0.0.0, NextHop: 192.168.40.16
   Destination: 10.198.122.63, Mask: 255.255.255.255, NextHop: 192.168.40.16
 DNS servers: 44.1.1.11 44.1.1.12
 Domain name: ddd.com
 Boot servers: 200.200.200.200  1.1.1.1
 ACS parameter:
```

```
  URL: http://192.168.1.1:7547/acs
  Username: bims
  Password: ******
Client ID type: acsii(type value=00)
Client ID value: 000c.29d3.8659-Vlan10
Client ID (with type) hex: 0030-3030-632e-3239-
                      6433-2e38-3635-392d-
                      4574-6830-2f30-2f32
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.
```

表 8-1 コマンド出力

フィールド	説明
Vlan-interface10 DHCP client information	DHCPクライアントを提供するインタフェースの情報
Current state	DHCPクライアントの現在の状態 • **HALT**—クライアントがIPサービスの適用を停止します。 • **INIT**—初期化状態です。 • **SELECTING**—クライアントがDHCPサーバを検索するため、DHCP-DISCOVERメッセージを送信し、DHCPサーバからの応答を待っています。 • **REQUESTING**—クライアントがIPアドレスを要求するDHCP-REQUESTメッセージを送信し、DHCPサーバからの応答を待っています。 • **BOUND**—クライアントがDHCPサーバからDHCP-ACKメッセージを受信し、正常にIPアドレスを受信しました。 • **RENEWING**—T1タイマがタイムアウトしました。 • **REBOUNDING**— T2タイマがタイムアウトしました。
Allocated IP	DHCPサーバによって割り当てられたIPアドレス
Allocated lease	割り当てられたリース時間
T1	DHCPクライアントのIPアドレスの1/2リース時間（秒）
T2	DHCPクライアントのIPアドレスの7/8リース時間（秒）
Lease from….to….	リース開始時間と終了時間
DHCP server	IPアドレスを割り当てたDHCPサーバのIPアドレス
Transaction ID	トランザクションID IPアドレスの割り当てを識別するために、クライアントがランダムに選択する番号です。

フィールド	説明
Default router	クライアントに割り当てられるゲートウェイアドレス
Classless static routes	クライアントに割り当てられるクラスレススタティックルート
Static routes	クライアントに割り当てられるクラスフルスタティックルート
DNS servers	クライアントに割り当てられるDHCPサーバのアドレス
Domain name	クライアントに割り当てられるドメイン名サフィックス
Boot servers	DHCPクライアント用に指定されるPXEサーバアドレス（最大16アドレス） オプション43によって取得されます。
ACS parameter	ACSパラメータ
URL	ACSのURL
Username	ACSにログインするユーザ名
Password	ACSにログインするパスワード パスワードが設定されている場合、******と表示されます。パスワードが設定されていない場合、表示されません。
Client ID type	DHCPクライアントIDタイプ • クライアントIDとしてASCIIが使用されている場合、タイプの値は00です。 • クライアントIDとして指定したインタフェースのMACアドレスが使用されている場合、タイプの値は01です。 • クライアントIDとしてhexが使用されている場合、タイプの値は文字列の最初の2文字です。
Client ID value	DHCPクライアントIDの値
Client ID (with type) hex	typeフィールドによるクライアントID 16進数の文字列です。
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.	T1タイマ（1/2リース時間）がタイムアウトする時間

関連コマンド

- **dhcp client identifier**
- **ip address dhcp-alloc**

8.1.5 ip address dhcp-alloc

Syntax

ip address dhcp-alloc

undo ip address dhcp-alloc

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

説明

ip address dhcp-alloc コマンドは DHCP を使用して IP アドレスを取得するインタフェースを設定します。

undo ip address dhcp-alloc コマンドはインタフェースで DHCP の使用を停止します。

undo ip address dhcp-alloc コマンドを実行すると、インタフェースは DHCP を通して取得した IP アドレスをリリースするため、DHCP-RELEASE メッセージを送信します。インタフェースがダウンしている場合、メッセージを送信することができません。

例

DHCP を使用して IP アドレスを取得する VLAN インタフェース 10 を設定します。

<AC> system-view

[AC] interface vlan-interface 10

[AC-Vlan-interface10] ip address dhcp-alloc

関連コマンド

display dhcp client

目次

このセクションのページは **5-x-x** です。

9 章 DHCP スヌーピング 9-1
9.1 DHCP スヌーピング設定コマンド 9-1
9.1.1 dhcp snooping binding record 9-1
9.1.2 dhcp snooping enable 9-2
9.1.3 dhcp snooping information circuit-id 9-2
9.1.4 dhcp snooping information enable 9-5
9.1.5 dhcp snooping information remote-id 9-6
9.1.6 dhcp snooping information strategy 9-7
9.1.7 dhcp snooping trust 9-8
9.1.8 display dhcp snooping binding 9-9
9.1.9 display dhcp snooping information 9-10
9.1.10 display dhcp snooping packet statistics 9-12
9.1.11 display dhcp snooping trust 9-13
9.1.12 reset dhcp snooping binding 9-13
9.1.13 reset dhcp snooping packet statistics 9-14

9章 DHCP スヌーピング

9.1 DHCPスヌーピング設定コマンド

9.1.1 dhcp snooping binding record

Syntax

dhcp snooping binding record

undo dhcp snooping binding record

デフォルト

無効

View

Layer 2 Ethernet interface

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

dhcp snooping binding record コマンドは DHCP snooping エントリのクライアント情報の記録を有効にします。

undo dhcp snooping binding record コマンドは DHCP snooping エントリのクライアント情報の記録を無効にします。

このコマンドはクライアントに直接接続しているポートで DHCP snooping が DHCP snooping エントリのクライアント情報の記録することを有効にします。

例

GigabitEthernet 1/0/1 で DHCP snooping エントリのクライアント情報の記録を有効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] dhcp snooping binding record

9.1.2 dhcp snooping enable

Syntax

dhcp snooping enable

undo dhcp snooping enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

dhcp snooping enable コマンドは DHCP snooping を有効にします。

undo dhcp snooping enable コマンドは DHCP snooping を無効にします。

DHCP snooping 機能はトラステッドポートの設定と一緒に使用します。トラステッドポートを設定する前に、DHCP snooping のすべてのポートは非トラステッドポートで、装置は DHCP サーバから送信されたすべての応答を廃棄します。

DHCP snooping が無効であるとき、装置は DHCP サーバからの応答をすべて転送します。

例

DHCP snooping を有効にします。

<AC> system-view

[AC] dhcp snooping enable

9.1.3 dhcp snooping information circuit-id

Syntax

dhcp snooping information circuit-id { [**vlan** *vlan-id*] **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] } [**format** { **ascii** | **hex** }] }

undo dhcp snooping information circuit-id [**vlan** *vlan-id*]

デフォルト

パディングモードは normal で、パディング形式は hex です。

View

Layer 2 Ethernet interface

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id*: circuit ID サブオプションの VLAN ID を指定します。指定しない場合、デフォルト VLAN から受信したパケットの circuit ID サブオプションをパティングします。

string *circuit-id*: circuit ID サブオプションのパディング内容を指定します。設定範囲は 3～63 です。大文字、小文字を区別します。

normal: パディング形式を normal モードに指定します。このパディングの内容は VLAN ID とポート番号から構成されます。

verbose: パディング形式を verbose モードに指定します。パディング内容はノード識別子、Ethernet タイプ、インタフェース情報、VLAN ID が含まれます。デフォルトノードの識別子はアクセスノードの MAC アドレスです。デフォルトのインタフェース情報は Ethernet タイプ（eth で固定です）、シャーシ番号、スロット番号、サブスロット番号、インタフェース番号から構成されます。

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: アクセスノードの識別子を指定します。

- **mac**: ノード識別子としてアクセスノードの MAC アドレスを使用します。デフォルトのノード識別子です。
- **sysname**: ノード識別子として装置名を使用します。装置名は system view の **sysname** コマンドを使用して設定することができます。装置名のパディング形式は指定したパディング形式に関わらず、常に ASCII です。

🕮 **メモ：**

ノード識別子として **sysname** を指定した場合、装置名を設定するときに半角スペースを含むことができません。そうでなければ、DHCP snooping はオプション 82 の追加あるいは置き換えに失敗します。

- **user-defined** *node-identifier*: ユーザ定義のノード識別子を使用します。設定範囲は 1～50 です。大文字、小文字を区別します。指定された文字列のパディング形式は指定したパディング形式に関われず、常に ASCII になります。

format: circuit ID サブオプションのパディング形式を指定します。

ascii: パディング形式を ASCII に指定します。

hex: パディング形式を hex に指定します。

説明

dhcp snooping information circuit-id コマンドは circuit ID サブオプションのパディング内容とパディング形式を設定します。

undo dhcp snooping information circuit-id コマンドはデフォルトに戻します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

ユーザ定義、normal モード、verbose モードのパディング形式はコマンドの設定によって変わります。表 9-1 に異なるモードのパディング形式を示します。

表 9-1 異なるモードのパディング形式

キーワード（モード）	パディング形式が指定されていない場合	パディング形式が ASCII	パディング形式が hex
string *circuit-id*	パディング形式を指定できません。常にASCIIになります。	ー	ー
normal	hexです。	ASCIIです。	hexです。
verbose	VLAN IDはhexです。 ノード識別子、Ethernetタイプ、シャーシ番号、スロット番号、サブスロット番号、インタフェース番号はASCIIです。	ASCIIです。	ノード識別子、EthernetタイプはASCIIです。 シャーシ番号､スロット番号、サブスロット番号、インタフェース番号、VLAN IDはhexです。

例

circuit ID サブオプションのパディングモードが verbose、ノード識別子が装置名、パディング形式が ASCII として設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] dhcp snooping information enable

[AC-GigabitEthernet1/0/1] dhcp snooping information strategy replace

[AC-GigabitEthernet1/0/1] dhcp snooping information circuit-id verbose node-identifier sysname format ascii

関連コマンド

- **dhcp snooping information enable**
- **dhcp snooping information strategy**
- **display dhcp snooping information**

9.1.4 dhcp snooping information enable

Syntax

dhcp snooping information enable

undo dhcp snooping information enable

デフォルト

無効

View

Layer 2 Ethernet interface

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

dhcp snooping information enable コマンドは DHCP snooping でオプション 82 のサポートを有効にします。

undo dhcp snooping information enable コマンドは DHCP snooping でオプション 82 のサポートを無効にします。

このコマンドによって DHCP snooping が DHCP サーバに要求を転送する前に、オプション 82 が含まれない DHCP 要求にオプション 82 を追加します。オプション 82 の内容は **dhcp snooping information circuit-id** コマンド、**dhcp snooping information remote-id** コマンドによって決まります。受信した DHCP 要求にオプション 82 が含まれる場合、DHCP snooping は **dhcp snooping information strategy** コマンドで設定された方法にしたがってパケットを処理します。

例

DHCP snooping でオプション 82 のサポートを有効にします。

<AC> system-view

[AC] interface gigabitethernet1/0/1

[AC-GigabitEthernet1/0/1] dhcp snooping information enable

関連コマンド

- **dhcp snooping information circuit-id**
- **dhcp snooping information remote-id**
- **dhcp snooping information strategy**

9.1.5 dhcp snooping information remote-id

Syntax

dhcp snooping information remote-id { **normal** [**format** { **ascii** | **hex** }] | [**vlan** *vlan-id*] { **string** *remote-id* | **sysname** } }

undo dhcp snooping information remote-id [**vlan** *vlan-id*]

デフォルト

パディングモードは normal で、パディング形式は hex です。

View

Layer 2 Ethernet interface

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id*: remote ID サブオプションの VLAN ID を指定します。指定しない場合、デフォルト VLAN から受信したパケットの remote ID サブオプションをパティングします。

string *remote-id*: remote ID サブオプションのパディング内容を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。

sysname: remote ID サブオプションの内容として装置名を指定します。装置名は system view で **sysname** コマンドを使用して設定することができます。

normal: パディングモードを normal に指定します。このパディングの内容は受信インタフェースの MAC アドレスです。

format: remote ID サブオプションのパディング形式を指定します。デフォルトは hex です。

ascii: パディング形式を ASCII に指定します。

hex: パディング形式を hex に指定します。

説明

dhcp snooping information remote-id コマンドは remote ID サブオプションのパディングモードとパディング形式を設定します。

undo dhcp snooping information remote-id コマンドはデフォルトに戻します。

DHCP snooping は remote ID サブオプションの指定した文字列（**string**）あるいは装置名（**sysname**）に ASCII を使用します。normal モードのパディングモードはコマンドの設定によって変わります。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

remote ID サブオプションのパディング内容を device001 に指定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] dhcp snooping information enable

[AC-GigabitEthernet1/0/1] dhcp snooping information strategy replace

[AC-GigabitEthernet1/0/1] dhcp snooping information remote-id string device001

関連コマンド

- **dhcp snooping information enable**
- **dhcp snooping information strategy**
- **display dhcp snooping information**

9.1.6 dhcp snooping information strategy

Syntax

dhcp snooping information strategy { **drop** | **keep** | **replace** }

undo dhcp snooping information strategy

Default

replace

View

Layer 2 Ethernet interface

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

drop: オプション 82 メッセージが含まれる DHCP メッセージを廃棄します。

keep: オプション 82 を含むメッセージをそのまま転送するよう指定します。

replace: もとのオプション 82 のメッセージを設定されたオプション 82 のメッセージに置き換えします。

説明

dhcp snooping information strategy コマンドはオプション 82 が含まれる要求メッセージの処理方法を設定します。

undo dhcp snooping information strategy コマンドはデフォルトに戻します。

このコマンドは DHCP 要求にオプション 82 が含まれるときのみ適用します。DHCP 要求にオプション 82 が含まれない場合、DHCP サーバに転送する前に、DHCP snooping は DHCP 要求にオプション 82 を追加します。

replace パラメータを指定した場合、オプション 82 のパディングモード、パディング形式を設定します。**keep** パラメータあるいは **drop** パラメータを指定した場合、オプション 82 のパディングモード、パディング形式を設定する必要がありません。

例

オプション 82 が含まれる要求メッセージの処理方法を keep に設定します。

<AC> system-view

[AC] interface gigabitethernet1/0/1

[AC-GigabitEthernet1/0/1] dhcp snooping information enable

[AC-GigabitEthernet1/0/1] dhcp snooping information strategy keep

関連コマンド

- **dhcp snooping information circuit-id**
- **dhcp snooping information remote-id**

9.1.7 dhcp snooping trust

Syntax

dhcp snooping trust

undo dhcp snooping trust

デフォルト

DHCP snooping を有効にしたのち、すべてのポートが非トラステッドポートです。

View

Layer 2 Ethernet interface

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

dhcp snooping trust コマンドはトラステッドポートとしてポートを設定します。

undo dhcp snooping trust コマンドはポートをデフォルト状態に戻します。

DHCP クライアントが正常な IP アドレスを取得できるように、DHCP サーバに面しているポートをトラステッドポートに指定し、他のポートを非トラステッドポートに指定します。

例

トラステッドポートとして GigabitEthernet 1/0/1 を設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] dhcp snooping trust

関連コマンド

display dhcp snooping trust

9.1.8 display dhcp snooping binding

Syntax

display dhcp snooping binding [**ip** *ip-address* [**vlan** *vlan-id*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip *ip-address*: 指定された IP アドレスの DHCP snooping エントリを表示します。指定しない場合、すべての IP アドレスの DHCP snooping エントリを表示します。

vlan *vlan-id*: IP アドレスが存在する VLAN ID を指定します。指定しない場合、すべての VLAN の DHCP snooping エントリを表示します。

説明

display dhcp snooping binding コマンドは DHCP snooping エントリを表示します。

例

すべての DHCP snooping エントリを表示します。

<AC> display dhcp snooping binding

```
2 DHCP snooping entries found
IP address     MAC address    Lease       VLAN  SVLAN Interface
============== ============== ============ ===== ===== =================
```

```
1.1.1.7         0000-0101-0107 16907533    2     N/A   GE1/0/1
1.1.1.11        0000-0101-010b 16907537    2     N/A   GE1/0/3
```

表 9-2 コマンド出力

フィールド	説明
DHCP snooping entries found	DHCP snoopingエントリの数です。
IP address	DHCPクライアントに割り当てられたIPアドレスです。
MAC address	DHCPクライアントのMACアドレスです。
Lease	残りリース期間です。単位は秒です。
VLAN	DHCP snoopingとQinQの両方が有効、あるいはDHCPパケットに2つのVLANタグが含まれる場合、このフィールドは外部VLANタグを示します。そうでない場合、DHCPクライアントが存在するポートに接続しているVLANを示します。
SVLAN	DHCP snoopingとQinQの両方が有効、あるいはDHCPパケットに2つのVLANタグが含まれる場合、このフィールドは内部VLANタグを示します。そうでない場合、**N/A**と表示されます。
Interface	DHCPクライアントに接続されたポートです。

関連コマンド

- **dhcp snooping enable**
- **reset dhcp snooping binding**

9.1.9 display dhcp snooping information

Syntax

display dhcp snooping information { **all** | **interface** *interface-type interface-number* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべてのレイヤ 2 Ethernet インタフェースのオプション 82 の設定を表示します。

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

説明

display dhcp snooping information コマンドは DHCP snooping 装置のオプション 82 の設定を表示します。

例

すべてのインタフェースのオプション 82 の設定を表示します。

<AC> display dhcp snooping information all

```
Interface: Bridge-Aggregation1
  Status: Disable
  Strategy: Drop
  Circuit ID:
    Padding format: User Defined
      User defined: abcd
    Format: ASCII
  Remote ID:
    Padding format: Normal
    Format: ASCII
  VLAN 10:
    Circuit ID: abcd
    Remote ID: company
```

表 9-3 コマンド出力

フィールド	説明
Interface	インタフェース名です。
Status	オプション82の状態です。**Enable**あるいは**Disable**です。
Strategy	DHCP要求の処理方法です。 **Option 82**、**Drop**、**Keep**、**Replace**が含まれます。
Circuit ID	circuit IDサブオプションの内容です。
Padding format	オプション82のパディング形式です。 ● circuit IDサブオプションでは、パディング形式は**Normal**、**User Defined**、**Verbose (sysname)**、**Verbose (MAC)**、**Verbose (user defined)**があります。 ● remote IDサブオプションでは、パディング形式は**Normal**、**Sysname**、**User Defined**があります。
Node identifier	アクセスノード識別子です。
User defined	ユーザ定義サブオプションの内容です。

フィールド	説明
Format	オプション82サブオプションのコードタイプです。 ● circuit IDサブオプションでは、コードタイプはASCII、Default、Hexがあります。 ● remote IDサブオプションでは、コードタイプはASCII、Hexがあります。
Remote ID	circuit IDサブオプションの内容です。
VLAN	指定したVLANで受信したDHCPパケットのcircuit IDサブオプションとremote IDサブオプションのパディングです。

9.1.10 display dhcp snooping packet statistics

Syntax

display dhcp snooping packet statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display dhcp snooping packet statistics コマンドは DHCP snooping の DHCP パケットの統計情報を表示します。

例

DHCP snooping の DHCP パケットの統計情報を表示します。

<AC> display dhcp snooping packet statistics

```
DHCP packets received              : 100
DHCP packets sent                  : 200
Invalid DHCP packets dropped         : 0
```

関連コマンド

reset dhcp snooping packet statistics

9.1.11 display dhcp snooping trust

Syntax

display dhcp snooping trust

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display dhcp snooping trust コマンドはトラステッドポートの情報を表示します。

例

トラステッドポートの情報を表示します。

<AC> display dhcp snooping trust

```
DHCP snooping is enabled.
Interface                              Trusted
=========================              ============
GigabitEthernet1/0/1                   Trusted
```

関連コマンド

dhcp snooping trust

9.1.12 reset dhcp snooping binding

Syntax

reset dhcp snooping binding { **all** | **ip** *ip-address* [**vlan** *vlan-id*] }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべての DHCP snooping エントリを削除します。

ip *ip-address*: 指定された IP アドレスの DHCP snooping エントリを削除します。

vlan *vlan-id*: 指定された VLAN の DHCP snooping エントリを削除します。指定しない場合、デフォルト VLAN の DHCP snooping エントリを削除します。

説明

reset dhcp snooping binding コマンドは DHCP snooping エントリを削除します。

例

すべての DHCP snooping エントリを削除します。

<AC> reset dhcp snooping binding all

関連コマンド

display dhcp snooping binding

9.1.13 reset dhcp snooping packet statistics

Syntax

reset dhcp snooping packet statistics

View

User view

定義済みユーザロール

network-admin

説明

reset dhcp snooping packet statistics コマンドは DHCP snooping の DHCP パケットの統計情報を削除します。

例

DHCP snooping の DHCP パケットの統計情報を削除します。

<AC> reset dhcp snooping packet statistics

関連コマンド

display dhcp snooping packet statistics

目次

このセクションのページは **5-x-x** です。

10 章 BOOTP 10-1
10.1 BOOTP クライアント設定コマンド 10-1
10.1.1 display bootp client 10-1
10.1.2 ip address bootp-alloc 10-2

10章 BOOTP

10.1 BOOTPクライアント設定コマンド

10.1.1 display bootp client

Syntax

display bootp client [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

説明

display bootp client コマンドは BOOTP クライアントの情報を表示します。

インタフェースを指定しなかった場合、すべてのインタフェースの BOOTP クライアント情報を表示します。

例

VLAN インタフェース 10 の BOOTP クライアントの情報を表示します。

<AC> display bootp client interface vlan-interface 10

```
Vlan-interface10 BOOTP client information:
Allocated IP: 169.254.0.2 255.255.0.0
Transaction ID: 0x3d8a7431
MAC Address: 74ea-c8fd-c180
```

表 10-1 コマンド出力

フィールド	説明
Vlan-interface10 BOOTP client information	BOOTPクライアントとして動作するインタフェースの情報
Allocated IP	BOOTPサーバによって割り当てられたBOOTPクライアントのIPアドレス

フィールド	説明
Transaction ID	BOOTPメッセージのXIDフィールドの値 BOOTPクライアントがBOOTPサーバにBOOTP要求を送信するときにランダムに選択される番号です。この値はBOOTPサーバからの応答メッセージを一致させるために使用します。 BOOTP応答とBOOTP要求のXIDフィールドの値が異なる場合、BOOTPクライアントはBOOTP応答を廃棄します。
Mac Address	BOOTPクライアントのMACアドレス

関連コマンド

ip address bootp-alloc

10.1.2 ip address bootp-alloc

Syntax

ip address bootp-alloc

undo ip address bootp-alloc

デフォルト

インタフェースは IP アドレス取得のために BOOTP を使用しません。

View

Interface view

定義済みユーザロール

network-admin

説明

ip address bootp-alloc コマンドは IP アドレスを取得するために BOOTP を使用するインタフェースを設定します。

undo ip address bootp-alloc コマンドはインタフェースで BOOTP を使用することを停止します。

例

IP アドレスを取得するために BOOTP を使用する VLAN インタフェース 10 を設定します。

<AC> system-view

[AC] interface vlan-interface 10

[AC-Vlan-interface10] ip address bootp-alloc

関連コマンド

display bootp client

目次

このセクションのページは **5-x-x** です。

11 章 DNS 11-1
11.1 DNS 設定コマンド 11-1
11.1.1 display dns domain 11-1
11.1.2 display dns host 11-2
11.1.3 display dns server 11-3
11.1.4 dns domain 11-5
11.1.5 dns dscp 11-6
11.1.6 dns proxy enable 11-6
11.1.7 dns server 11-7
11.1.8 ip host 11-8
11.1.9 ip host interface 11-9
11.1.10 reset dns host 11-10

11章 DNS

11.1 DNS設定コマンド

11.1.1 display dns domain

Syntax

display dns domain [**dynamic**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dynamic: DHCP または他のプロトコルによってダイナミックに取得したドメイン名のサフィックスを表示します。指定しない場合、スタティックに設定したドメイン名のサフィックス、およびダイナミックに取得したドメイン名のサフィックスを表示します。

説明

display dns domain コマンドはドメイン名のサフィックスを表示します。

例

パブリックネットワークのドメイン名のサフィックスを表示します。

<AC> display dns domain

```
Type:
  D: Dynamic    S: Static

No.    Type   Domain suffix
1      S      com
2      D      net
```

表 11-1 コマンド出力

フィールド	説明
No.	シーケンス番号です。

フィールド	説明
Type	ドメイン名のサフィックスのタイプです。 • **S**—スタティックに設定されたドメイン名のサフィックスです。 • **D**—DHCPまたは他のプロトコルによってダイナミックに取得したドメイン名のサフィックスです。
Domain suffix	ドメイン名のサフィックスです。

関連コマンド

dns domain

11.1.2 display dns host

Syntax

display dns host [**ip**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip: タイプ A のクエリを指定します。タイプ A のクエリは IPv4 アドレスにドメイン名サフィックスをマッピングします。

説明

display dns host コマンドはドメイン名－IP アドレスのマッピングを表示します。

パラメータを指定しない場合、すべてのクエリタイプのドメイン名－IP アドレスのマッピングを表示します。

例

すべてのクエリタイプのドメイン名－IP アドレスのマッピングを表示します。

<AC> display dns host

```
Type:
  D: Dynamic    S: Static
```

```
Total number: 3
No.  Host name        Type  TTL       Query type   IP addresses
1    sample.com       D     3132      A            192.168.10.1
                                                    192.168.10.2
                                                    192.168.10.3
2    zig.sample.com   S     -         A            192.168.1.1
3    sample.net       S     -         AAAA         FE80::4904:4448
```

表 11-2 コマンド出力

フィールド	説明
No.	シーケンス番号です。
Host name	ドメイン名です。
Type	ドメイン名－IPアドレスマッピングのタイプです。 • **S**—**ip host**コマンドで設定されたスタティックマッピングです。 • **D**—ダイナミックドメイン名解決によってダイナミックに取得したマッピングです。
TTL	マッピングがキャッシュに記録できる時間です。単位は秒です。 スタティックマッピングの場合、ハイフン（-）が表示されます。
Query type	クエリタイプです。タイプA、タイプAAAAがあります。
IP addresses	応答したIPアドレスです。 • タイプAクエリでは、応答したIPアドレスはIPv4アドレスです。

関連コマンド

- **ip host**
- **reset dns host**

11.1.3 display dns server

Syntax

display dns server [**dynamic**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dynamic: DHCP あるいは他のプロトコルによってダイナミックに取得した IPv4 DNS サーバの情報です。指定しない場合、スタティックに設定された IPv4 DNS サーバとダイナミックに取得した IPv4 DNS サーバを表示します。

説明

display dns server コマンドは IPv4 DNS サーバの情報を表示します。

例

パブリックネットワークの IPv4 DNS サーバの情報を表示します。

<AC> display dns server

```
Type:
  D: Dynamic    S: Static

No. Type  IP address
1   S     202.114.0.124
2   S     169.254.65.125
```

表 11-3 コマンド出力

フィールド	説明
No.	シーケンス番号です。
Type	DNSサーバタイプです。 • **S**—スタティックに設定されたDNSサーバの情報です。 • **D**—DHCPあるいは他のプロトコルによってダイナミックに取得したDNSサーバの情報です。
IP address	DNSサーバのIPv4アドレスです。

関連コマンド

dns server

11.1.4 dns domain

Syntax

dns domain *domain-name*

undo dns domain *domain-name*

デフォルト

ドメイン名サフィックスは設定されていません。既定のドメイン名のみが解決できます。

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-name: ドメイン名サフィックスを指定します。ドメイン名サフィックスは、ドットにより区切られた文字列により構成されます。ドメイン名サフィックスは、大文字、小文字を区別しない文字、数字、ハイフン（-）、アンダーバー（_）、ドット（.）を使用することができます。たとえば、aabbcc.com です。合計の文字数は 253 文字までです。それぞれの区切られた文字列は 63 文字までです。

説明

dns domain コマンドはドメイン名サフィックスを設定します。

undo dns domain コマンドは指定されたドメイン名サフィックスを削除します。

システムはホスト解決を行うため、ホストから受信したドメイン名の順番でサフィックスを自動で追加します。

パブリックネットワークで最大 16 のドメイン名サフィックスを指定することができます。

例

パブリックネットワークのドメイン名サフィックス com を設定します。

<AC> system-view

[AC] dns domain com

関連コマンド

display dns domain

11.1.5 dns dscp

Syntax

dns dscp *dscp-value*

undo dns dscp

デフォルト

0

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: DSCP 値を指定します。設定範囲は 0～63 です。

説明

dns dscp コマンドは DNS クライアントあるいは DNS Proxy によって送信された DNS パケットの DSCP を設定します。

undo dns dscp コマンドはデフォルトに戻します。

DHCP パケットの DSCP の値はパケットのプライオリティを指定します。パケットを送信するプライオリティに影響します。DSCP の値が大きくなると、プライオリティが高くなります。

例

送信 DNS パケットの DSCP 値を 30 に設定します。

<AC> system-view

[AC] dns dscp 30

11.1.6 dns proxy enable

Syntax

dns proxy enable

undo dns proxy enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

dns proxy enable コマンドは DNS Proxy を有効にします。

undo dns proxy enable コマンドは DNS Proxy を無効にします。

例

DNS Proxy を有効にします。

<AC> system-view

[AC] dns proxy enable

11.1.7 dns server

Syntax

dns server *ip-address*

undo dns server [*ip-address*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: DNS サーバの IPv4 アドレスを指定します。

説明

dns server コマンドは DNS サーバの IPv4 アドレスを指定します。

undo dns server コマンドは DNS サーバの IPv4 アドレスを削除します。

装置はIPv4アドレスが指定された順番で、DNSサーバにDNSクエリ要求を送信します。

パブリックネットワークで最大 6 つの DNS サーバの IPv4 アドレスを指定することができます。

IPv4 アドレスを指定しない場合、**undo dns server** コマンドはパブリックネットワークのすべての DNS サーバの IPv4 アドレスを削除します。

例

DNS サーバの IPv4 アドレス 172.16.1.1 を指定します。

<AC> system-view

[AC] dns server 172.16.1.1

関連コマンド

display dns server

11.1.8 ip host

Syntax

ip host *host-name ip-address*

undo ip host *host-name ip-address*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

host-name: ホスト名を指定します。設定範囲は 1～253 です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含めることができます。

ip-address: ホストの IPv4 アドレスを指定します。

説明

ip host コマンドはホスト名－IPv4 アドレスマッピングを作成します。

undo ip host コマンドはマッピングを削除します。

最大 1024 のホスト名－IPv4 アドレスマッピングを作成することができます。

パブリックネットワークで各ホスト名は 1 つの IPv4 アドレスのみマッピングすることができます。コマンドを複数回設定した場合、最後に行った設定が適用されます。

ホスト名を使用して **ping** コマンドのパラメータ **ip**、**-a**、**-c**、**-f**、**-h**、**-i**、**-m**、**-n**、**-p**、**-q**、**-r**、**-s**、**-t**、**-tos**、**–v** を実行することができます。**ping** コマンドのパラメータの詳細はコ

マンドマニュアルのセクション 11 *システム管理 “システムの保守とデバッグ”* を参照してください。

例

パブリックネットワークの IPv4 アドレス 10.110.0.1 をホスト名 aaa にマッピングします。

<AC> system-view

[AC] ip host aaa 10.110.0.1

関連コマンド

display dns host

11.1.9 ip host interface

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.85a を含む以降のソフトウェアからサポートしています。

Syntax

ip host *host-name* **interface** *interface-type interface-number*

undo ip host *host-name* **interface** *interface-type interface-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

host-name: ホスト名を指定します。設定範囲は 1～253 です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含めることができます。

interface *interface-type interface-number*: インタフェースタイプと番号を指定します。

VLAN インタフェースを指定する必要があります。

説明

ip host interface コマンドは、ホスト名とインタフェースのマッピングを作成します。

undo ip host interface コマンドはホスト名とインタフェースのマッピングを削除します。

デバイスの Web 管理インタフェースにドメイン名を通じてアクセスするには、**ip host** コマンドを使用してホスト名と IPv4 アドレスのマッピングを作成し、デバイスが DHCP で取得した IP アドレスを指定します。しかし、デバイスが取得した IP アドレスが変更された場合、ドメイン名でデバイスの Web 管理インタフェースにアクセスできなくなります。

この機能を設定すると、デバイスが IP アドレスを取得した際に、システムがドメイン名と IP アドレスのマッピングを生成します。

デバイスが取得した IP アドレスが変更された場合、システムは自動的にドメイン名に対応する IP アドレスを更新します。

これにより、デバイスが取得した IP アドレスが変更されても、ユーザはドメイン名を通じてデバイスの Web 管理インタフェースにアクセスできます。

複数の IP アドレスを VLAN インタフェースが取得した場合、メイン IP アドレスがドメイン名に対応するアドレスとして使用されます。

同じホスト名に対して以下のコマンドを同時に設定することは出来ません。

- **ip host** *host-name ip-address*
- **ip host** *host-name* **interface** *interface-type interface-number*

同じホスト名が指定された場合最新の設定が有効になります。

例

ホスト名 aaa に対応する IP アドレスを Vlan-interface10 の IP アドレスとして設定します。

<AC> system-view

[AC] ip host aaa interface vlan-interface 10

関連コマンド

ip host

11.1.10 reset dns host

Syntax

reset dns host [**ip**]

View

User view

定義済みユーザロール

network-admin

パラメータ

ip: タイプ A のクエリを指定します。タイプ A のクエリは IPv4 アドレスにドメイン名サフィックスをマッピングします。

説明

reset dns host コマンドはダイナミック DNS キャッシュの情報を削除します。

パラメータを指定しない場合、すべてのクエリタイプのダイナミック DNS キャッシュ情報を削除します。

例

パブリックネットワークのすべてのクエリタイプのダイナミック DNS キャッシュ情報を削除します。

<AC> reset dns host

関連コマンド

display dns host

目次

このセクションのページは **5-x-x** です。

12 章 IP パフォーマンスの最適化.....12-1
12.1 IP パフォーマンスの最適化設定コマンド.....12-1
12.1.1 display icmp statistics 12-1
12.1.2 display ip statistics.....12-2
12.1.3 display rawip.....12-4
12.1.4 display rawip verbose 12-4
12.1.5 display tcp 12-8
12.1.6 display tcp statistics.....12-9
12.1.7 display tcp verbose 12-11
12.1.8 display udp 12-15
12.1.9 display udp statistics.....12-16
12.1.10 display udp verbose.....12-17
12.1.11 ip forward-broadcast 12-20
12.1.12 ip icmp error-interval 12-21
12.1.13 ip mtu 12-22
12.1.14 ip redirects enable 12-23
12.1.15 ip ttl-expires enable.....12-24
12.1.16 ip unreachables enable.....12-25
12.1.17 reset ip statistics 12-26
12.1.18 reset tcp statistics 12-27
12.1.19 reset udp statistics.....12-27
12.1.20 tcp path-mtu-discovery.....12-28
12.1.21 tcp timer fin-timeout 12-29
12.1.22 tcp timer syn-timeout.....12-29
12.1.23 tcp window.....12-30

12章 IP パフォーマンスの最適化

12.1 IPパフォーマンスの最適化設定コマンド

12.1.1 display icmp statistics

Syntax

display icmp statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display icmp statistics コマンドは ICMP パケットの送受信に関する統計情報を表示します。

例

ICMP の統計情報を表示します。

<AC> display icmp statistics

```
  Input: bad formats   0               bad checksum          0
        echo         175              destination unreachable 0
        source quench 0               redirects             0
        echo replies  201             parameter problem      0
        timestamp     0               information requests    0
        mask requests 0               mask replies           0
        time exceeded 0               invalid type           0
        router advert 0               router solicit         0
        broadcast/multicast echo requests ignored          0
        broadcast/multicast timestamp requests ignored      0
 Output: echo         0               destination unreachable 0
        source quench 0               redirects             0
        echo replies  175             parameter problem      0
        timestamp     0               information replies     0
        mask requests 0               mask replies           0
        time exceeded 0               bad address            0
        packet error  1442            router advert          3
```

12.1.2 display ip statistics

Syntax

display ip statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ip statistics コマンドは IP パケットの統計情報を表示します。

IP 統計情報はパケットの送受信、再構築に関する情報が含まれます。

例

IP パケットの統計情報を表示します。

<AC> display ip statistics

```
Input:   sum           7120           local           112
        bad protocol   0              bad format       0
        bad checksum   0              bad options      0
        dropped       0
Output:  forwarding     0              local           27
        dropped       0              no route         2
        compress fails 0
Fragment:input         0              output           0
        dropped       0
        fragmented     0              couldn't fragment 0
Reassembling:sum       0              timeouts         0
```

表 12-1 コマンド出力

フィールド	説明
Input	受信したパケットの統計情報です。 ● **sum**–受信したパケットの総数です。 ● **local**–装置へ送信されたパケットの総数です。 ● **bad protocol**–不明なプロトコルのパケットの総数です。 ● **bad format**–不正なフォーマットのパケットの総数です。 ● **bad checksum**–不正なチェックサムのパケットの総数です。 ● **bad options**–不正なオプションのパケットの総数です。 ● **dropped-**廃棄されたパケットの総数です。
Output	送信したパケットの統計情報です。 ● **forwarding**–転送されたパケットの総数です。 ● **local**–ローカルに送信されたパケットの総数です。 ● **dropped**–廃棄されたパケットの総数です。 ● **no route**–ルートが無効なパケットの総数です。 ● **compress fails**–圧縮に失敗したパケットの総数です。
Fragment	フラグメントパケットの統計情報です。 ● **input**–受信したフラグメントパケットの総数です。 ● **output**–送信したフラグメントパケットの総数です。 ● **dropped**–廃棄されたフラグメントパケットの総数です。 ● **fragmented**–正常にフラグメントされたパケットの総数です。 ● **couldn't fragment**–フラグメントに失敗したパケットの総数です。
Reassembling	リアセンブルパケットの統計情報です。 ● **sum**–リアセンブルしたパケットの総数です。 ● **timeouts**–一定時間内にリアセンブルできなかったパケットの総数です。

関連コマンド

- **display ip interface**
- **reset ip statistics**

12.1.3 display rawip

Syntax

display rawip

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display rawip コマンドは RawIP 接続の概要情報を表示します。

RawIP 接続の概要情報はローカルアドレス、ピアのアドレス、プロトコル、PCB が含まれます。

例

RawIP 接続の概要情報を表示します。

<AC> display rawip

```
Local Addr      Foreign Addr    Protocol  Slot  PCB
 0.0.0.0         0.0.0.0         1         1     0x0000000000000009
 0.0.0.0         0.0.0.0         1         1     0x0000000000000008
```

表 12-2 コマンド出力

フィールド	説明
Local Addr	ローカルIPアドレスです。
Foreign Addr	ピアのIPアドレスです。
Protocol	プロトコル番号です。
Slot	プロトコルコントロールブロックです。
PCB	ローカルIPアドレスです。

12.1.4 display rawip verbose

Syntax

display rawip verbose [**pcb** *pcb-index*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pcb *pcb-index*: 指定した PCB の RawIP 接続の詳細情報を表示します。*pcb-index* は PCB のインデックスを指定します。設定範囲は 16 進数で 1～ffffffffffffffff です。

説明

display rawip verbose コマンドは RawIP 接続の詳細情報を表示します。

RawIP 接続の詳細情報はソケット作成のタスク名、状態、オプション、タイプ、プロトコル番号、RawIP 接続の送信元 IP アドレス、RawIP 接続の宛先 IP アドレスが含まれます。

例

RawIP 接続の詳細情報を表示します。

<AC> display rawip verbose

```
Total RawIP socket number: 1


 Location:
 Creator: ping[320]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 9216 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 3
 Protocol: 1
 Connection info: src = 0.0.0.0, dst = 0.0.0.0
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV4
 TTL: 255(minimum TTL: 0)
 Send VRF: 0xffff
 Receive VRF: 0xffff
```

表 12-3 コマンド出力

フィールド	説明
Total RawIP socket number	RawIPソケットの総数です。
Location	ソケットを作成したタスク名です。括弧の数はタスク名の処理番号です。
Creator	ソケットのオプションです。
State	エラーコードです。

Options	以下の順番で受信バッファ情報を表示します。
	• **cc**–使用されているバッファ空間です。
	• **hiwat**–最大バッファ空間です。
	• **lowat**–最小バッファ空間です。
	• **drop**–パケット廃棄数です。
	• **state**–バッファ状態です。
	  • **CANTSENDMORE**–ピアにデータを送信できません。
	  • **CANTRCVMORE**–ピアからデータを受信できません。
	  • **RCVATMARK**–タグを受信しています。
	  • **N/A**–上記以外の状態です。

Error	以下の順番で送信バッファ情報を表示します。
	• **cc**–使用されているバッファ空間です。
	• **hiwat**–最大バッファ空間です。
	• **lowat**–最小バッファ空間です。
	• **state**–バッファ状態です。
	  • **CANTSENDMORE**–ピアにデータを送信できません。
	  • **CANTRCVMORE**–ピアからデータを受信できません。
	  • **RCVATMARK**–タグを受信しています。
	  • **N/A**–上記以外の状態です。

Receiving buffer (cc/hiwat/lowat/drop/state)	• RawIPソケットの総数です。
Sending buffer (cc/hiwat/lowat/state)	• ソケットを作成したタスク名です。括弧の数はタスク名の処理番号です。
Type	ソケットタイプです。 • **1**–SOCK_STREAMです。このソケットはストリームの信頼できる転送を提供するためにTCPを使用します。 • **2**–SOCK_DGRAMです。このソケットはデータグラムの転送を提供するためにUDPを使用します。 • **3**–SOCK_RAWです。このソケットはアプリケーションが

フィールド	説明
	次の上位レイヤプロトコルヘッダを変更することを許可します。 • **N/A**–上記以外のタイプです。
Protocol	ソケットを使用したプロトコル数です。
Connection info	送信元IPアドレスと宛先IPアドレスです。
Inpcb flags	インタネットPCBのフラグです。 • **INP_RECVOPTS**–IPオプションを受信します。 • **INP_RECVRETOPTS**–応答したIPオプションを受信します。 • **INP_RECVDSTADDR**–宛先IPアドレスを受信します。 • **INP_HDRINCL**–全体のIPヘッダを提供します。 • **INP_REUSEADDR**–IPアドレスを再利用します。 • **INP_REUSEPORT**–ポート番号を再利用します。 • **INP_ANONPORT**–ポート番号が指定されていません。 • **INP_RECVIF**–パケットの入力インタフェースを記録します。 • **INP_RECVTTL**–パケットのTTLを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_DONTFRAG**–DF(Don't Fragment)フラグを設定します。 • **INP_ROUTER_ALERT**–ルータ警告オプションのパケットを受信します。このフラグはRawIPのみサポートします。 • **INP_PROTOCOL_PACKET**–プロトコルパケットを識別します。 • **INP_RCVVLANID**–パケットのVLAN IDを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_RCVMACADDR**–フレームのMACアドレスを受信します。 • **INP_SNDBYLSPV–VPN**--インスタンスを通して送信します。 • **INP_RECVTOS**–パケットのTOSを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_USEICMPSRC**–送信ICMPパケットの送信元IPアドレスとして指定したIPアドレスを使用します。 • **INP_SYNCPCB**–インタネットPCBが同期されるまで待ちます。 • **N/A**–上記以外のフラグです。
Inpcb extflag	インタネットPCBの拡張フラグです。 • **INP_EXTRCVPVCIDX**–受信したパケットのPVCインデック

フィールド	説明
	スの記録です。 • **INP_RCVPWID**–受信したパケットのPW IDの記録です。 • **N/A**–上記以外のフラグです。
Inpcb vflag	インタネットPCBのIPバージョンフラグです。 • **INP_IPV4**–IPv4プロトコルです。 • **INP_TIMEWAIT**–TIMEWAIT状態です。 • **INP_ONESBCAST**–ブロードキャストパケットを送信します。 • **INP_DROPPED**–プロトコルがフラグを廃棄しました。 • **INP_SOCKREF**–Strongソケットを参照します。 • **INP_DONTBLOCK**–インタネットPCBの同期をブロックしません。 • **N/A**–上記以外のフラグです。
TTL	インタネットPCBのTTLです。

12.1.5 display tcp

Syntax

display tcp

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display tcp コマンドは TCP 接続の概要情報を表示します。

TCP 接続の概要情報はローカル IP アドレス、ローカルポート番号、ピアの IP アドレス、ピアのポート番号、TCP 接続情報が含まれます。

例

TCP 接続の概要情報を表示します。

<AC> display tcp

```
*: TCP MD5 Connection
 Local Addr:port      Foreign Addr:port    State      Slot  PCB
```

```
*0.0.0.0:21          0.0.0.0:0           LISTEN      1     0x000000000000c387
 192.168.20.200:23   192.168.20.14:1284   ESTABLISHED 1     0x0000000000000009
 192.168.20.200:23   192.168.20.14:1283   ESTABLISHED 1     0x0000000000000002
```

表 12-4 コマンド出力

フィールド	説明
*	TCP接続が認証を使用することを示します。
Local Addr:port	ローカルIPアドレスとポート番号です。
Foreign Addr:port	ピアのIPアドレスとポート番号です。
State	TCP接続状態です。
Slot	１固定です。
PCB	PCBインデックスです。

12.1.6 display tcp statistics

Syntax

display tcp statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display tcp statistics コマンドは TCP トラフィックの統計情報を表示します。

TCP トラフィックの統計情報は受信 TCP パケット、送信 TCP パケット、Syncache/syncookie が含まれます。

例

TCP トラフィックの統計情報を表示します。

<AC> display tcp statistics

```
Received packets:
   Total: 4150
   packets in sequence: 1366 (134675 bytes)
```

```
    window probe packets: 0, window update packets: 0
    checksum error: 0, offset error: 0, short error: 0
    packets dropped for lack of memory: 0
    packets dropped due to PAWS: 0
    duplicate packets: 12 (36 bytes), partially duplicate packets: 0 (0 bytes)
    out-of-order packets: 0 (0 bytes)
    packets with data after window: 0 (0 bytes)
    packets after close: 0
    ACK packets: 3531 (795048 bytes)
    duplicate ACK packets: 33, ACK packets for unsent data: 0

Sent packets:
    Total: 4058
    urgent packets: 0
    control packets: 50
    window probe packets: 3, window update packets: 11
    data packets: 3862 (795012 bytes), data packets retransmitted: 0 (0 bytes)
    ACK-only packets: 150 (52 delayed)
    unnecessary packet retransmissions: 0

Syncache/syncookie related statistics:
    entries added to syncache: 12
    syncache entries retransmitted: 0
    duplicate SYN packets: 0
    reply failures: 0
    successfully build new socket: 12
    bucket overflows: 0
    zone failures: 0
    syncache entries removed due to RST: 0
    syncache entries removed due to timed out: 0
    ACK checked by syncache or syncookie failures: 0
    syncache entries aborted: 0
    syncache entries removed due to bad ACK: 0
    syncache entries removed due to ICMP unreachable: 0
    SYN cookies sent: 0
    SYN cookies received: 0

SACK related statistics:
    SACK recoveries: 1
    SACK retransmitted segments: 0 (0 bytes)
    SACK blocks (options) received: 0
    SACK blocks (options) sent: 0
    SACK scoreboard overflows: 0
```

```
Other statistics:
   retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
   persist timeout: 0
   keepalive timeout: 21, keepalive probe: 0
   keepalive timeout, so connections disconnected: 0
   fin_wait_2 timeout, so connections disconnected: 0
   initiated connections: 29, accepted connections: 12, established connections:
23
   closed connections: 50051 (dropped: 0, initiated dropped: 0)
   bad connection attempt: 0
   ignored RSTs in the window: 0
   listen queue overflows: 0
   RTT updates: 3518(attempt segment: 3537)
   correct ACK header predictions: 0
   correct data packet header predictions: 568
   resends due to MTU discovery: 0
   packets dropped with MD5 authentication: 0
   packets permitted with MD5 authentication: 0
```

関連コマンド

reset tcp statistics

12.1.7 display tcp verbose

Syntax

display tcp verbose [**pcb** *pcb-index*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pcb *pcb-index*: 指定した PCB の TCP 接続の詳細情報を表示します。*pcb-index* 引数は PCB のインデックスを指定します。*pcb-index* 引数の設定範囲は 1～16 です。

説明

display tcp verbose コマンドは TCP 接続の詳細情報を表示します。

TCP 接続の詳細情報はソケット作成のタスク名、状態、オプション、タイプ、プロトコル番号、送信元 IP アドレス、送信元ポート番号、宛先 IP アドレス、宛先ポート番号、接続状態が含まれます。

例

TCP 接続の詳細情報を表示します。

<AC> display tcp verbose

```
Location:
NSR standby: N/A
Creator: telnetd[439]
State: N/A
Options: SO_ACCEPTCONN SO_REUSEADDR
Error: 0
Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 65700 / 1 / 0 / N/A
Sending buffer(cc/hiwat/lowat/state): 0 / 65700 / 512 / N/A
Type: 1
Protocol: 6
Connection info: src = 192.168.20.200:179 ,  dst = 192.168.20.14:4181
Inpcb flags: INP_REUSEADDR INP_PROTOCOL_PACKET INP_SYNCPCB
Inpcb extflag: N/A
Inpcb vflag: INP_IPV4
TTL: 255(minimum TTL: 0)
Connection state: ESTABLISHED
TCP options: TF_REQ_SCALE TF_REQ_TSTMP TF_SACK_PERMIT
NSR state: CLOSED(M)
Send VRF: 0xffff
Receive VRF: 0xffff
```

表 12-5 コマンド出力

フィールド	説明
TCP inpcb number	TCP IP PCBの数です。
tcpcb number	TCP PCBの数です。 TCP接続の状態がTIME_WAITである場合、表示されません。
Location	装置のロケーション
NSR standby:	N/Aと表示されます。
Creator	ソケットを作成したタスク名です。括弧の数はタスク名の処理番号です。
State	ソケットの状態です。

フィールド	説明
Options	ソケットのオプションです。
Error	エラーコードです。

Receiving buffer
(cc/hiwat/lowat/drop/state)
	以下の順番で受信バッファ情報を表示します。
	• **cc**–使用されているバッファ空間です。
	• **hiwat**–最大バッファ空間です。
	• **lowat**–最小バッファ空間です。
	• **state**–バッファ状態です。
	  • **CANTSENDMORE**–ピアにデータを送信できません。
	  • **CANTRCVMORE**–ピアからデータを受信できません。
	  • **RCVATMARK**–タグを受信しています。
	  • **N/A**–上記以外の状態です。

Sending buffer
(cc/hiwat/lowat/state)
	以下の順番で送信バッファ情報を表示します。
	• **cc**–使用されているバッファ空間です。
	• **hiwat**–最大バッファ空間です。
	• **lowat**–最小バッファ空間です。
	• **state**–バッファ状態です。
	  • **CANTSENDMORE**–ピアにデータを送信できません。
	  • **CANTRCVMORE**–ピアからデータを受信できません。
	  • **RCVATMARK**–タグを受信しています。
	  • **N/A**–上記以外の状態です。

Type	ソケットタイプです。 • **1**–SOCK_STREAMです。このソケットはストリームの信頼できる転送を提供するためにTCPを使用します。 • **2**–SOCK_DGRAMです。このソケットはデータグラムの転送を提供するためにUDPを使用します。 • **3**–SOCK_RAWです。このソケットはアプリケーションが次の上位レイヤプロトコルヘッダを変更することを許可します。 • **N/A**–上記以外のタイプです。
Protocol	ソケットを使用したプロトコル数です。
Connection info	送信元IPアドレス、送信元ポート番号、宛先IPアドレス、宛先ポート番号です。

フィールド	説明
Inpcb flags	インタネットPCBのフラグです。 • **INP_RECVOPTS**–IPオプションを受信します。 • **INP_RECVRETOPTS**–応答したIPオプションを受信します。 • **INP_RECVDSTADDR**–宛先IPアドレスを受信します。 • **INP_HDRINCL**–IPヘッダ全体を提供します。 • **INP_REUSEADDR**–IPアドレスを再利用します。 • **INP_REUSEPORT**–ポート番号を再利用します。 • **INP_ANONPORT**–ポート番号が指定されていません。 • **INP_RECVIF**–パケットの入力インタフェースを記録します。 • **INP_RECVTTL**–パケットのTTLを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_DONTFRAG**–DF(Don't Fragment)フラグを設定します。 • **INP_ROUTER_ALERT**–ルータで警告オプションのパケットを受信します。このフラグはRawIPのみサポートします。 • **INP_PROTOCOL_PACKET**–プロトコルパケットを識別します。 • **INP_RCVVLANID**–パケットのVLAN IDを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_RCVMACADDR**–フレームのMACアドレスを受信します。 • **INP_SNDBYLSPV–VPN**–インスタンスを通して送信します。 • **INP_RECVTOS**–パケットのTOSを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_SYNCPCB**–インタネットPCBが同期されるまで待ちます。 • **N/A**–上記以外のフラグです。
Inpcb extflag	インタネットPCBの拡張フラグです。 • **INP_EXTRCVPVCIDX**–受信したパケットのPVCインデックスを記録します。 • **INP_RCVPWID**–受信したパケットのPW IDを記録します。 • **INP_EXTDONTDROP**–受信したパケットを廃棄しません。 • **N/A**–上記以外のフラグです。

フィールド	説明
Inpcb vflag	インタネットPCBのIPバージョンフラグです。 ● **INP_IPV4**–IPv4プロトコルです。 ● **INP_TIMEWAIT**–TIMEWAIT状態です。 ● **INP_ONESBCAST**–ブロードキャストパケットを送信します。 ● **INP_DROPPED**–プロトコルがフラグを廃棄しました。 ● **INP_SOCKREF**–Strongソケットを参照します。 ● **INP_DONTBLOCK**–インタネットPCBの同期をブロックしません。 ● **N/A**–上記以外のフラグです。
TTL	インタネットPCBのTTLです。
NSR state	TCP接続の状態です。括弧の数は接続の役割です。 ● **M**–メイン接続です。 ● **S**–Standby接続です。

12.1.8 display udp

Syntax

display udp

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display udp コマンドは UDP 接続の概要情報を表示します。

UDP 接続の概要情報はローカル IP アドレス、ローカルポート番号、ピアの IP アドレス、ピアのポート番号が含まれます。

例

UDP 接続の概要情報を表示します。

<AC> display udp

```
Local Addr:port       Foreign Addr:port     Slot  PCB
 0.0.0.0:69             0.0.0.0:0            1     0x0000000000000003
```

```
192.168.20.200:1024    192.168.20.14:69      1     0x0000000000000002
```

表 12-6 コマンド出力

フィールド	説明
Local Addr:port	ローカルIPアドレスとポート番号です。
Foreign Addr:port	ピアのIPアドレスとポート番号です。
Slot	1 固定です。
PCB	PCBインデックスです。

12.1.9 display udp statistics

Syntax

display udp statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display udp statistics コマンドは UDP トラフィックの統計情報を表示します

UDP トラフィックの統計情報は受信 UDP パケット、送信 UDP パケットが含まれます。

例

UDP トラフィックの統計情報を表示します。

<AC> display udp statistics

```
Received packets:
    Total: 240
    checksum error: 0, no checksum: 0
    shorter than header: 0, data length larger than packet: 0
    no socket on port(unicast): 0
    no socket on port(broadcast/multicast): 240
    not delivered, input socket full: 0
Sent packets:
    Total: 0
```

関連コマンド

reset udp statistics

12.1.10 display udp verbose

Syntax

display udp verbose [**pcb** *pcb-index*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pcb *pcb-index*: 指定した PCB の UDP 接続の詳細情報を表示します。*pcb-index* 引数は PCB のインデックスを指定します。*pcb-index* 引数の設定範囲は 1～16 です。

説明

display udp verbose コマンドは UDP 接続の詳細情報を表示します。

UDP 接続の詳細情報は UDP 接続のソケット作成のタスク名、状態、オプション、タイプ、プロトコル番号、送信元 IP アドレス、送信元ポート番号、宛先 IP アドレス、宛先ポート番号が含まれます。

例

UDP 接続の詳細情報を表示します。

<AC> display udp verbose

```
Total UDP socket number: 1


 Location:
 Creator: sock_test_mips[250]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 41600 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 2
 Protocol: 17
 Connection info: src = 0.0.0.0:69, dst = 0.0.0.0:0
```

```
Inpcb flags: N/A
Inpcb extflag: N/A
Inpcb vflag: INP_IPV4
TTL: 255(minimum TTL: 0)
Send VRF: 0xffff
Receive VRF: 0xffff
```

表 12-7 コマンド出力

フィールド	説明
Total UDP socket number	UDPソケットの総数です。
Location	装置のロケーション
Creator	ソケットを作成したタスク名です。括弧の数はタスク名の処理番号です。
State	ソケットの状態です。
Options	ソケットのオプションです。
Error	エラーコードです。

Receiving buffer(cc/hiwat/lowat/state)	以下の順番で受信バッファ情報を表示します。
	• **cc**–使用されているバッファ空間です。
	• **hiwat**–最大バッファ空間です。
	• **lowat**–最小バッファ空間です。
	• **drop**–廃棄されたパケット数です。
	• **state**–バッファ状態です。
	  • **CANTSENDMORE**–ピアにデータを送信できません。
	  • **CANTRCVMORE**–ピアからデータを受信できません。
	  • **RCVATMARK**–タグを受信しています。
	  • **N/A**–上記以外の状態です。

Sending buffer(cc/hiwat/lowat/drop/state)	以下の順番で送信バッファ情報を表示します。
	• **cc**–使用されているバッファ空間です。
	• **hiwat**–最大バッファ空間です。
	• **lowat**–最小バッファ空間です。
	• **state**–バッファ状態です。
	  • **CANTSENDMORE**–ピアにデータを送信できません。
	  • **CANTRCVMORE**–ピアからデータを受信できません。
	  • **RCVATMARK**–タグを受信しています。
	  • **N/A**–上記以外の状態です。

フィールド	説明
Type	ソケットタイプです。 • **1**–SOCK_STREAMです。このソケットはストリームの信頼できる転送を提供するためにTCPを使用します。 • **2**–SOCK_DGRAMです。このソケットはデータグラムの転送を提供するためにUDPを使用します。 • **3**–SOCK_RAWです。このソケットはアプリケーションが次の上位レイヤプロトコルヘッダを変更することを許可します。 • **N/A**–上記以外のタイプです。
Protocol	ソケットを使用したプロトコル数です。
Inpcb flags	インタネットPCBのフラグです。 • **INP_RECVOPTS**–IPオプションを受信します。 • **INP_RECVRETOPTS**–応答したIPオプションを受信します。 • **INP_RECVDSTADDR**–宛先IPアドレスを受信します。 • **INP_HDRINCL**–全体のIPヘッダを提供します。 • **INP_REUSEADDR**–IPアドレスを再利用します。 • **INP_REUSEPORT**–ポート番号を再利用します。 • **INP_ANONPORT**–ポート番号が指定されていません。 • **INP_RECVIF**–パケットの入力インタフェースを記録します。 • **INP_RECVTTL**–パケットのTTLを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_DONTFRAG**–DF(Don't Fragment)フラグを設定します。 • **INP_ROUTER_ALERT**–ルータで警告オプションのパケットを受信します。このフラグはRawIPのみサポートします。 • **INP_PROTOCOL_PACKET**–プロトコルパケットを識別します。 • **INP_RCVVLANID**–パケットのVLAN IDを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_RCVMACADDR**–フレームのMACアドレスを受信します。 • **INP_SNDBYLSPV**–VPNインスタンスを通して送信します。 • **INP_RECVTOS**–パケットのTOSを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_SYNCPCB**–インタネットPCBが同期されるまで待ちます。

フィールド	説明
	• **N/A**–上記以外のフラグです。
Inpcb extflag	インタネットPCBの拡張フラグです。 • **INP_EXTRCVPVCIDX**–受信したパケットのPVCインデックスを記録します。 • **INP_RCVPWID**–受信したパケットのPW IDを記録します。 • **N/A**–上記以外のフラグです。
Inpcb vflag	インタネットPCBのIPバージョンフラグです。 • **INP_IPV4**–IPv4プロトコルです。 • **INP_TIMEWAIT**–TIMEWAIT状態です。 • **INP_ONESBCAST**–ブロードキャストパケットを送信します。 • **INP_DROPPED**–プロトコルがフラグを廃棄しました。 • **INP_SOCKREF**–Strongソケットを参照します。 • **INP_DONTBLOCK**–インタネットPCBの同期をブロックしません。 • **N/A**–上記以外のフラグです。
TTL	インタネットPCBのTTLです。

12.1.11 ip forward-broadcast

Syntax

ip forward-broadcast

undo ip forward-broadcast

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

説明

ip forward-broadcast コマンドは直接接続されたネットワークにダイレクトブロードキャストパケットの送受信をインタフェースで有効にします。

undo ip forward-broadcast コマンドは直接接続されたネットワークにダイレクトブロードキャストパケットの送受信をインタフェースで無効にします。

ダイレクトブロードキャストパケットは指定したネットワークのすべてのホストに送信されるブロードキャストパケットのことです。ダイレクトブロードキャストパケットの宛先 IP アドレスのネットワーク ID は宛先ネットワークを識別し、ホスト ID は値がすべて 1 です。

例

直接接続されたネットワークにダイレクトブロードキャストパケットの送受信を VLAN インタフェース 2 で有効にします。

<AC> system-view

[AC] interface vlan-interface 2

[AC-Vlan-interface2] ip forward-broadcast

12.1.12 ip icmp error-interval

Syntax

ip icmp error-interval *interval* [*bucketsize*]

undo ip icmp error-interval

デフォルト

最大バケットサイズは最大 10 トークンで、バケットに 100 ミリ秒の間隔でトークンが配置されます。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: バケットに到着するトークンの間隔を設定します。設定範囲は 0～2147483647 です。ICMP レートリミットを無効にする場合 0 に設定します。

bucketsize: 最大トークンバケットサイズを指定します。設定範囲は 1～200 です。

説明

ip icmp error-interval コマンドは ICMP エラーメッセージがトークンバケット（bucket）に到着する間隔と、トークンパケットサイズを設定します。

undo ip icmp error-interval コマンドはデフォルトに戻します。

本コマンドは ICMP エラーメッセージが送信されるレートを制限します。本コマンドを使用することで、ネットワークの衝突が発生する可能性のある短い時間内に過度の ICMP エラーメッセージを送信することを防ぐことができます。トークンバケットアルゴリズムは 1 つの ICMP エラーメッセージを表す 1 つのトークンが用いられます。

バケットに入ることができるトークンが最大に到達するまでトークンは指定された間隔でバケットに配置されます。

ICMP エラーメッセージが送信されるとき、バケットからトークンがバケットから取り除かれます。バケットが空の時、新しいトークンがバケットに配置されるまで ICMP エラーメッセージは送信されません。

例

ICMP エラーメッセージの送信間隔を 200 ミリ秒、トークンのバケットサイズを 40 に設定します。

<AC> system-view

[AC] ip icmp error-interval 200 40

12.1.13 ip mtu

Syntax

ip mtu *mtu-size*

undo ip mtu

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

mtu-size: MTU をバイト単位で指定します。WAN インタフェースの値の範囲は 128～1560 です.VLAN インタフェースの値の範囲は 128～1748 です。

説明

ip mtu コマンドはインタフェースの MTU を設定します。

undo ip mtu コマンドはデフォルトに戻します。

出力インタフェースの MTU を超過したとき、装置は以下のどちらか 1 つの方法で処理します。

- パケットのフラグメントが禁止されている場合、装置はパケットを廃棄します。
- パケットのフラグメントが許可されている場合、装置はパケットを分割し、フラグメントしたパケットを転送します。

フラグメントと再構築はシステムリソースを消費します。フラグメントを防止するため、ネットワーク環境に基づいて適切にインタフェースの MTU サイズを設定します。

例

VLAN インタフェース 100 の MTU を 1280 バイトに設定します。

<AC> system-view

[AC] interface vlan-interface 100

[AC-Vlan-interface100] ip mtu 1280

12.1.14 ip redirects enable

Syntax

ip redirects enable

undo ip redirects enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ip redirects enable コマンドは ICMP リダイレクトメッセージの送信を有効にします。

undo ip redirects enable コマンドは ICMP リダイレクトメッセージの送信を無効にします。

ICMP リダイレクトパケット機能はホストの管理を簡略化し、最適なルートを見つけ出すために、ホストが正しいルーティングテーブルを徐々に確立することができます。

ホストはすべてのパケットをデフォルトゲートウェイに送信するため、デフォルトルートへのルートのみがあります。デフォルトゲートウェイは、以降のパケットを送信するために正しいネクストホップを再選択するよう、以下の条件で、送信元の装置に ICMP リダイレクトパケットを送信します。

- 受信インタフェースと送信インタフェースが同じです。

- 選択したルートが ICMP リダイレクトパケットで作成されていない、あるいは変更されていません。
- 選択されたルートが 0.0.0.0 へのルートではありません。
- 受信したパケットに送信元ルートオプションがありません。

例

ICMP リダイレクトメッセージの送信を有効にします。

<AC> system-view

[AC] ip redirects enable

12.1.15 ip ttl-expires enable

Syntax

ip ttl-expires enable

undo ip ttl-expires enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ip ttl-expires enable コマンドは ICMP time exceeded メッセージの送信を有効にします。

undo ip ttl-expires enable コマンドは ICMP time exceeded メッセージの送信を無効にします。

装置は以下のルールによって ICMP time exceeded メッセージを送信します。

- 以下の状況になった場合、装置は ICMP TTL exceeded in transit メッセージを送信元に送信します。
  - 受信したパケットが装置宛てでない
  - パケットの TTL フィールドが 1 である
- 宛先が装置自身である IP データグラムの最初のフラグメントパケットを、装置が受信したとき、タイマを始動します。データグラムのすべてのフラグメントパケットを受信する前にタイマが満了した場合、装置は ICMP fragment reassembly time exceeded メッセージを送信元に送信します。

ICMP time exceeded メッセージの送信を無効にした装置は ICMP TTL exceeded in transit メッセージを送信しませんが、ICMP fragment reassembly time exceeded メッセージは送信します。

例

ICMP time exceeded メッセージの送信を有効にします。

<AC> system-view

[AC] ip ttl-expires enable

12.1.16 ip unreachables enable

Syntax

ip unreachables enable

undo ip unreachables enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ip unreachables enable コマンドは ICMP destination unreachable メッセージの送信を有効にします。

undo ip unreachables enable コマンドは ICMP destination unreachable メッセージの送信を無効にします。

装置は以下のルールで ICMP destination unreachable メッセージを送信します。

- 以下の状態の場合、装置は ICMP network unreachable メッセージを送信元に送信します。
  - 受信したパケットがルートに一致しません。
  - ルーティングテーブルにデフォルトルートがありません。
- 以下の状態の場合、装置は ICMP protocol unreachable メッセージを送信元に送信します。
  - 受信したパケットの宛先が装置です。
  - パケットのトランスポート層プロトコルが装置でサポートしていません。
- 以下の状態の場合、装置は ICMP port unreachable メッセージを送信元に送信します。

- 受信したパケットの宛先が装置です。
- パケットのポート番号が実行中のプロセスとマッチしません。

- 以下の状態の場合、装置は ICMP source route failed メッセージを送信元に送信します。
  - パケットを送信するために送信元が、Strict ソースルーティングを使用しています。
  - 中継装置で、送信元により指定されたネクストホップが直接接続されていないことを検出しました。
- 以下の状態の場合、装置は ICMP fragmentation needed and DF set メッセージを送信元に送信します。
  - 送信インタフェースの MTU がパケットより小さい。
  - パケットに DF セット(フラグメント禁止)が付与されている。

例

ICMP destination unreachable メッセージの送信を有効にします。

<AC> system-view

[AC] ip unreachables enable

12.1.17 reset ip statistics

Syntax

reset ip statistics

View

User view

定義済みユーザロール

network-admin

説明

reset ip statistics コマンドは IP トラフィックの統計情報を削除します。

新しく一定期間内の IP トラフィックの統計情報を取得する場合、このコマンドを使用し、最初に既存の IP トラフィックの統計情報を削除します。

例

IP トラフィックの統計情報を削除します。

<AC> reset ip statistics

関連コマンド

- **display ip interface**
- **display ip statistics**

12.1.18 reset tcp statistics

Syntax

reset tcp statistics

View

User view

定義済みユーザロール

network-admin

説明

reset tcp statistics コマンドは TCP トラフィックの統計情報を削除します。

例

TCP トラフィックの統計情報を削除します。

<AC> reset tcp statistics

関連コマンド

display tcp statistics

12.1.19 reset udp statistics

Syntax

reset udp statistics

View

User view

定義済みユーザロール

network-admin

説明

reset udp statistics コマンドは UDP トラフィックの統計情報を削除します。

例

UDP トラフィックの統計情報を削除します。

<AC> reset udp statistics

関連コマンド

display udp statistics

12.1.20 tcp path-mtu-discovery

Syntax

tcp path-mtu-discovery [**aging** *age-time* | **no-aging**]

undo tcp path-mtu-discovery

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

aging *age-time*: path MTU のエージングタイマを設定します。設定時間は 10～30 分です。デフォルトは 10 分です。

no-aging: path MTU をエージアウトしません。

説明

tcp path-mtu-discovery コマンドは TCP path MTU discovery を有効にします。

undo tcp path-mtu-discovery コマンドは TCP path MTU discovery を無効にします。

TCP path MTU discovery を有効にしたのち、すべての新しい TCP 接続は、path MTU を検出します。装置は IP のフラグメントを発生させないように MSS の計算をするため、path MTU を使用します。

TCP path MTU discovery を無効にしたのち、システムはすべての path MTU タイマを停止します。その後に確立された TCP 接続は path MTU を検出しませんが、以前に確立された TCP 接続は path MTU を検出することができます。

例

TCP path MTU discovery を有効にし、path MTU のエージングタイマを 20 分に設定します。

<AC> system-view

[AC] tcp path-mtu-discovery aging 20

12.1.21 tcp timer fin-timeout

Syntax

tcp timer fin-timeout *time-value*

undo tcp timer fin-timeout

デフォルト

675 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

time-value: TCP FIN wait タイマを指定します。設定範囲は 76～3600 秒です。

説明

tcp timer fin-timeout コマンドは TCP FIN wait タイマを設定します。

undo tcp timer fin-timeout コマンドはデフォルトに戻します。

TCP は状態が FIN_WAIT_2 に変更されると、TCP FIN wait タイマを開始します。時間内に FIN パケットを受信しなかった場合、TCP 接続が終了します。

FIN パケットを受信した場合、TCP は TIME_WAIT に接続状態を変更します。non-FIN パケットを受信すると TCP はタイマを再スタートし､TCP はタイマが満了したとき TCP 接続を切断します。

例

TCP FIN wait タイマを 800 秒に設定します。

<AC> system-view

[AC] tcp timer fin-timeout 800

12.1.22 tcp timer syn-timeout

Syntax

tcp timer syn-timeout *time-value*

undo tcp timer syn-timeout

デフォルト

75 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

time-value: TCP SYN wait タイマを指定します。設定範囲は 2～600 秒です。

説明

tcp timer syn-timeout コマンドは TCP SYN wait タイマを設定します。

undo tcp timer syn-timeout コマンドはデフォルトに戻します。

TCP は SYN パケットを送信した後、SYN wait タイマを開始します。SYN wait タイマの期間にパケットを受信しなかった場合、TCP は接続の確立に失敗します。

例

TCP SYN wait タイマを 80 秒に設定します。

<AC> system-view

[AC] tcp timer syn-timeout 80

12.1.23 tcp window

Syntax

tcp window *window-size*

undo tcp window

デフォルト

64 KB

View

System view

定義済みユーザロール

network-admin

パラメータ

window-size: TCP 受信/送信バッファのサイズを指定します。設定範囲は 1～64KB です。

説明

tcp window コマンドは TCP 受信/送信バッファのサイズを設定します。

undo tcp window コマンドはデフォルトに戻します。

例

TCP 受信/送信バッファのサイズを 3KB に設定します。

<AC> system-view

[AC] tcp window 3

目次

このセクションのページは **5-x-x** です。

13 章 NAT 13-1
13.1 NAT コマンド 13-1
13.1.1 address 13-1
13.1.2 block-size 13-2
13.1.3 display nat address-group 13-3
13.1.4 display nat alg 13-5
13.1.5 display nat all 13-6
13.1.6 display nat dns-map 13-14
13.1.7 display nat eim 13-15
13.1.8 display nat inbound 13-16
13.1.9 display nat log 13-18
13.1.10 display nat no-pat 13-20
13.1.11 display nat outbound 13-21
13.1.12 display nat outbound port-block-group 13-23
13.1.13 display nat port-block 13-25
13.1.14 display nat port-block-group 13-26
13.1.15 display nat port-block-usage 13-29
13.1.16 display nat server 13-30
13.1.17 display nat server-group 13-32
13.1.18 display nat session 13-34
13.1.19 display nat static 13-36
13.1.20 display nat statistics 13-39
13.1.21 global-ip-pool 13-41
13.1.22 inside ip 13-42
13.1.23 local-ip-address 13-43
13.1.24 nat address-group 13-44
13.1.25 nat alg 13-45
13.1.26 nat dns-map 13-47
13.1.27 nat icmp-error reply 13-48
13.1.28 nat inbound 13-49
13.1.29 nat inbound rule move 13-52
13.1.30 nat log alarm 13-53
13.1.31 nat log enable 13-54
13.1.32 nat log flow-active 13-55
13.1.33 nat log flow-begin 13-56
13.1.34 nat log flow-end 13-57

13.1.35 nat log port-block usage threshold....13-58
13.1.36 nat log port-block-assign....13-59
13.1.37 nat log port-block-withdraw....13-60
13.1.38 nat mapping-behavior endpoint-independent....13-61
13.1.39 nat outbound....13-62
13.1.40 nat outbound port-block-group....13-66
13.1.41 nat outbound rule move....13-67
13.1.42 nat port-block global-share enable....13-68
13.1.43 nat port-block-group....13-69
13.1.44 nat server....13-70
13.1.45 nat server rule move....13-76
13.1.46 nat server-group....13-77
13.1.47 nat static enable....13-78
13.1.48 nat static inbound....13-79
13.1.49 nat static inbound net-to-net....13-81
13.1.50 nat static inbound rule move....13-83
13.1.51 nat static outbound....13-84
13.1.52 nat static outbound net-to-net....13-87
13.1.53 nat static outbound rule move....13-89
13.1.54 nat timestamp delete....13-90
13.1.55 port-block....13-91
13.1.56 port-range....13-92
13.1.57 reset nat count statistics....13-93
13.1.58 reset nat session....13-94

13章 NAT

🕮 **メモ：**

NAT 機能は Version 7.2.44 を含む以降のソフトウェアからサポートしています。

13.1 NATコマンド

13.1.1 address

Syntax

address *start-address end-address*

undo address *start-address end-address*

デフォルト

設定なし

View

NAT address group view

定義済みユーザロール

network-admin

パラメータ

start-address end-address: アドレス範囲の開始 IP アドレスと終了 IP アドレスを指定します。終了アドレスは開始アドレスより小さくできません。同じ場合、アドレス範囲には IP アドレスが 1 つしかありません。IP アドレスの範囲は 65535 個まで指定できます。

説明

address コマンドは NAT アドレスグループにアドレス範囲を追加します。

undo address コマンドは NAT アドレスグループからアドレス範囲を削除します。

NAT アドレスグループは、アドレス範囲のセットです。外部ネットワーク宛てのパケットの送信元アドレスは、アドレス範囲の 1 つのアドレスに変換されます。

単一の NAT アドレスグループまたは複数の NAT アドレスグループのアドレス範囲が重複していないことを確認します。

例

#アドレスグループにアドレス範囲を追加します。

<AC> system-view

[AC] nat address-group 2

[AC-address-group-2] address 10.1.1.1 10.1.1.15

[AC-address-group-2] address 10.1.1.20 10.1.1.30

関連コマンド

nat address-group

13.1.2 block-size

Syntax

block-size *block-size*

undo block-size

デフォルト

256

View

NAT port block group view

定義済みユーザロール

network-admin

パラメータ

block-size: ポートブロックのポート数を指定します。値の範囲は 1~65535 です。

説明

block-size コマンドはポートブロックサイズを設定します。

undo block-size コマンドはデフォルト状態に戻します。

プライベート IP アドレスの数、パブリック IP アドレスの数、およびポートブロックグループ内のポート範囲に基づいて、適切なポートブロックサイズを設定します。

ポートブロックサイズは、ポート範囲内のポート数より大きくすることはできません。

例

ポートブロックグループ 1 のポートブロックサイズを 1024 に設定します。

<AC> system-view
[AC] nat port-block-group 1
[AC-port-block-group-1] block-size 1024

関連コマンド

nat port-block-group

13.1.3 display nat address-group

Syntax

display nat address-group [*group-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-id: NAT アドレスグループの ID を指定します。この値の範囲は 0 から 65535 です。*group-id* 引数を指定しない場合、このコマンドはすべての NAT アドレスグループに関する情報を表示します。

説明

display nat address-group コマンドは NAT アドレスグループ情報を表示します。

例

すべての NAT アドレスグループに関する情報を表示します。

<AC> display nat address-group

```
NAT address group information:
  Totally 5 NAT address groups.
  Address group ID: 1    Address group name: a
    Port range: 1-65535
    Address information:
      Start address        End address
      202.110.10.10        202.110.10.15

  Address group ID: 2
    Port range: 1-65535
    Address information:
      Start address        End address
      202.110.10.20        202.110.10.25
      202.110.10.30        202.110.10.35
```

```
Address group ID: 3
  Port range: 1024-65535
  Address information:
    Start address        End address
    202.110.10.40        202.110.10.50

Address group ID: 4
  Port range: 10001-65535
  Port block size: 500
  Extended block number: 1
  Address information:
    Start address        End address
    202.110.10.60        202.110.10.65

Address group ID: 6
  Port range: 1-65535
  Address information:
    Start address        End address
    ---                 ---
```

#NAT アドレスグループ 1 に関する情報を表示します。

<AC> display nat address-group 1

```
Address group ID: 1    Address group name: a
  Port range: 1-65535
  Address information:
    Start address        End address
    202.110.10.10        202.110.10.15
```

表 13-1 コマンド出力

フィールド	説明
NAT address group information	NATアドレスグループに関する情報
Address group ID	NATアドレスグループのID。
Totally n NAT address groups	NATアドレスグループの総数。
Address group name	NATアドレスグループの名前。アドレスグループ名が設定されていない場合、このフィールドは表示されません。
Port range	パブリックIPアドレスのポート範囲。
Port block size	ポートブロック内のポート数。ポートブロックサイズが設定されていない場合、このフィールドは表示されません。

フィールド	説明
Extended block number	拡張ポートブロックの数。拡張ポートブロック数が設定されていない場合、このフィールドは表示されません。

Address information	アドレスグループ内のIPアドレスに関する情報。
	• addressコマンドを使用して追加されたアドレスの場合:
	  • Start address :アドレス範囲の開始IPアドレス。範囲の開始アドレスを指定しない場合、このフィールドにはハイフン (---) が表示されます。
	  • End address:アドレス範囲の終了IPアドレス。範囲の終了アドレスを指定しない場合、このフィールドにはハイフン (---) が表示されます。
	• address interfaceコマンドを使用して追加されたアドレスの場合:
	  • 20.1.1.1 (Vlan-interface 10) :VLAN-interface 10のIPアドレス20.1.1.1がNATアドレスグループに追加されました。
	  • --- (Vlan-interface 10) :VLAN-interface 10のIPアドレスをNATアドレスグループに追加できませんでした。これは、このインタフェースにIPアドレスがないためです。

関連コマンド

nat address-group

13.1.4 display nat alg

Syntax

display nat alg

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat alg コマンドはサポートされているすべてのプロトコルの NAT ALG ステータスを表示します。

例

#サポートされているすべてのプロトコルの NAT ALG ステータスを表示します。

<AC> display nat alg

```
NAT ALG:
  DNS       : Enabled
  FTP       : Disabled
  H323      : Disabled
  ICMP-ERROR : Disabled
  ILS       : Disabled
  MGCP      : Disabled
  NBT       : Disabled
  PPTP      : Disabled
  RTSP      : Disabled
  RSH       : Disabled
  SCCP      : Disabled
  SIP       : Disabled
  SQLNET    : Disabled
  TFTP      : Disabled
  XDMCP     : Disabled
```

関連コマンド

display nat all

13.1.5 display nat all

Syntax

display nat all

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat all コマンドはすべての NAT 設定情報を表示します。

例

すべての NAT 設定情報を表示します。

<AC> display nat all

```
NAT address group information:
  Totally 5 NAT address groups.
  Address group ID: 1:
    Port range: 1-65535
    Address information:
      Start address       End address
      202.110.10.10       202.110.10.15

  Address group ID: 2:
    Port range: 1-65535
    Address information:
      Start address       End address
      202.110.10.20       202.110.10.25
      202.110.10.30       202.110.10.35

  Address group ID: 3:
    Port range: 1024-65535
    Address information:
      Start address       End address
      202.110.10.40       202.110.10.50

  Address group ID: 4:
    Port range: 10001-65535
    Port block size: 500
    Extended block number: 1
    Address information:
      Start address       End address
      202.110.10.60       202.110.10.65

  Address group ID: 6:
    Port range: 1-65535
    Address information:
      Start address       End address
      ---                 ---

NAT server group information:
  Totally 3 NAT server groups.
  Group Number       Inside IP           Port       Weight
  1                  192.168.0.26        23         100
                     192.168.0.27        23         500
  2                  ---                 ---        ---
  3                  192.168.0.26        69         100
```

```
NAT inbound information:
  Totally 1 NAT inbound rules.
  Interface: Vlan-interface20
    ACL: 2038
    Address group ID: 2
    Add route: Y        NO-PAT:Y  Reversible: N
    Rule name: abc
    Priority: 1000
    NAT counting: 0
    Config status: Active

NAT outbound information:
  Totally 2 NAT outbound rules.
  Interface: Vlan-interface10
    ACL: 2036
    Address group ID: 1
    Port-preserved: Y       NO-PAT: N  Reversible: N
    Rule name: lee
    Priority: 122
    NAT counting: 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

  Interface: Vlan-interface10
    ACL: 2037
    Address group ID: 1
    Port-preserved: N       NO-PAT: Y  Reversible: Y
    Rule name: rabbit
    Priority: 100
    NAT counting: 0
      The following items don't exist or aren't effective: ACL.

NAT internal server information:
  Totally 2 internal servers.
  Interface: Vlan-interface10
    Global ACL    : 2000
    Local IP/port : 192.168.10.1/23
    Rule name     : sept
    Priority      : 1000
    NAT counting  : 0
    Config status : Active
```

```
  Interface: Vlan-interface20
    Protocol: 6(TCP)
    Global IP/port: 50.1.1.1/23
    Local IP/port : 192.168.10.15/23
    ACL          : 2000
    Rule name     : blue
    NAT counting  : 0
    Config status : Active

 Static NAT mappings:
  Totally 2 inbound static NAT mappings.
  Net-to-net:
    Global IP    : 2.2.2.1 - 2.2.2.255
    Local IP     : 1.1.1.0
    Netmask      : 255.255.255.0
    ACL         : 3000
    Reversible   : Y
    Rule name    : green
    Priority     : 4
    NAT counting : 0
    Config status: Active

  IP-to-IP:
    Global IP    : 5.5.5.5
    Local IP     : 4.4.4.4
    ACL         : 2001
    Reversible   : Y
    Rule name    : blue
    Priority     : 4
    NAT counting : 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

  Totally 2 outbound static NAT mappings.
  Net-to-net:
    Local IP     : 1.1.1.1 - 1.1.1.255
    Global IP    : 2.2.2.0
    Netmask      : 255.255.255.0
    ACL         : 3000
    Reversible   : Y
    Rule name    : yellow
```

```
    Priority    : 5
    NAT counting : 0
    Config status: Active

  IP-to-IP:
    Local IP    : 4.4.4.4
    Global IP   : 5.5.5.5
    ACL:        : 2001
    Reversible  : Y
    Rule name   : pink
    Priority    : 6
    NAT counting : 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

Interfaces enabled with static NAT:
  Totally 2 interfaces enabled with static NAT.
  Interface: Vlan-interface20
    Config status: Active

  Interface: Vlan-interface30
    Config status: Active

NAT DNS mappings:
  Totally 2 NAT DNS mappings.
  Domain name  : www.server.com
  Global IP    : 6.6.6.6
  Global port  : 23
  Protocol     : TCP(6)
  Config status: Active

  Domain name  : www.service.com
  Global IP    : ---
  Global port  : 12
  Protocol     : TCP(6)
  Config status: Inactive
  Reasons for inactive status:
    The following items don't exist or aren't effective: interface IP address.

NAT logging:
  Log enable         : Enabled(ACL 2000)
  Flow-begin         : Disabled
```

```
  Flow-end          : Disabled
  Flow-active       : Enabled(10 minutes)
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm             : Disabled
  NO-PAT IP usage     : Disabled

NAT hairpinning:
  Totally 2 interfaces enabled with NAT hairpinning.
  Interface: Vlan-interface10
    Config status: Active

  Interface: Vlan-interface20
    Config status: Active

NAT mapping behavior:
  Mapping mode : Endpoint-Independent
  ACL          : 2050
  Config status: Active

NAT ALG:
  DNS       : Enabled
  FTP       : Disabled
  H323      : Enabled
  ICMP-ERROR : Enabled
  ILS       : Enabled
  MGCP      : Enabled
  NBT       : Enabled
  PPTP      : Enabled
  RSH       : Enabled
  RTSP      : Enabled
  SCCP      : Enabled
  SIP       : Disabled
  SQLNET    : Enabled
  TFTP      : Enabled
  XDMCP     : Enabled

NAT port block group information:
  Totally 3 NAT port block groups.
  Port block group 1:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
```

```
    Start address       End address         VPN instance
    172.16.1.1          172.16.1.254        ---
    192.168.1.1         192.168.1.254       ---
    192.168.3.1         192.168.3.254       ---
  Global IP pool information:
    Start address       End address
    201.1.1.1           201.1.1.10
    201.1.1.21          201.1.1.25

 Port block group 2:
  Port range: 10001-30000
  Block size: 500
  Local IP address information:
    Start address       End address         VPN instance
    10.1.1.1            10.1.10.255         ---
  Global IP pool information:
    Start address       End address
    202.10.10.101       202.10.10.120

 Port block group 3:
  Port range: 1-65535
  Block size: 256
  Local IP address information:
    Start address       End address         VPN instance
    ---                 ---                 ---
  Global IP pool information:
    Start address       End address
    ---                 ---

NAT outbound port block group information:
 Totally 2 outbound port block group items.
 Interface: Vlan-interface20
  port-block-group: 2
  Rule name      : red
  NAT counting: 0
  Config status   : Active

 Interface: Vlan-interface20
  port-block-group: 10
  Rule name: lee
  NAT counting: 0
  Config status   : Inactive
  Reasons for inactive status:
```

```
        The following items don't exist or aren't effective: port block group.

Static NAT load balancing:    Disabled
```

表 13-2 コマンド出力

フィールド	説明
NAT address group information	NATアドレスグループに関する情報。出力の説明については、表 13-1を参照してください。
NAT server group information	内部サーバグループに関する情報。出力の説明は、表 13-14を参照してください。
NAT inbound information:	インバウンドダイナミックNATコンフィグレーション。出力の説明については、表 13-5を参照してください。
NAT outbound information	送信ダイナミックNATの設定。出力の説明については、表 13-8を参照してください。
NAT internal server information	NATサーバマッピングの設定。出力の説明は、表 13-13を参照してください。
Static NAT mappings	スタティックNATマッピング。出力の説明は、表 13-16を参照してください。
NAT DNS mappings	NAT DNSマッピング。出力の説明については、表 13-3を参照してください。
NAT logging	NATログの設定。出力の説明については、表 13-6を参照してください。
NAT hairpinning	NATヘアピンの設定。
Interface	NATヘアピンを有効にしたインタフェース。
Rule name	NATルールの名前。
NAT counting	NATルールが一致した回数。
Priority	NATルールのプライオリティ。
Config status	NATヘアピン設定のステータス： ActiveまたはInactive
Reasons for inactive status	NATヘアピン設定が有効にならない理由。このフィールドは、Configステータスが Inactiveの場合に使用できます。
NAT mapping behavior	PATのマッピング動作モード: Endpoint-Independent または Address and Port-Dependent。
ACL	ACL番号または名前。NATにACLが指定されていない場合、このフィールドにはハイフン (---) が表示されます。
Config status	NATマッピング動作設定のステータス (Activeまたは Inactive) 。
Reasons for inactive status	NATマッピング動作の設定が有効にならない理由。このフィールドは、Configステータスが Inactiveの場合に使用できます。

フィールド	説明
NAT ALG	異なるプロトコルのNAT ALG設定。
NAT port block group information	NATポートブロックグループに関する設定情報。出力の説明は、表 13-11を参照してください。
NAT outbound port block group information	スタティックアウトバウンドポートブロックマッピングルールに関する設定情報。出力の説明については、表 13-9を参照してください。

13.1.6 display nat dns-map

Syntax

display nat dns-map

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat dns-map コマンドは NAT DNS マッピングを表示します。

例

#NAT DNS マッピングを表示します。

<AC> display nat dns-map

```
NAT DNS mapping information:
  Totally 2 NAT DNS mappings.
  Domain name  : www.server.com
  Global IP    : 6.6.6.6
  Global port  : 23
  Protocol     : TCP(6)
  Config status: Active

  Domain name  : www.service.com
  Global IP    : ---
  Global port  : 12
  Protocol     : TCP(6)
  Config status: Inactive
  Reasons for inactive status:
```

```
The following items don't exist or aren't effective: interface IP address.
```

表 13-3 コマンド出力

フィールド	説明
NAT DNS mapping information	NAT DNSマッピングに関する情報。
Totally n NAT DNS mappings	NAT DNSマッピングの合計数。
Domain name	内部サーバのドメイン名。
Global IP	内部サーバのパブリックIPアドレス。 ● Easy IPが設定されている場合、このフィールドには指定されたインタフェースのIPアドレスが表示されます。 ● パブリックIPアドレスを指定しない場合、このフィールドにはハイフン (---) が表示されます。
Global port	内部サーバのパブリックポート番号。
Protocol	内部サーバのプロトコル名と番号。
Config status	DNSマッピングのステータス (ActiveまたはInactive) 。
Reasons for inactive status	DNSマッピングが有効にならない理由。このフィールドは、Configステータスがinactiveの場合に使用できます。

関連コマンド

nat dns-map

13.1.7 display nat eim

Syntax

display nat eim

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat eim コマンドは NAT EIM (Endpoint-Independent Mapping) エントリに関する情報を表示します。

EIM エントリは、PAT が EIM モードで動作しているときに作成されます。EIM エントリは 3 タプルのエントリで、プライベートアドレス/ポートとパブリックアドレス/ポート間のマッピングを記録します。

EIM エントリには、次の機能があります。

- 同じ送信元 IP およびポートから開始される後続の接続には、同じ EIM エントリが適用されます。
- EIM エントリを使用すると、外部ホストから内部ホストへの接続を逆変換できます。

例

NAT EIM エントリに関する情報を表示します。

<AC> display nat eim

```
Slot 0:
Local  IP/port: 192.168.100.100/1024
Global IP/port: 200.100.1.100/2048
Protocol: TCP(6)

Local  IP/port: 192.168.100.200/2048
Global IP/port: 200.100.1.200/4096
Protocol: UDP(17)

Total entries found: 2
```

表 13-4 コマンド出力

フィールド	説明
Protocol	プロトコルの名前と番号。
Total entries found	EIMエントリの合計数。

関連コマンド

- **nat mapping-behavior**
- **nat outbound**

13.1.8 display nat inbound

Syntax

display nat inbound

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat inbound コマンドは受信ダイナミック NAT に関する設定を表示します。

例

インバウンドダイナミック NAT コンフィグレーションを表示します。

<AC> display nat inbound

```
NAT inbound information:
  Totally 2 NAT inbound rules.
  Interface: Vlan-interface20
    ACL: 2038
    Address group ID: 2
    Add route: Y         NO-PAT: Y  Reversible: N
    Rule name: abcd
    Priority: 1000
    NAT counting: 0
    Config status: Active

Interface: Vlan-interface30
    ACL: 2037
    Address group ID: 1      Address group name: abc
    Add route: Y          NO-PAT: Y  Reversible: N
    Rule name: eif
    Priority: 1000
    NAT counting: 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.
```

表 13-5 コマンド出力

フィールド	説明
NAT inbound information	インバウンドダイナミックNAT設定に関する情報。
Totally n NAT inbound rules	インバウンドダイナミックNATルールの合計数。

フィールド	説明
Interface	受信ダイナミックNATルールが設定されているインタフェース。
ACL	ACL番号または名前。
Address group ID	受信ダイナミックNATルールで使用されるNATアドレスグループのID。
Address group name	NATアドレスグループの名前。アドレスグループ名が設定されていない場合、このフィールドは表示されません。
Add route	パケットがインバウンドダイナミックNATルールと一致したときにルートを追加するかどうか。 ・ Y:ルートを追加します。 ・ N:ルートを追加しません。
NO-PAT	NO-PATまたはPATが使用されているかどうか。 ・ Y:NO-PATが使用されます。 ・ N:PATが使用されます。
Reversible	逆アドレス変換が許可されているかどうか。 ・ Y:逆アドレス変換が許可されます。 ・ N:逆アドレス変換は許可されません。
Rule name	NATルールの名前。
Priority	NATルールのプライオリティ。
NAT counting	NATルールが一致した回数。
Config status	受信ダイナミックNATルールのステータス（Activeまたは Inactive）。
Reasons for inactive status	インバウンドダイナミックNATルールが有効にならない理由: このフィールドは、Configステータスが Inactiveの場合に使用できます。

関連コマンド

nat inbound

13.1.9 display nat log

Syntax

display nat log

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat log コマンドは NAT のログ設定を表示します

例

NAT ログ設定を表示します。

<AC> display nat log

```
NAT logging:
  Log enable         : Enabled(ACL 2000)
  Flow-begin         : Disabled
  Flow-end           : Disabled
  Flow-active        : Enabled(10 minutes)
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm              : Disabled
```

表 13-6 コマンド出力

フィールド	説明
NAT logging	NATログの設定。
Log enable	NATログのステータスを有効にします。 NATログにACLが指定されている場合、このフィールドにはACLの番号または名前も表示されます。
Flow-begin	NATセッション確立イベントのログのステータスを有効にします。
Flow-end	NATセッション削除イベントのログのステータスを有効にします。
Flow-active	アクティブなNATフローのログステータスを有効にします。有効の場合、このフィールドにはアクティブフローログが生成される間隔 (分単位) も表示されます。
Port-block-assign	ポートブロック割り当てのNAT 444ユーザログのステータスを有効にします。
Port-block-withdraw	ポートブロック取り消しのためのNAT 444ユーザログのステータスを有効にします。
Alarm	NATアラームのログステータスの有効化。

関連コマンド

- **nat log enable**
- **nat log flow-active**
- **nat log flow-begin**

13.1.10 display nat no-pat

Syntax

display nat no-pat

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat no-pat コマンドは AT NO-PAT エントリに関する情報を表示します。

NO-PAT エントリは、プライベートアドレスとパブリックアドレス間のマッピングを記録します。

NO-PAT エントリは、次の機能を提供します。

- 同じ送信元 IP アドレスから開始される後続の接続には、同じエントリが適用されます。
- NO-PAT エントリを使用すると、外部ホストから内部ホストへの接続を逆変換できます。

送信および受信 NO-PAT アドレス変換では、独自の NO-PAT テーブルが作成されます。この 2 種類のテーブルは別々に表示されます。

例

すべてのカードの NO-PAT エントリに関する情報を表示します。

<AC> display nat no-pat

```
Slot 0:
Global  IP: 200.100.1.100
Local   IP: 192.168.100.100
Reversible: N
Type     : Inbound
Local   IP: 192.168.100.200
Global  IP: 200.100.1.200
Reversible: Y
```

```
Type      : Outbound
Total entries found: 2
```

表 13-7 コマンド出力

フィールド	説明
Global IP	パブリックIPアドレス。
Local IP	プライベートIPアドレス。
Reversible	逆アドレス変換が許可されているかどうか。 • Y:逆アドレス変換が許可されます。 • N:逆アドレス変換は許可されません。
Type	NO-PATエントリのタイプ: • インバウンド:インバウンドダイナミックNAT中に作成されたNO-PATエントリ。 • Outbound :送信ダイナミックNAT中に作成されたNO-PATエントリ。
Total entries found	NO-PATエントリの総数。

関連コマンド

- **nat inbound**
- **nat outbound**

13.1.11 display nat outbound

Syntax

display nat outbound

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat outbound コマンドは送信ダイナミック NAT 設定に関する情報を表示します。

例

送信ダイナミック NAT の設定を表示します。

<AC> display nat outbound

```
NAT outbound information:
  Totally 2 NAT outbound rules.
  Interface: Vlan-interface10
    Address group ID: 1
    Port-preserved: Y       NO-PAT: N  Reversible: N
    Rule name: acdefg
    Priority: 1000
    NAT counting: 0
    Config status: Active

  Interface: Vlan-interface10
    ACL: 2037
    Address group ID: ---
    Port-preserved: N        NO-PAT: Y  Reversible: Y
    Rule name: abefg
    Priority: 1000
    NAT counting: 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL

  Interface: Vlan-interface10
    ACL: 2100
    Address group ID: 2
    Port-preserved: N         NO-PAT: N  Reversible: N
    Priority: 0
    NAT counting: 0
    Config status: Active
```

表 13-8 コマンド出力

フィールド	説明
NAT outbound information	送信ダイナミックNAT設定に関する情報。
Totally n NAT outbound rules	送信ダイナミックNATルールの合計数。
Interface	送信ダイナミックNATルールが設定されているインタフェース。
ACL	IPv 4 ACLの番号または名前。送信ダイナミックNATルールにIPv 4 ACLが指定されていない場合、このフィールドにはハイフン (---) が表示されます。

フィールド	説明
Address group ID	送信ダイナミックNATルールで使用されるアドレスグループのID。アドレスグループが指定されていない場合、フィールドにはハイフン (---) が表示されます。
Address group name	NATアドレスグループの名前。アドレスグループ名が設定されていない場合、このフィールドは表示されません。
Port-preserved	PATのポート番号を保持しようとするかどうか。 • Y:ポート番号を保持しようとします。 • N:ポート番号の変換を許可します。
NO-PAT	NO-PATが使用されているかどうか。 • Y:NO-PATが使用されます。 • N:PATが使用されます。
Reversible	逆アドレス変換が許可されているかどうか。 • Y:逆アドレス変換が許可されます。 • N:逆アドレス変換は許可されません。
Rule name	NATルールの名前。
Priority	NATルールのプライオリティ。
NAT counting	NATルールが一致した回数。
Config status	送信ダイナミックNATルールのステータス (Activeまたは Inactive) 。
Reasons for inactive status	送信ダイナミックNATルールが有効にならない理由。 このフィールドは、Configステータスが Inactiveの場合に使用できます。

関連コマンド

nat outbound

13.1.12 display nat outbound port-block-group

Syntax

display nat outbound port-block-group

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat outbound port-block-group コマンドは NAT 444 のスタティックな送信ポートブロックマッピングルールを表示します。

例

#NAT 444 のスタティック送信ポートブロックマッピングルールを表示します。

<AC> display nat outbound port-block-group

```
NAT outbound port block group information:
  Totally 2 outbound port block group items.
  Interface: Vlan-interface20
    port-block-group: 2
    Rule name: abcdefg
    NAT counting: 0
    Config status   : Active

  Interface: Vlan-interface20
    port-block-group: 10
    Rule name: abcfg
    NAT counting: 0
    Config status   : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: port block group.
```

表 13-9 コマンド出力

フィールド	説明
NAT outbound port block group information	スタティックアウトバウンドポートブロックマッピングルールに関する情報。
Totally n outbound port block group items	スタティックアウトバウンドポートブロックマッピングルールの合計数。
Interface	スタティックアウトバウンドポートブロックマッピングルールが設定されているインタフェース。
port-block-group	ポートブロックグループのID。
Rule name	スタティック送信ポートブロックマッピングルールの名前。
NAT counting	マッピングルールが一致した回数。
Config status	ポートブロックマッピングルールのステータス（Activeまたはは Inactive）。

フィールド	説明
Reasons for inactive status	ポートブロックマッピングルールが有効にならない理由。このフィールドは、Configステータスが Inactiveの場合に使用できます。

関連コマンド

nat outbound port-block-group

13.1.13 display nat port-block

Syntax

display nat port-block { **dynamic** [**address-group** { *group-id* | **name** *group-name* }] | **static** [**port-block-group** *group-id*] }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dynamic: ダイナミックポートブロックマッピングを表示します。

address-group: 指定されたアドレスグループのポートブロックマッピングを表示します。NAT アドレスグループを指定しない場合、このコマンドはすべてのアドレスグループのポートブロックマッピングを表示します。

group-id: アドレスグループの ID を指定します。この値の範囲は 0 から 65535 です。

name *group-name*: アドレスグループの名前を指定します。名前は、大文字と小文字を区別しない 1~63 文字の文字列です。

static: スタティックポートブロックマッピングを表示します。

port-block-group *group-id*: 指定されたポートブロックグループのポートブロックマッピングを表示します。*group-id* 引数には、ポートブロックグループの ID を指定します。*group-id* 引数の値の範囲は 0~65535 です。ポートブロックグループを指定しない場合、このコマンドはすべてのポートブロックグループのポートブロックマッピングを表示します。

説明

display nat port-block コマンドは NAT ポートブロックマッピングを表示します。

例

スタティックポートブロックマッピングを表示します。

<AC> display nat port-block static

```
Slot 0:
Local VPN    Local IP        Global IP       Port block   Connections
---          100.100.100.111  202.202.100.101  10001-10256  0
---          100.100.100.112  202.202.100.101  10257-10512  0
---          100.100.100.113  202.202.100.101  10513-10768  0
---          100.100.100.113  202.202.100.101  10769-11024  0
Total mappings found: 4
```

ダイナミックポートブロックマッピングを表示します。

<AC> display nat port-block dynamic

```
Slot 0:
Local VPN    Local IP        Global IP       Port block   Connections
---          101.1.1.12      192.168.135.201  10001-11024  1
Total mappings found: 1
```

表 13-10 コマンド出力

フィールド	説明
Local VPN	このフィールドは、現在のソフトウェアバージョンではサポートされていません。 プライベートIPアドレスが属するMPLS L 3 VPNインスタンス。プライベートIPアドレスがどのVPNインスタンスにも属していない場合、このフィールドにはハイフン (---) が表示されます。
Local IP	プライベートIPアドレス。
Global IP	パブリックIPアドレス。
Port block	開始ポート番号と終了ポート番号で定義されたポートブロック。
Connections	ポートブロック内のポートを使用して確立された接続の数。

13.1.14 display nat port-block-group

Syntax

display nat port-block-group [*group-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-id: NAT ポートブロックグループの ID を指定します。この値の範囲は 0 から 65535 です。この引数を指定しない場合、コマンドはすべての NAT ポートブロックグループの設定を表示します。

説明

display nat port-block-group コマンドは NAT ポートブロックグループの設定を表示します。

例

#すべての NAT ポートブロックグループの設定を表示します。

<AC> display nat port-block-group

```
NAT port block group information:
  Totally 3 NAT port block groups.
  Port block group 1:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address       End address         VPN instance
      172.16.1.1          172.16.1.254        ---
      192.168.1.1         192.168.1.254       ---
      192.168.3.1         192.168.3.254       ---
    Global IP pool information:
      Start address       End address
      201.1.1.1           201.1.1.10
      201.1.1.21          201.1.1.25

  Port block group 2:
    Port range: 10001-30000
    Block size: 500
    Local IP address information:
      Start address       End address         VPN instance
      10.1.1.1            10.1.10.255         ---
    Global IP pool information:
      Start address       End address
```

```
    202.10.10.101       202.10.10.120

Port block group 3:
  Port range: 1-65535
  Block size: 256
  Local IP address information:
    Start address       End address         VPN instance
    ---                 ---                 ---
  Global IP pool information:
    Start address       End address
    ---                 ---
```

NAT ポートブロックグループ 1 の情報を表示します。

<AC> display nat port-block-group 1

```
Port block group 1:
  Port range: 1-65535
  Block size: 256
  Local IP address information:
    Start address       End address         VPN instance
    172.16.1.1          172.16.1.254        ---
    192.168.1.1         192.168.1.254       ---
    192.168.3.1         192.168.3.254       ---
  Global IP pool information:
    Start address       End address
    201.1.1.1           201.1.1.10
    201.1.1.21          201.1.1.25
```

表 13-11 コマンド出力

フィールド	説明
NAT port block group information	ポートブロックグループの設定に関する情報。
Totally n NAT port block groups	ポートブロックグループの合計数。
Port block group	ポートブロックグループのID。
Port range	パブリックIPアドレスのポート範囲。
Block size	ポートブロック内のポート数。
Local IP address information	プライベートIPアドレスに関する情報。
Global IP pool information	パブリックIPアドレスに関する情報。

フィールド	説明
Start address	プライベートまたはパブリックIPアドレス範囲の開始IPアドレス。アドレス範囲に開始IPアドレスが指定されていない場合は、ハイフン (---) が表示されます。
End address	プライベートまたはパブリックIPアドレス範囲の終了IPアドレス。アドレス範囲に終了IPアドレスを指定していない場合は、 「---」 が表示されます。
VPN instance	このフィールドは、現在のソフトウェアバージョンではサポートされていません。 プライベートIPアドレス範囲が属するMPLS L 3 VPNインスタンス。プライベートアドレス範囲にVPNインスタンスが指定されていない場合、このフィールドにはハイフン (---) が表示されます。

関連コマンド

nat port-block-group

13.1.15 display nat port-block-usage

Syntax

display nat port-block-usage [**address-group** *group-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

address-group *group-id*: アドレスグループの ID を指定します。*group-id* 引数の値の範囲は 0~65535 です。アドレスグループを指定しない場合、このコマンドはすべてのアドレスグループのポートブロック使用状況を表示します。

説明

display nat port-block-usage コマンドはアドレスグループのポートブロック使用状況を表示します。

例

#アドレスグループのポートブロック使用状況を表示します。

<AC> display nat port-block-usage

```
Slot 1:
Address group 0 on channel 0:
  Total port block entries :10
  Active port block entries:9
  Current port block usage :90%

Total NAT address groups found: 1
```

表 13-12 コマンド出力

フィールド	説明
CPU	CPUの番号。
Address group	アドレスグループのID。
channel	Field-Programmable Gate Array (FPGA) ID。
Total port block entries	アドレスグループ内のポートブロックの合計数。
Active port block entries	アドレスグループ内の割り当てられたポートブロックの合計数。
Current port block usage	アドレスグループのポートブロック使用状況。
Total NAT address groups found	アドレスグループの合計数。

13.1.16 display nat server

Syntax

display nat server

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat server コマンドは NAT サーバマッピングを表示します。

例

NAT サーバマッピングを表示する。

<AC> display nat server

```
NAT internal server information:
  Totally 2 internal servers.
  Interface: Vlan-interface10
    Protocol: 6(TCP)
    Global IP/port: 50.1.1.1/23-30
    Local IP/port : 192.168.10.15-192.168.10.22/23
    Rule name     : abcg
    NAT counting  : 0
    Config status : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

  Interface: Vlan-interface20
    Protocol: 255(Reserved)
    Global IP/port: 50.1.1.100/---
    Local IP/port : 192.168.10.150/---
    Rule name     : abcdefg
    NAT counting  : 0
    Config status : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: interface IP address.
```

表 13-13 コマンド出力

フィールド	説明
NAT internal server information	NATサーバマッピングに関する情報。
Interface	NATサーバマッピングが設定されているインタフェース。
Protocol	内部サーバのプロトコル番号と名前。
Global IP/port	内部サーバのパブリックIPアドレスとポート番号。 • Global IP:単一のIPアドレスまたはIPアドレス範囲。Easy IP を使用する場合、このフィールドには指定したインタフェースのIPアドレスが表示されます。インタフェースのアドレスを指定しない場合、 [Global IP] フィールドにはハイフン (---) が表示されます。 • port:単一のポート番号またはポート番号の範囲。指定したプロトコルにポート番号がない場合、ポートフィールドにはハイフン (---) が表示されます。

フィールド	説明
Local IP/port	一般的なNATサーバマッピングとオブジェクトグループベースのNATサーバマッピングの場合、このフィールドには内部サーバのプライベートIPアドレスとポート番号が表示されます。 ● Local IP :単一のIPアドレスまたはIPアドレス範囲。 ● port:単一のポート番号またはポート番号の範囲。指定したプロトコルにポート番号がない場合、ポートフィールドにはハイフン (---) が表示されます。 負荷分散NATサーバマッピングの場合、このフィールドには、内部サーバグループID、IPアドレス、ポート番号、および各メンバーの接続数が表示されます。
ACL	ACL番号または名前。ACLが指定されていない場合、このフィールドは表示されません。
Rule name	NATサーバマッピングの名前。
NAT counting	NATサーバマッピングが一致した回数。
Config status	NATサーバマッピングのステータス (ActiveまたはInactive) 。
Reasons for inactive status	NATサーバマッピングが有効にならない理由。このフィールドは、ConfigステータスがInactiveの場合に使用できます。

関連コマンド

nat server

13.1.17 display nat server-group

Syntax

display nat server-group [*group-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-id: 内部サーバグループの ID を指定します。この値の範囲は 0 から 65535 です。この引数を指定しない場合、すべての内部サーバグループの設定が表示されます。

説明

display nat server-group コマンドは内部サーバグループの設定を表示します。

例

すべての内部サーバグループの設定を表示します。

<AC> display nat server-group

```
NAT server group information:
  Totally 3 NAT server groups.
  Group Number       Inside IP           Port       Weight
  1                192.168.0.26         23         100
                   192.168.0.27         23         500
  2                ---                 ---        ---
  3                192.168.0.26         69         100
```

内部サーバグループ 1 の設定を表示します。

<AC> display nat server-group 1

```
  Group Number       Inside IP           Port       Weight
  1                192.168.0.26         23         100
                   192.168.0.27         23         500
```

表 13-14 コマンド出力

フィールド	説明
NAT server group information	NATサーバグループの設定に関する情報。
Totally n NAT server groups	NATサーバグループの総数。
Group Number	内部サーバグループのID。
Inside IP	内部サーバグループ内のサーバのプライベートIPアドレス。アドレスが指定されていない場合、このフィールドにはハイフン (---) が表示されます。
Port	内部サーバグループ内のサーバのプライベートポート番号。ポート番号が指定されていない場合、このフィールドにはハイフン (---) が表示されます。
Weight	内部サーバグループ内のサーバの重み。重み値が指定されていない場合、このフィールドにはハイフン (---) が表示されます。

関連コマンド

nat server-group

13.1.18 display nat session

Syntax

display nat session [[**responder**] { **source-ip** *source-ip* | **destination-ip** *destination-ip* } *] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

responder: NAT セッションをレスポンダ別に表示します。このキーワードを指定しない場合、このコマンドは NAT セッションを発信側別に表示します。

source-ip *source-ip*: source-ip 引数で指定された送信元 IP アドレスの NAT セッションを表示します。IP アドレスは、セッションの確立をトリガーするパケットの送信元 IP アドレスである必要があります。

destination-ip *destination-ip*: destination-ip 引数で指定された宛先 IP アドレスの NAT セッションを表示します。IP アドレスは、セッションの確立をトリガーするパケットの宛先 IP アドレスである必要があります。

verbose: NAT セッションに関する詳細情報を表示します。このキーワードを指定しない場合、このコマンドは NAT セッションに関する簡単な情報を表示します。

説明

display nat session コマンドは NAT セッションを表示します。

パラメータを指定しない場合、このコマンドはすべての NAT セッションを表示します。

例

NAT セッションに関する詳細情報を表示します。

<AC> display nat session verbose

```
Slot 0:
Initiator:
  Source     IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Vlan-interface10
  Source security zone: SrcZone
```

```
Responder:
  Source     IP/port: 192.168.1.55/22
  Destination IP/port: 192.168.1.10/1877
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Vlan-interface20
  Source security zone: DestZone
State: TCP_SYN_SENT
Application: SSH
Rule ID: -/-/-
Rule name:
Start time: 2011-07-29 19:12:36  TTL: 28s
Initiator->Responder:        1 packets        48 bytes
Responder->Initiator:        0 packets         0 bytes

Total sessions found: 1
```

表 13-15 コマンド出力

フィールド	説明
Initiator	イニシエータに関するセッション情報。
Responder	応答側に関するセッション情報。
Source IP/port	送信元IPアドレスおよびポート番号。
Destination IP/port	宛先IPアドレスおよびポート番号。
DS-Lite tunnel peer	DS-Liteトンネルインタフェースの宛先アドレス。セッションがどのDS-Liteトンネルにも属していない場合、このフィールドにはハイフン (-) が表示されます。
VPN instance/VLAN ID/Inline ID	セッションが属するMPLS L 3 VPNインスタンス。VPNインスタンスフィールドは、現在のソフトウェアバージョンではサポートされていません。
Protocol	レイヤ2転送のためにセッションが属するVLAN ID。
Inbound interface	レイヤ2転送のためにセッションが属するINLINE。
State	設定が指定されていない場合、このフィールドにはハイフン (-) が表示されます。
Application	FTPやDNSなどのアプリケーション層プロトコル・タイプ。このフィールドには、既知でないポートによって識別されるプロトコルタイプのOTHERが表示されます。

フィールド	説明
Rule ID	セキュリティ・ポリシー・ルールのID。
Rule name	セキュリティ・ポリシー・ルールの名前。
Start time	セッションの開始時刻。
TTL	残りのNATセッションライフタイム (秒) 。
Initiator->Responder	送信側から応答側へのパケット数およびパケットバイト数。
Responder->Initiator	応答側から送信側へのパケット数およびパケットバイト数。
Total sessions found	セッションの合計数。

関連コマンド

reset nat session

13.1.19 display nat static

Syntax

display nat static

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat static コマンドはスタティック NAT マッピングを表示します。

例

スタティック NAT マッピングを表示します。

<AC> display nat static

```
Static NAT mappings:
  Totally 2 inbound static NAT mappings.
  Net-to-net:
```

```
    Global IP    : 1.1.1.1 - 1.1.1.255
    Local IP     : 2.2.2.0
    Netmask      : 255.255.255.0
    ACL         : 2000
    Reversible   : Y
    NAT counting : 0
    Rule name    : abcdefg
    Priority     : 1000
    Config status: Active

  IP-to-IP:
    Global IP    : 5.5.5.5
    Local IP     : 4.4.4.4
    ACL         : 2000
    Reversible   : Y
    Rule name    : abefg
    Priority     : 1000
    NAT counting : 0
   Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: local VPN, global VPN,
and ACL.

Totally 2 outbound static NAT mappings.
  Net-to-net:
    Local IP     : 1.1.1.1 - 1.1.1.255
    Global IP    : 2.2.2.0
    Netmask      : 255.255.255.0
    ACL         : 2000
    Reversible   : Y
    Rule name    : abefg
    Priority     : 1000
    NAT counting : 0
    Config status: Active

  IP-to-IP:
    Local IP     : 4.4.4.4
    Global IP    : 5.5.5.5
    ACL:        : 2001
    Reversible   : Y
    Rule name    : abcd
    Priority     : 1000
    NAT counting : 0
```

```
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

Interfaces enabled with static NAT:
  Totally 2 interfaces enabled with static NAT.
  Interface: Vlan-interface20
    Config status: Active

  Interface: Vlan-interface30
    Config status: Active
```

表 13-16 コマンド出力

フィールド	説明
Static NAT mappings	スタティックNATマッピングの設定に関する情報。
Totally n inbound static NAT mappings	インバウンドスタティックNATマッピングの合計数。
Totally n outbound static NAT mappings	送信スタティックNATマッピングの合計数。
Net-to-net	Net-to-netスタティックNATマッピング。
IP-to-IP	1対1のスタティックNATマッピング。
Local IP	プライベートIPアドレスまたはアドレス範囲。
Global IP	パブリックIPアドレスまたはアドレス範囲。
Netmask	ネットワークマスク。
ACL	ACL番号または名前。ACLが指定されていない場合、このフィールドは表示されません。
Reversible	逆アドレス変換を許可するかどうか。逆アドレス変換が許可されている場合、このフィールドにはYと表示されます。逆アドレス変換が許可されていない場合、このフィールドは表示されません。
Interfaces enabled with static NAT	スタティックNATが有効になっているインタフェース。
Totally n interfaces enabled with static NAT	スタティックNATが有効になっているインタフェースの総数。
Interface	スタティックNATが有効になっているインタフェース。
Rule name	NATルールの名前。

フィールド	説明
Priority	NATルールのプライオリティ。
NAT counting	NATルールが一致した回数。
Config status	スタティックNATマッピングのステータス (Activeまたは Inactive) 。
Reasons for inactive status	スタティックNATマッピングが有効にならない理由。このフィールドは、Configステータスがinactiveの場合に使用できます。

関連コマンド

- **nat static enable**
- **nat static inbound**
- **nat static inbound net-to-net**
- **nat static outbound**
- **nat static outbound net-to-net**

13.1.20 display nat statistics

Syntax

display nat statistics [**summary**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

summary: NAT 統計情報の要約を表示します。このキーワードを指定しない場合、このコマンドは詳細な NAT 統計情報を表示します。

説明

display nat statistics コマンドは NAT 統計情報を表示します。

例

NAT 統計情報の詳細情報を表示します。

<AC> display nat statistics

```
Slot 0:
```

```
Session creation rate: 0
Total session entries: 100
Total EIM entries: 1
Total inbound NO-PAT entries: 0
Total outbound NO-PAT entries: 0
Total static port block entries: 10
Total dynamic port block entries: 15
Active static port block entries: 0
Active dynamic port block entries: 0
```

表 13-17 コマンド出力

フィールド	説明
Total session entries	NATセッションエントリの数。
Session creation rate	1秒あたりに作成されたNATセッションの数。
Total EIM entries	EIMエントリの合計数。
Total inbound NO-PAT entries	インバウンドNO-PATエントリの合計数。
Total outbound NO-PAT entries	送信NO-PATエントリの合計数。
Total static port block entries	スタティックNAT 444マッピングの合計数。
Total dynamic port block entries	作成可能なダイナミックポートブロックマッピングの総数。これは、割り当て済みおよび未割り当てのポートブロックを含む、ダイナミック割り当てのポートブロック数と同じです。
Active static port block entries	使用中のスタティックポートブロックマッピングの数。
Active dynamic port block entries	作成されたダイナミックポートブロックマッピングの数。これは、ダイナミックに割り当てられたポートブロックの数と同じです。

NAT 統計情報のサマリーを表示します。

<AC> display nat statistics summary

```
EIM: Total EIM entries.
SPB: Total static port block entries.
DPB: Total dynamic port block entries.
ASPB: Active static port block entries.
ADPB: Active dynamic port block entries.
Slot Sessions  EIM      SPB      DPB      ASPB     ADPB
0    100       1        10       15       0        0
```

表 13-18 コマンド出力

フィールド	説明
Sessions	NATセッションエントリの数。
EIM	EIMエントリの数。
SPB	スタティックNAT 444マッピングの数。
DPB	作成可能なダイナミックポートブロックマッピングの数。これは、割り当て済みおよび未割り当てのポートブロックを含む、ダイナミック割り当てのポートブロック数と同じです。
ASPB	使用中のスタティックポートブロックマッピングの数。
ADPB	作成されたダイナミックポートブロックマッピングの数。これは、ダイナミックに割り当てられたポートブロックの数と同じです。

13.1.21 global-ip-pool

Syntax

global-ip-pool *start-address end-address*

undo global-ip-pool *start-address* [*end-address*]

デフォルト

設定なし

View

NAT port block group view

定義済みユーザロール

network-admin

パラメータ

start-address end-address: パブリック IP アドレス範囲の開始 IP アドレスと終了 IP アドレスを指定します。終了 IP アドレスは開始 IP アドレスより小さくできません。開始 IP アドレスと終了 IP アドレスが同じ場合は、パブリック IP アドレスを 1 つだけ指定します。

説明

global-ip-pool コマンドは、パブリック IP アドレス範囲を NAT ポートブロックグループに追加します。

undo global-ip-pool コマンドは NAT ポートブロックグループからパブリック IP アドレス範囲を削除します。

スタティックポートブロックマッピングは、パブリック IP アドレスを複数のプライベート IP アドレスにマッピングし、各プライベート IP アドレスに一意のポートブロックを割り当てます。パブリック IP アドレスが割り当てることができるポートブロックの数は、ポート範囲内のポート数をポートブロックサイズで割って決定されます。

このコマンドを実行するたびに、アドレス範囲に最大 255 のパブリック IP アドレスを含めることができます。1 つのポートブロックグループ内のすべてのパブリック IP アドレス範囲は重複できません。

異なるポートブロックグループ内のパブリック IP アドレス範囲は重複する可能性があります。重複するパブリック IP アドレス範囲のポート範囲は重複できません。

例

#ポートブロックグループ 1 にパブリック IP アドレス範囲を追加します。パブリック IP アドレスの範囲は、202.10.1.1~202.10.1.10 の IP アドレスで構成されます。

<AC> system-view

[AC] nat port-block-group 1

[AC-port-block-group-1] global-ip-pool 202.10.1.1 202.10.1.10

関連コマンド

nat port-block-group

13.1.22 inside ip

Syntax

inside ip *inside-ip* **port** *port-number* [**weight** *weight-value*]

undo inside ip *inside-ip* **port** *port-number*

デフォルト

設定なし

View

Internal server group view

定義済みユーザロール

network-admin

パラメータ

inside-ip: 内部サーバの IP アドレスを指定します。

port *port-number*: 内部サーバのポート番号を 1~65535 の範囲で指定します (FTP ポート 20 は除く) 。

weight *weight-value*: 内部サーバの重みを指定します。値の範囲は 1 から 1000 で、デフォルト値は 100 です。

説明

inside ip コマンドは内部サーバグループにサーバを追加します。

undo inside ip コマンドは内部サーバグループからサーバを削除します。

重みが大きい内部サーバほど、内部サーバグループ内の接続の割合が大きくなります。

例

#IP アドレス 10.1.1.2、ポート番号 30 のサーバを内部サーバグループ 1 に追加します。

<AC> system-view

[AC] nat server-group 1

[AC-nat-server-group-1] inside ip 10.1.1.2 port 30

関連コマンド

nat server-group

13.1.23 local-ip-address

Syntax

local-ip-address *start-address end-address*

undo local-ip-address *start-address* [*end-address*]

デフォルト

設定なし

View

NAT port block group view

定義済みユーザロール

network-admin

パラメータ

start-address end-address: プライベート IP アドレス範囲の開始 IP アドレスと終了 IP アドレスを指定します。終了 IP アドレスは開始 IP アドレスより小さくできません。開始 IP アドレスと終了 IP アドレスが同じ場合は、プライベート IP アドレスを 1 つだけ指定します。

説明

local-ip-address コマンドはプライベート IP アドレス範囲を NAT ポートブロックグループに追加します。

undo local-ip-address コマンドは NAT ポートブロックグループからプライベート IP アドレス範囲を削除します。

スタティックポートブロックマッピングは、1 つのパブリック IP アドレスを複数のプライベート IP アドレスにマッピングし、各プライベート IP アドレスに一意のポートブロックを割り当てます。

NAT ポートブロックグループでは、プライベート IP アドレスの数を、割り当て可能なポートブロックの数より大きくすることはできません。そうしないと、一部のプライベート IP アドレスはポートブロックを取得できません。パブリック IP アドレスが割り当てることができるポートブロックの数は、ポート範囲内のポート数をポートブロックサイズで割って決定されます。

例

#プライベート IP アドレス範囲をポートブロックグループ 1 に追加します。プライベート IP アドレス範囲は、172.16.1.1~172.16.1.255 の IP アドレスで構成されます。

<AC> system-view

[AC] nat port-block-group 1

[AC-port-block-group-1] local-ip-address 172.16.1.1 172.16.1.255

関連コマンド

nat port-block-group

13.1.24 nat address-group

Syntax

nat address-group *group-id* [**name** *group-name*]

undo nat address-group *group-id*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id : NAT アドレスグループの ID を指定します。この引数の値の範囲は 0 から 65535 です。

name *group-name*: NAT アドレスグループに名前を割り当てます。*group-name* 引数は、1~63 文字のストリングで、大文字と小文字が区別されます。

説明

nat address-group コマンドは NAT アドレスグループを作成し、そのビューを移行するか、または既存の NAT アドレスグループのビューを移行します。

undo nat address-group コマンドは NAT アドレスグループを削除します。

NAT アドレスグループは、アドレス範囲のセットです。address コマンドを使用して、NAT アドレスグループにアドレス範囲を追加します。ダイナミック NAT は、パケットの送信元 IP アドレスをアドレスグループ内の IP アドレスに変換します。

例

#番号が 1 で名前が abc の NAT アドレスグループを作成します。

<AC> system-view

[AC] nat address-group 1 name abc

関連コマンド

- **address**
- **display nat address-group**
- **display nat all**
- **nat inbound**
- **nat outbound**

13.1.25 nat alg

Syntax

nat alg { **all** | **dns** | **ftp** | **h323** | **icmp-error** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **sip** | **sqlnet** | **tftp** | **xdmcp** }

undo nat alg { **all** | **dns** | **ftp** | **h323** | **icmp-error** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **sip** | **sqlnet** | **tftp** | **xdmcp** }

デフォルト

dns, ftp, icmp-error, rtsp, pptp：有効

その他：無効

View

System view

定義済みユーザロール

network-admin

パラメータ

all: サポートされているすべてのプロトコルに対して NAT ALG を有効にします。

dns: DNS の NAT ALG を有効にします。

ftp: FTP の NAT ALG を有効にします。

h323: H.323 の NAT ALG を有効にします。

icmp-error: ICMP エラーパケットの NAT ALG を有効にします。

ils: ILS の NAT ALG を有効にします。

mgcp: MGCP の NAT ALG を有効にします。

nbt: NBT の NAT ALG を有効にします。

pptp: PPTP の NAT ALG を有効にします。

rsh: RSH の NAT ALG を有効にします。

rtsp: RTSP の NAT ALG を有効にします。

sccp: SCCP の NAT ALG を有効にします。

sip: SIP の NAT ALG を有効にします。

sqlnet: SQLNET 用の NAT ALG を有効にします。

tftp: TFTP の NAT ALG を有効にします。

xdmcp: XDMCP の NAT ALG を有効にします。

説明

nat alg コマンドは、指定されたプロトコルまたはサポートされているすべてのプロトコルに対して NAT ALG を有効にします。

undo nat alg コマンドは、指定したプロトコルまたはサポートされているすべてのプロトコルの NAT ALG を無効にします。

NAT ALG は、アプリケーション層ペイロード内のアドレスまたはポート情報を変換して、接続の確立を保証します。

たとえば、FTP アプリケーションには、データ接続と制御接続が含まれます。データ接続の IP アドレスとポート番号は、制御接続のペイロード情報によって異なります。これには、NAT ALG がアドレスおよびポート情報を変換してデータ接続を確立する必要があります。

例

#FTP の NAT ALG を有効にします。

<AC> system-view

[AC] nat alg ftp

関連コマンド

display udp statistics

13.1.26 nat dns-map

Syntax

nat dns-map domain *domain-name* **protocol** *pro-type* { **interface** *interface-type interface-number* | **ip** *global-ip* } **port** *global-port*

undo nat dns-map domain *domain-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

domain *domain-name*: 内部サーバのドメイン名を指定します。ドメイン名は、大文字と小文字を区別しないドット区切りの文字列で、文字、数字、ハイフン (-) 、アンダースコア (_) 、およびドット (。) (例:aabbcc.com)。ドメイン名には最大 253 文字を含めることができ、各文字列は 63 文字以下で区切ります。

protocol *pro-type*: 内部サーバによって使用されるプロトコルのタイプ (tcp または udp) を指定します。

interface *interface-type interface-number*: Easy IP がインタフェースのタイプと番号で指定された IP アドレスを内部サーバのパブリックアドレスとして使用できるようにします。

ip *global-ip*: 外部ネットワークにサービスを提供するために内部サーバによって使用されるパブリック IP アドレスを指定します。

port *global-port*: 外部ネットワークにサービスを提供するために内部サーバによって使用されるパブリックポート番号を指定します。ポート番号の形式は、次のいずれかです。

- 1 から 65535 までの数値。
- プロトコル名。1 から 15 文字の文字列。(例)ftp、telnet

説明

nat dns-map コマンドは NAT DNS マッピングを設定します。

undo nat dns-map コマンドは NAT DNS マッピングを削除します。

NAT DNS マッピングは、NAT サーバ機能と連携する必要があります。

- NAT DNS マッピングは、内部サーバのドメイン名を、内部サーバのパブリック IP アドレス、パブリックポート番号、およびプロトコルタイプにマッピングします。
- NAT サーバマッピングは、パブリック IP およびポートを内部サーバのプライベート IP およびポートにマッピングします。

この連携により、内部ホストは、DNS サーバがパブリックネットワーク上にあるときに、内部サーバのドメイン名を使用して同じプライベートネットワーク上の内部サーバにアクセスできます。外部 DNS サーバからの DNS 応答には、ペイロード内の内部サーバのドメイン名とパブリック IP アドレスだけが含まれます。NAT インタフェースには、複数の内部サーバが同じパブリック IP アドレスを持つが、異なるプライベート IP アドレスを持つように設定されている場合があります。DNS ALG は、パブリック IP アドレスだけを使用して不正な内部サーバを検出する場合があります。DNS マッピングが設定されている場合、DNS ALG はドメイン名を使用して内部サーバのパブリック IP アドレス、パブリックポート番号、およびプロトコルタイプを取得できます。次に、内部サーバのパブリック IP アドレス、パブリックポート番号、およびプロトコルタイプを使用して、正しい内部サーバを検索できます。

複数の NAT DNS マッピングを設定できます。

例

#NAT DNS マッピングを設定して、ドメイン名 www.server.com をパブリック IP アドレス 202.112.0.1、パブリックポート番号 12345、およびプロトコルタイプ TCP にマッピングします。

<AC> system-view

[AC] nat dns-map domain www.server.com protocol tcp ip 202.112.0.1 port 12345

関連コマンド

- **display nat all**
- **display nat dns-map**
- **nat server**

13.1.27 nat icmp-error reply

Syntax

nat icmp-error reply

undo nat icmp-error reply

デフォルト

NAT 障害時の ICMP エラーメッセージの送信無効

View

System view

定義済みユーザロール

network-admin

説明

nat icmp-error reply コマンドは NAT 障害時の ICMP エラーメッセージの送信を有効にします。

undo nat icmp-error reply コマンドはデフォルト状態に戻します。

NAT 障害時の ICMP エラーメッセージの送信を無効にすると、不要なパケットが減少し、帯域幅が節約され、デバイスの IP アドレスがパブリックネットワークに公開されなくなります。

このコマンドは traceroute に必要です。

例

#NAT 失敗時の ICMP エラーメッセージの送信を有効にします。

<AC> system-view

[AC] nat icmp-error reply

13.1.28 nat inbound

Syntax

nat inbound { *ipv4-acl-number* | **name** *ipv4-acl-name* } **address-group** { *group-id* | **name** *group-name* } [**no-pat** [**reversible**] [**add-route**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*] [**counting**]

undo nat inbound { *ipv4-acl-number* | **name** *ipv4-acl-name* }

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ipv4-acl-number: 2000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、すべてを指定することはできません。

address-group: アドレス変換のアドレスグループを指定します。

group-id: アドレスグループ ID を指定します。この引数の値の範囲は 0 から 65535 です。

name *group-name*: アドレスグループ名を指定します。1~63 文字で、大文字と小文字は区別されません。

no-pat: NO-PAT モードを使用します。このキーワードを指定しない場合は、PAT が使用されます。PAT では、TCP、UDP、および ICMP クエリーパケットだけがサポートされます。ICMP パケットの場合、送信元ポート番号として ICMP ID が使用されます。

reversible: 逆アドレス変換をイネーブルにします。逆アドレス変換は、既存の NO-PAT エントリを使用して、内部ネットワークからアクティブに開始された接続の宛先アドレスを外部ネットワークに変換します。

add-route: 変換後に自動的に送信元アドレスにルートを追加します。出力インタフェースは NAT インタフェースで、ネクストホップは変換前の送信元アドレスです。

rule *rule-name*: ルールの名前を指定します。大文字と小文字が区別され、1~63 文字のストリングで指定します。バックスラッシュ (¥) 、スラッシュ (/) 、コロン (:) 、アスタリスク (*) 、疑問符 (?) 、左かぎかっこ (<) 、右かぎかっこ (>) 、縦棒 (|) 、引用符 (") 、またはアット記号 (@) です。このオプションを指定しない場合、規則に名前はありません。

priority *priority*: ルールのプライオリティを 0~2147483647 の範囲で指定します。値が小さいほど、優先順位が高くなります。このオプションを指定しない場合、同じタイプの NAT 規則の中で優先順位が最も低くなります。

disable: 受信ダイナミック NAT ルールを無効にします。このキーワードを指定しない場合、ルールは有効になります。

description *text*: 受信ダイナミック NAT ルールの説明を指定します。text 引数は、大文字と小文字を区別しない 1~63 文字の文字列です。

counting: NAT カウントを有効にします。アドレスマッピングを使用するフローの数がカウントされます。

説明

nat inbound コマンドは受信ダイナミック NAT ルールを設定します。

undo nat inbound コマンドは受信ダイナミック NAT ルールを削除します。

受信ダイナミック NAT は、ACL によって許可された受信パケットの送信元 IP アドレスをアドレスグループ内の IP アドレスに変換します。

受信ダイナミック NAT は、次のモードをサポートします。

- [PAT] :IP アドレス変換とポート変換の両方を実行します。
- [NO-PAT] :IP アドレス変換だけを実行します。

NO-PAT モードでは、逆アドレス変換がサポートされます。逆アドレス変換では、ACL 逆マッチングを使用して、変換するパケットを識別します。ACL リバースマッチングは次のように機能します。

- パケットの送信元 IP アドレス/ポートと ACL 内の宛先 IP アドレス/ポートを比較します。
- 一致する NO-PAT エントリに従ってパケットの宛先 IP アドレスを変換し、変換された宛先 IP アドレス/ポートを ACL 内の送信元 IP アドレス/ポートと比較します。

受信ダイナミック NAT は通常、次のいずれかと連携して双方向 NAT を実装します。

- 送信ダイナミック NAT (nat outbound コマンド) 。
- NAT Server (nat server コマンド) 。
- 送信スタティック NAT (nat static コマンド) 。

アドレスグループは、nat inbound コマンドと nat outbound コマンドの両方で使用できません。nat inbound コマンドでは、PAT モードと NO-PAT モードの両方で使用できません。

内部ネットワークと外部ネットワークが存在するサブネットが重複している場合は、add-route キーワードを指定しないでください。その他のネットワークシナリオの場合:

- add-route キーワードを指定すると、デバイスはパケットの変換後に自動的に送信元アドレスにルートを追加します。宛先アドレスは NAT アドレスグループ内の NAT アドレス、出力インタフェースはコマンドが実行されるインタフェース、ネクストホップは変換前の送信元アドレスです。
- add-route キーワードを指定しない場合は、ルートを手動で追加する必要があります。自動ルート追加は低速であるため、手動でルートを追加することをお勧めします。

ACL は、インタフェース上の 1 つの受信ダイナミック NAT ルールだけで使用できます。

1 つのインタフェースに複数の受信ダイナミック NAT ルールを設定できます。

同じプライオリティ値で設定された受信ダイナミック NAT ルールは、その ACL を使用して照合されます。

- 名前付き ACL を持つ NAT ルールは、名前なし ACL を持つ NAT ルールよりも優先順位が高くなります。
- 名前付き ACL を持つ NAT ルールは、ACL 名のアルファベット順に照合されます。
- 名前なし ACL を持つ NAT ルールは、ACL 番号の降順で照合されます。

例

#サブネット 10.110.10.0/24 からのパケットだけを通過させるには、ACL 2001 を設定します。

<AC> system-view

[AC] acl basic 2001

[AC-acl-ipv4-basic-2001] rule permit source 10.110.10.0 0.0.0.255

[AC-acl-ipv4-basic-2001] rule deny

[AC-acl-ipv4-basic-2001] quit

#アドレスグループ 1 を作成し、アドレス範囲 202.110.10.10~202.110.10.12 をグループに追加します。

[AC] nat address-group 1

[AC-address-group-1] address 202.110.10.10 202.110.10.12

[AC-address-group-1] quit

#インバウンド NO-PAT ルールをインタフェース VLAN インタフェース 10 に設定します。NAT は、受信パケットの送信元アドレスをアドレスグループ 1 のアドレスに変換し、変換されたパケットのルートを自動的に追加します。ルール名を abc に、優先順位を 0 に設定します。

[AC] interface vlan-interface 10

[AC-Vlan-interface10] nat inbound 2001 address-group 1 no-pat add-route rule abc priority 0

関連コマンド

- **display nat all**
- **display nat inbound**
- **display nat no-pat**

13.1.29 nat inbound rule move

Syntax

nat inbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

View

Interface view

定義済みユーザロール

network-admin

パラメータ

nat-rule-name1: 移動するルールの名前を指定します。

after: ルール nat-rule-name 1 をルール nat-rule-name 2 の後の行 (参照ルールと呼ばれます) に移動します。参照規則の優先度の値は変更されません。移動されたルールの優先度の値は、参照ルールの優先度の値に 1 を加えた値と等しくなります。

before: ルール nat-rule-name 1 をルール nat-rule-name 2 の前の行に移動します。参照規則の優先度の値は変更されません。移動したルールの優先度値は、参照ルールの優先度値から 1 を引いた値と等しくなります。

nat-rule-name2: 移動する NAT 規則の参照規則として、NAT 規則の名前を指定します。

説明

nat inbound rule move コマンドは受信ダイナミック NAT ルールのプライオリティを変更します。

このコマンドは、名前付きインバウンドダイナミック NAT ルールにのみ適用できます。

ルールリストの前の方に表示されている NAT ルールは、パケットマッチングの優先順位が高くなります。

例

#インバウンドダイナミック NAT ルール abc を、ルール def の前の行に移動します。

<AC> system-view

[AC] interface vlan-interface 10

[AC-Vlan-interface10] nat inbound rule move abc before def

関連コマンド

nat inbound

13.1.30 nat log alarm

Syntax

nat log alarm

undo nat log alarm

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

nat log alarm コマンドは NAT アラームのログを有効にします。

undo nat log alarm コマンドは NAT アラームのログを無効にします。

NAT リソースが十分でない場合、変換が必要なパケットはドロップされます。NO-PAT では、NAT リソースはパブリック IP アドレスを参照します。EIM PAT では、NAT リソースはパブリック IP アドレスおよびポートを参照します。NAT 444 では、NAT リソースはパブリック IP アドレス、ポートブロック、またはポートブロック内のポートを参照し

ます。NAT アラームログは NAT リソースの使用状況を監視し、NAT リソースが十分でない場合はログを出力します。

ダイナミックポートブロックマッピングの拡張ポートブロック内のポートがすべて占有されている場合、NAT 444 ゲートウェイはアラームログを生成します。

NAT のアラームログを設定する前に、カスタム NAT ログ生成および出力機能を設定する必要があります。

このコマンドは、nat log enable コマンドを使用して NAT ログを有効にした後にだけ有効になります。

例

#NAT アラームログを有効にします。

<AC> system-view

[AC] nat log alarm

関連コマンド

- **display nat all**
- **display nat log**
- **nat log enable**

13.1.31 nat log enable

Syntax

nat log enable [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }]

undo nat log enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

acl: ACL を指定します。

ipv4-acl-number: 2000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、all を指定することはできません。

説明

nat log enable コマンドは NAT のログを有効にします。

undo nat log enable コマンドは NAT のログを無効にします。

NAT セッションログ、NAT 444 ユーザログ (ポートブロック割り当ておよび取り消しログを含む) 、NAT アラームログ、または NAT NO-PAT ログを有効にする前に、NAT ログを有効にする必要があります。

acl キーワードは、NAT セッションログに対してだけ有効です。ACL が指定されている場合、許可ルールに一致するフローが NAT セッションログをトリガーすることがあります。ACL を指定しない場合、NAT によって処理されるすべてのフローが NAT セッションログをトリガーする可能性があります。

例

#NAT ログを有効にします。

<AC> system-view

[AC] nat log enable

関連コマンド

- **display nat all**
- **display nat log**
- **nat log alarm**
- **nat log flow-active**
- **nat log flow-begin**
- **nat log flow-end**
- **nat log port-block-assign**
- **nat log port-block-withdraw**

13.1.32 nat log flow-active

Syntax

nat log flow-active *time-value*

undo nat log flow-active

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

time-value: アクティブ NAT フローのログ間隔を 10~120 分の範囲で指定します。

説明

nat log flow-active コマンドは、アクティブな NAT フローのログを有効にし、ログ間隔を設定します。

undo nat log flow-active コマンドはアクティブな NAT フローのログを無効にします。

アクティブ NAT フローは、長時間続く NAT セッションです。ログ機能は、アクティブな NAT フローを定期的にログすることで、アクティブな NAT フローを追跡するのに役立ちます。

アクティブ NAT フローのログが有効になるのは、NAT ログを有効にした場合だけです。

例

#アクティブな NAT フローのログを有効にし、ログ間隔を 10 分に設定します。

<AC> system-view

[AC] nat log flow-active 10

関連コマンド

- **display nat all**
- **display nat log**
- **nat log enable**

13.1.33 nat log flow-begin

Syntax

nat log flow-begin

undo nat log flow-begin

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

nat log flow-begin コマンドは NAT セッション確立イベントのログを有効にします。

undo nat log flow-begin コマンドは NAT セッション確立イベントのログを無効にします。

NAT セッション確立イベントのログは、NAT ログを有効にした後にだけ有効になります。

例

#NAT セッション確立イベントのログを有効にします。

<AC> system-view

[AC] nat log flow-begin

関連コマンド

- **display nat all**
- **display nat log**
- **nat log enable**

13.1.34 nat log flow-end

Syntax

nat log flow-end

undo nat log flow-end

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

nat log flow-end コマンドは NAT セッション削除イベントのログを有効にします。

undo nat log flow-end コマンドは NAT セッション削除イベントのログを無効にします。

NAT セッション削除イベントのログは、NAT ログを有効にした後にだけ有効になります。

例

#NAT セッション削除イベントのログを有効にします。

<AC> system-view

[AC] nat log flow-end

関連コマンド

- **display nat all**
- **display nat log**
- **nat log enable**

13.1.35 nat log port-block usage threshold

Syntax

nat log port-block usage threshold *value*

undo nat log port-block usage threshold

デフォルト

90%

View

System view

定義済みユーザロール

network-admin

パラメータ

value: 40~100 の範囲のしきい値をパーセンテージで指定します。

説明

nat log port-block usage threshold コマンドはポートブロック使用率のしきい値を設定します。

undo nat log port-block usage threshold コマンドはデフォルトに戻します。

ポートブロックの使用率がしきい値を超えると、ログが生成されます。

例

#ポートブロックの使用率しきい値を 60%に設定します。

<AC> system-view

[AC] nat log port-block usage threshold 60

関連コマンド

- **display nat all**
- **display nat log**
- **nat log enable**

13.1.36 nat log port-block-assign

Syntax

nat log port-block-assign

undo nat log port-block-assign

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

nat log port-block-assign コマンドはポートブロック割り当ての NAT 444 ユーザログを有効にします。

undo nat log port-block-assign コマンドはポートブロック割り当ての NAT 444 ユーザログを無効にします。

スタティックポートブロックマッピングの場合、NAT 444 ゲートウェイは、プライベート IP アドレスからの最初の接続を変換するときにユーザログを生成します。

ダイナミックポートブロックマッピングの場合、NAT 444 ゲートウェイは、プライベート IP アドレスのポートブロックを割り当てまたは拡張するときにユーザログを生成します。

このコマンドは、nat log enable コマンドを使用して NAT ログを有効にした後にだけ有効になります。

例

#ポートブロック割り当ての NAT 444 ユーザログを有効にします。

<AC> system-view

[AC] nat log port-block-assign

関連コマンド

- **display nat all**
- **display nat log**
- **nat log enable**

13.1.37 nat log port-block-withdraw

Syntax

nat log port-block-withdraw

undo nat log port-block-withdraw

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

nat log port-block-withdraw コマンドはポートブロック取り消しの NAT 444 ユーザログを有効にします。

undo nat log port-block-withdraw コマンドはポートブロック取り消しの NAT 444 ユーザログを無効にします。

スタティックポートブロックマッピングの場合、NAT 444 ゲートウェイは、プライベート IP アドレスからのすべての接続が切断されると、ユーザログを生成します。

ダイナミックポートブロックマッピングの場合、次の条件がすべて満たされると、NAT 444 ゲートウェイはユーザログを生成します。

- プライベート IP アドレスに割り当てられたポートブロック (拡張ブロックを含む) は取り消されます。
- 対応するマッピングエントリが削除されます。

このコマンドは、nat log enable コマンドを使用して NAT ログを有効にした後にだけ有効になります。

例

#ポートブロック取り消しのための NAT 444 ユーザログを有効にします。

<AC> system-view

[AC] nat log port-block-withdraw

関連コマンド

- **display nat all**
- **display nat log**
- **nat log enable**

13.1.38 nat mapping-behavior endpoint-independent

Syntax

nat mapping-behavior endpoint-independent [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }]

undo nat mapping-behavior endpoint-independent

デフォルト

Address and Port-Dependent Mapping

View

System view

定義済みユーザロール

network-admin

パラメータ

acl: Endpoint-Independent Mapping の適用可能なスコープを定義する ACL を指定します。

ipv4-acl-number: 2000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、all を指定することはできません。

説明

nat mapping-behavior endpoint-independent コマンドは PAT に対して EMI（Endpoint-Independent Mapping）モードを指定します。

undo nat mapping-behavior endpoint-independent コマンドはデフォルトに戻します。

PAT では、次の NAT マッピングモードがサポートされています。

- Endpoint-Independent Mapping:同じ送信元およびポートから任意の宛先へのパケットに、同じ IP およびポートマッピング (EIM エントリ) を使用します。EIM では、変換された IP アドレスとポートを使用して、外部ホストから内部ホストにアクセスできます。異なる NAT ゲートウェイの背後にある内部ホストが相互にアクセスできるようにします。
- Address and Port-Dependent Mapping :同じ送信元 IP およびポートを持つパケットに対して、異なる宛先 IP アドレスおよびポートへの異なる IP およびポートマッピングを使用します。APDM では、内部ホストがすでに外部ホストにアクセスしている場合にのみ、外部ホストが内部ホストにアクセスできます。これは安全ですが、異なるNAT ゲートウェイの背後にある内部ホストが相互にアクセスすることはできません。

このコマンドは、送信 PAT だけで有効になります。Address and Port-Dependent Mapping は、受信 PAT に常に適用されます。

ACL を指定すると、Endpoint-Independent Mapping が ACL によって許可されたパケットに適用されます。ACL を指定しない場合、Endpoint-Independent Mapping はすべてのパケットに適用されます。

例

#アドレス変換用のすべてのパケットに、エンドポイントに依存しないマッピングモードを適用します。

<AC> system-view

[AC] nat mapping-behavior endpoint-independent

#FTP および HTTP パケットにはエンドポイントに依存しないマッピングモードを適用し、アドレス変換のために他のパケットにはアドレスおよびポート依存マッピングモードを適用します。

<AC> system-view

[AC] acl advanced 3000

[AC-acl-ipv4-adv-3000] rule permit tcp destination-port eq 80

[AC-acl-ipv4-adv-3000] rule permit tcp destination-port eq 21

[AC-acl-ipv4-adv-3000] quit

[AC] nat mapping-behavior endpoint-independent acl 3000

関連コマンド

nat outbound

display nat eim

13.1.39 nat outbound

Syntax

NO-PAT:

nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*] **address-group** { *group-id* | **name** *group-name* } **no-pat** [**reversible**] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*] [**counting**]

undo nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*]

PAT:

nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*] [**address-group** { *group-id* | **name** *group-name* }] [**port-preserved**] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** text] [**counting**]

undo nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*]

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ipv4-acl-number: ipv 4-acl-number:2000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、all を指定することはできません。

address-group: NAT のアドレスグループを指定します。アドレスグループを指定しない場合、インタフェースの IP アドレスが NAT アドレスとして使用されます。Easy IP が使用されている。

group-id: アドレスグループ ID を指定します。この引数の値の範囲は 0 から 65535 です。

name *group-name*: アドレスグループ名を指定します。1~63 文字で、大文字と小文字は区別されません。

no-pat: NO-PAT モードを使用します。このキーワードを指定しない場合は、PAT が使用されます。PAT では、TCP、UDP、および ICMP クエリーパケットだけがサポートされます。ICMP パケットの場合、送信元ポート番号として ICMP ID が使用されます。

reversible: 逆アドレス変換を有効にします。逆アドレス変換では、既存の NO-PAT エントリを使用して、外部ネットワークからアクティブに開始された接続の宛先アドレスを内部ネットワークに変換します。

port-preserved: PAT のポート番号を保持しようとします。このキーワードは、ダイナミック NAT ポートブロックマッピングでは有効になりません。

rule *rule-name*: ルールの名前を指定します。大文字と小文字が区別され、1~63 文字のストリングで指定します。バックスラッシュ (¥) 、スラッシュ (/) 、コロン (:) 、アスタリスク (*) 、疑問符 (?) 、左かぎかっこ (<) 、右かぎかっこ (>) 、縦棒 (|) 、引用符 (") 、またはアット記号 (@) です。このオプションを指定しない場合、規則に名前はありません。

priority *priority*: ルールのプライオリティを 0~2147483647 の範囲で指定します。値が小さいほど、優先順位が高くなります。このオプションを指定しない場合、同じタイプの NAT 規則の中で優先順位が最も低くなります。

disable: 送信ダイナミック NAT ルールを無効にします。このキーワードを指定しない場合、ルールは有効になります。

description *text*: 送信ダイナミック NAT ルールの説明を指定します。text 引数は、大文字と小文字を区別しない 1~63 文字の文字列です。

counting: NAT カウントを有効にします。アドレスマッピングを使用するフローの数がカウントされます。

説明

nat outbound コマンドは送信ダイナミック NAT 規則を設定します。

undo nat outbound コマンドは送信ダイナミック NAT 規則を削除します。

送信ダイナミック NAT は通常、外部ネットワークに接続されたインタフェースで設定されます。1 つのインタフェースに複数の送信ダイナミック NAT ルールを設定できます。

送信ダイナミック NAT は、次のモードをサポートします。

- PAT :IP アドレス変換とポート変換の両方を実行します。PAT モードでは、エンドポイントに依存しないマッピング動作が使用されている場合、外部ホストは内部ホストにアクティブにアクセスできます。
- NO-PAT :IP アドレス変換だけを実行します。reversible キーワードを指定した場合、NO-PAT モードでは、外部ホストが内部ホストにアクティブにアクセスできます。ACL が指定されている場合、リバースアドレス変換は ACL リバースマッチングで許可されたパケットだけに適用されます。ACL リバースマッチングは次のように機能します。
  - □ パケットの送信元 IP アドレス/ポートと ACL 内の宛先 IP アドレス/ポートを比較します。
  - □ 一致する NO-PAT エントリに従ってパケットの宛先 IP アドレスを変換し、変換された宛先 IP アドレス/ポートを ACL 内の送信元 IP アドレス/ポートと比較します。

ダイナミック NAT 444 は、NO-PAT モードをサポートしません。

NAT アドレスグループを指定する場合は、次の制約事項および注意事項に従ってください。

- アドレスグループは、nat inbound コマンドと nat outbound コマンドの両方で使用できません。
- nat outbound コマンドでは、PAT モードと NO-PAT モードの両方でアドレスグループを使用できません。
- NAT アドレスグループでポートブロックパラメータが指定されている場合、このコマンドはダイナミック NAT ポートブロックマッピングを設定します。ACL 許可ルールに一致するパケットは、ダイナミック NAT 444 によって処理されます。

ACL を指定する場合は、次の制約事項および注意事項に従ってください。

- ACL は、インタフェース上の 1 つの送信ダイナミック NAT ルールだけで使用できます。
- ACL を指定すると、NAT は ACL によって許可された送信パケットの送信元 IP アドレスをアドレスグループの IP アドレスに変換します。ACL を指定しない場合、NAT はすべてのパケットを変換します。
- インタフェースに ACL が設定されている送信ダイナミック NAT ルールは、ACL が設定されていないルールよりも優先されます。ACL ベースのダイナミック NAT ルー

ルが 2 つ設定されている場合、ACL 番号が大きい方のルールのプライオリティが高くなります。

同じプライオリティ値で設定された送信ダイナミック NAT ルールと ACL は、ルール内の ACL を使用して照合されます。

- 名前付き ACL を持つ NAT ルールは、名前なし ACL を持つ NAT ルールよりも優先順位が高くなります。
- 名前付き ACL を持つ NAT ルールは、ACL 名のアルファベット順に照合されます。
- 名前なし ACL を持つ NAT ルールは、ACL 番号の降順で照合されます。

例

#サブネット 10.110.10.0/24 からのパケットだけを通過させるには、ACL 2001 を設定します。

<AC> system-view

[AC] acl basic 2001

[AC-acl-ipv4-basic-2001] rule permit source 10.110.10.0 0.0.0.255

[AC-acl-ipv4-basic-2001] rule deny

[AC-acl-ipv4-basic-2001] quit

#アドレスグループ 1 を作成し、アドレス範囲 202.110.10.10~202.110.10.12 をグループに追加します。

[AC] nat address-group 1

[AC-address-group-1] address 202.110.10.10 202.110.10.12

[AC-address-group-1] quit

#インタフェース VLAN インタフェース 10 の送信ダイナミック PAT ルールを設定して、ACL 2001 で許可された送信パケットの送信元アドレスをアドレスグループ 1 のアドレスに変換します。

[AC] interface vlan-interface 10

[AC-Vlan-interface10] nat outbound 2001 address-group 1

[AC-Vlan-interface10] quit

#インタフェース VLAN インタフェース 10 で送信 NO-PAT ルールを設定して、ACL 2001 で許可された送信パケットの送信元アドレスをアドレスグループ 1 のアドレスに変換します。

[AC] interface vlan-interface 10

[AC-Vlan-interface10] nat outbound 2001 address-group 1 no-pat

[AC-Vlan-interface10] quit

#VLAN インタフェース 10 の IP アドレスを変換後のアドレスとして使用するには、Easy IP を有効にします。

[AC] interface Vlan-interface 10

[AC-Vlan-interface10] nat outbound 2001

[AC-Vlan-interface10] quit

#VLAN インタフェース 10 で送信 NO-PAT ルールを設定して、ACL 2001 で許可された送信パケットの送信元アドレスをアドレスグループ 1 のアドレスに変換します。逆アドレス変換を有効にします。

[AC] interface Vlan-interface 10

[AC-Vlan-interface10] nat outbound 2001 address-group 1 no-pat reversible

関連コマンド

- **display nat eim**
- **display nat outbound**
- **nat mapping-behavior**

13.1.40 nat outbound port-block-group

Syntax

nat outbound port-block-group *group-id* [**rule** *rule-name*] [**counting**]

undo nat outbound port-block-group *group-id*

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

group-id: ID によって NAT ポートブロックグループを指定します。この引数の値の範囲は 0 から 65535 です。

rule *rule-name*: ルールの名前を指定します。大文字と小文字が区別され、1~63 文字のストリングで指定します。バックスラッシュ (¥) 、スラッシュ (/) 、コロン (:) 、アスタリスク (*) 、疑問符 (?) 、左かぎかっこ (<) 、右かぎかっこ (>) 、縦棒 (|) 、引用符 (") 、またはアット記号 (@) です。このオプションを指定しない場合、規則に名前はありません。

counting: NAT カウントを有効にします。アドレスマッピングを使用するフローの数がカウントされます。

説明

nat outbound port-block-group コマンドはインタフェースにスタティックな送信ポートブロックマッピングルールを設定します。

undo nat outbound port-block-group コマンドはインタフェース上のスタティックな送信ポートブロックマッピングルールを削除します。

インタフェースでこのコマンドを設定すると、マッピングが自動的に計算され、マッピングのエントリが作成されます。プライベート IP アドレスがパブリックネットワークにアクセスすると、プライベート IP アドレスはマッピングされたパブリック IP アドレスに変換され、ポートは選択されたポートブロック内のポートに変換されます。

1 つのインタフェースに複数のポートブロックマッピングルールを設定できます。

例

#VLAN インタフェース 10 にスタティックな送信ポートブロックマッピングルールを設定し、ルール名を abc と指定します。

<AC> system-view

[AC] interface vlan-interface 10

[AC-Vlan-interface10] nat outbound port-block-group 1 rule abc

関連コマンド

- **display nat all**
- **display nat outbound port-block-group**
- **display nat port-block**
- **nat port-block-group**

13.1.41 nat outbound rule move

Syntax

nat outbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

View

Interface view

定義済みユーザロール

network-admin

パラメータ

nat-rule-name1: 移動する NAT ルールの名前を指定します。

after: ルール nat-rule-name 1 をルール nat-rule-name 2 の後の行 (参照ルールと呼ばれます) に移動します。参照規則の優先度の値は変更されません。移動されたルールの優先度の値は、参照ルールの優先度の値に 1 を加えた値と等しくなります。

before: ルール nat-rule-name 1 をルール nat-rule-name 2 の前の行に移動します。参照規則の優先度の値は変更されません。移動したルールの優先度値は、参照ルールの優先度値から 1 を引いた値と等しくなります。

nat-rule-name2: 移動する NAT 規則の参照規則として、NAT 規則の名前を指定します。

説明

nat outbound rule move コマンドは送信ダイナミック NAT ルールのプライオリティを変更します。

このコマンドは、名前付き送信ダイナミック NAT 規則にだけ適用できます。

ルールリストの前の方に表示されている NAT ルールは、パケットマッチングの優先順位が高くなります。

例

#送信ダイナミック NAT ルール abc を、ルール def の前の行に移動します。

<AC> system-view

[AC] interface vlan-interface 10

[AC-Vlan-interface10] nat outbound rule move abc before def

関連コマンド

nat outbound

13.1.42 nat port-block global-share enable

Syntax

nat port-block global-share enable

undo nat port-block global-share enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

nat port-block global-share enable コマンドはポートブロックのグローバル共有を有効にします。

undo nat port-block global-share enable コマンドはポートブロックのグローバル共有を無効にします。

複数のインタフェースにダイナミック NAT ポートブロックマッピングが設定されている場合、インタフェースは同じ IP アドレスからのパケットに対して異なるポートブロックマッピングを作成することがあります。このコマンドを使用すると、同じ IP アドレスからのパケットの変換に同じポートブロックマッピングを使用するようにインタフェースを設定できます。

例

#ポートブロックのグローバル共有を有効にします。

<AC> system-view

[AC] nat port-block global-share enable

関連コマンド

port-block

13.1.43 nat port-block-group

Syntax

nat port-block-group *group-id*

undo nat port-block-group *group-id*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id: NAT ポートブロックグループに ID を割り当てます。この引数の値の範囲は 0 から 65535 です。

説明

nat port-block-group コマンドは NAT ポートブロックグループを作成し、そのビューを移行するか、または既存の NAT ポートブロックグループのビューを移行します。

undo nat port-block-group コマンドは NAT ポートブロックグループを削除します。

NAT ポートブロックグループは、NAT 444 のスタティックポートブロックマッピングを実装するように設定されます。

NAT ポートブロックグループには、次の項目を設定する必要があります。

- 少なくとも 1 つのプライベート IP アドレス範囲 (local-ip-address コマンドを参照) 。
- 少なくとも 1 つのパブリック IP アドレス範囲 (global-ip-address コマンドを参照) 。
- ポート範囲 (port-range コマンドを参照) 。
- ポートブロックサイズ (block-size コマンドを参照) 。

システムは、ポートブロックグループ設定に従ってスタティックポートブロックマッピングを計算し、マッピングのエントリを作成します。

例

#NAT ポートブロックグループ 1 を作成します。

<AC>system-view

[AC]nat port-block-group 1

[AC-port-block-group-1]

関連コマンド

- **block-size**
- **display nat all**
- **display nat port-block-group**
- **global-ip-pool**
- **local-ip-address**
- **nat outbound port-block-group**
- **port-range**

13.1.44 nat server

Syntax

一般的な NAT サーバマッピング:

- 1 つもしくは存在しないパブリックポートでの単一パブリックアドレス:

nat server [**protocol** *pro-type*] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } [*global-port*] **inside** *local-address* [*local-port*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**reversible**] [**rule** *rule-name*] [**disable**] [**counting**]

undo nat server [**protocol** *pro-type*] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } [*global-port*]

- 連続するパブリックポートでの単一のパブリックアドレス:

nat server protocol *pro-type* **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } *global-port*1 *global-port*2 **inside** { { *local-address* | *local-address*1 *local-address*2 } *local-port* | *local-address local-port*1 *local-port*2 } [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*] [**disable**] [**counting**]

undo nat server protocol *pro-type* **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } *global-port*1 *global-port*2

- 1 つもしくは存在しないパブリックポートでの連続パブリックアドレス:

nat server protocol *pro-type* **global** *global-address*1 *global-address*2 [*global-port*] **inside** { *local-address* | *local-address*1 *local-address*2 } [*local-port*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*] [**disable**] [**counting**]

undo nat server protocol *pro-type* **global** *global-address*1 *global-address*2 [*global-port*]

- 単一パブリックポートでの連続パブリックアドレス:

nat server protocol *pro-type* **global** *global-address*1 *global-address*2 *global-port* **inside** *local-address local-port*1 *local-port*2 [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*] [**disable**] [**counting**]

undo nat server protocol *pro-type* **global** *global-address*1 *global-address*2 *global-port*

ロードシェアリング NAT サーバマッピング:

nat server protocol *pro-type* **global** { { *global-address* | **current-interface** | **interface** *interface-type interface-number* } { *global-port* | *global-port*1 *global-port*2 } | *global-address*1 *global-address*2 *global-port* } **inside server-group** *group-id* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*] [**disable**] [**counting**]

undo nat server protocol *pro-type* **global** { { *global-address* | **current-interface** | **interface** *interface-type interface-number* } { *global-port* | *global-port*1 *global-port*2 } | *global-address*1 *global-address*2 *global-port* }

ACL ベースの NAT サーバマッピング:

nat server global { *ipv4-acl-number* | **name** *ipv4-acl-name* } **inside** *local-address* [*local-port*] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*] [**counting**]

undo nat server global { *ipv4-acl-number* | **name** *ipv4-acl-name* }

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

protocol *pro-type*: プロトコルタイプを指定します。プロトコルが TCP または UDP の場合、NAT サーバはポート情報を使用して設定できます。プロトコルタイプを指定しない場合、コマンドはすべてのプロトコルのパケットに適用されます。プロトコルタイプの形式は、次のいずれかです。

- 1 から 255 までの数値。
- icmp、tcp、または udp のプロトコル名。

global: 内部サーバに関するパブリックネットワーク情報を指定します。

global-address: 内部サーバのパブリックアドレスを指定します。

*global-address*1 *global-address*2: 最大 1 万個のアドレスを含むことができるパブリック IP アドレス範囲を指定します。global-address 1 引数は開始アドレスを指定し、global address 2 引数は開始アドレスより大きい必要がある終了アドレスを指定します。

ipv4-acl-number: 2000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、all を指定することはできません。

current-interface: 現在のインタフェースで Easy IP を有効にします。インタフェースのプライマリ IP アドレスは、内部サーバのパブリックアドレスとして使用されます。

interface *interface-type interface-number*: タイプと番号で指定されたインタフェース上で Easy IP を有効にします。インタフェースのプライマリ IP アドレスは、内部サーバのパブリックアドレスとして使用されます。ループバックインタフェースだけがサポートされます。

*global-port*1 *global-port*2: 最大 1 万個のポートを含むことができるパブリックポート番号の範囲を指定します。global-port 1 引数は開始ポートを指定し、global-port 2 引数は開始ポートより大きい必要がある終了ポートを指定します。パブリックポート番号の形式は、次のいずれかです。

- 1 から 65535 までの数値。開始ポートと終了ポートの両方がこの形式をサポートします。
- プロトコル名。1 から 15 文字の文字列。たとえば、http や telnet などです。この形式をサポートするのは開始ポートだけです。

inside: 内部サーバに関するプライベートネットワーク情報を指定します。

*local-address*1 *local-address*2: プライベート IP アドレス範囲を指定します。local-address 1 引数には開始アドレスを指定し、local-address 2 引数には開始アドレスより大きい必要がある終了アドレスを指定します。範囲内のアドレスの数は、パブリックポート番号範囲内のポートの数と同じである必要があります。

local-port: プライベートポート番号を指定します。プライベートポート番号の形式は、次のいずれかです。

- FTP ポート 20 を除く 1~65535 の範囲の番号。
- プロトコル名。1 から 15 文字の文字列。たとえば、http や telnet などです。

global-port: パブリックポート番号を指定します。デフォルト値と値の範囲は、local-port 引数の値と同じです。

local-address: プライベート IP アドレスを指定します。

server-group *group-id*: 内部サーバが属する内部サーバグループを指定します。このパラメータを使用して、ロードシェアリング NAT サーバ機能が設定されます。group-id 引数には、内部サーバグループ ID を指定します。group-id 引数の値の範囲は 0~65535 です。

acl: ACL を指定します。ACL を指定した場合、マッピングを使用して変換できるのは、ACL によって許可されたパケットだけです。

ipv4-acl-number: 2000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、all を指定することはできません。

reversible: 逆アドレス変換を許可します。逆アドレス変換は、内部サーバによってアクティブに開始された外部ネットワークへの接続に適用されます。内部サーバのプライベート IP アドレスをパブリック IP アドレスに変換します。

rule *rule-name*: マッピングの名前を指定します。大文字と小文字が区別され、1~63 文字の文字列になります。バックスラッシュ (¥) 、スラッシュ (/) 、コロン (:) 、アスタリスク (*) 、疑問符 (?) 、左かぎかっこ (<) 、右かぎかっこ (>) 、縦棒 (|) 、引用符 (") 、またはアット記号 (@) です。このオプションを指定しない場合、マッピングに名前はありません。

priority *priority*: マッピングのプライオリティを 0~2147483647 の範囲で指定します。値が小さいほど、優先順位が高くなります。このオプションを指定しない場合、マッピングのプライオリティは同じタイプの NAT 規則の中で最も低くなります。

disable: NAT サーバマッピングを無効にします。このキーワードを指定しない場合、マッピングは有効になります。

description *text*: マッピングの説明を指定します。text 引数は、大文字と小文字を区別しない 1~63 文字の文字列です。

counting: NAT カウントを有効にします。アドレスマッピングを使用するフローの数がカウントされます。

説明

nat server コマンドは NAT サーバマッピング (NAT サーバルール) を作成します。

undo nat server コマンドは NAT サーバマッピング (NAT サーバルール)を削除します。

内部ネットワーク内のサーバ(Web、FTP、Telnet、POP 3、DNS サーバなど)が外部ユーザにサービスを提供できるように、NAT サーバマッピングを設定できます。

NAT サーバマッピングは通常、NAT デバイス上の外部ネットワークに接続されたインタフェースで設定されます。global-address 引数と global-port 引数を使用すると、外部ユーザは local-address と local-port にある内部サーバにアクセスできます。プロトコルタイプが udp (プロトコル番号 17) または tcp (プロトコル番号 6) でない場合、1 対 1 の IP アドレスマッピングだけを設定できます。次の表では、NAT サーバの外部ネットワークと内部ネットワーク間のアドレスとポートのマッピングについて説明します。

表 13-19 NAT サーバのアドレスとポートのマッピング

外部ネットワーク	内部ネットワーク
1つのパブリックアドレス	1つのプライベートアドレス
1つのパブリックアドレスと1つのパブリックポート番号	1つのプライベートアドレスと1つのプライベートポート番号
1つのパブリックアドレスとN個の連続したパブリックポート番号	• 1つのプライベートアドレスと1つのプライベートポート番号 • N個の連続したプライベートアドレスと1つのプライベートポート番号 • 1つのプライベートアドレスとN個の連続するプライベートポート番号
N個の連続したパブリックアドレス	• 1つのプライベートアドレス • N個の連続するプライベートアドレス
N個の連続したパブリックアドレスと1つのパブリックポート番号	• 1つのプライベートアドレスと1つのプライベートポート番号 • N個の連続したプライベートアドレスと1つのプライベートポート番号 • 1つのプライベートアドレスとN個の連続するプライベートポート番号
1つのパブリックアドレスと1つのパブリックポート番号	1つの内部サーバグループ
1つのパブリックアドレスとN個の連続したパブリックポート番号	
N個の連続したパブリックアドレスと1つのパブリックポート番号	
ACLに一致するパブリックアドレス	1つのプライベートアドレス
	1つのプライベートアドレスと1つのプライベートポート

プロトコルタイプ、パブリックアドレス、およびパブリックポート番号のマッピングは、インタフェース上の内部サーバで一意である必要があります。この制限は、Easy IP を使用する場合にも適用されます。NAT サーバマッピングの最大数は、指定されたパブリックポート範囲内のパブリックポートの数と同じです。

同じインタフェースを使用して、複数の NAT サーバマッピングに Easy IP を設定しないことを推奨します。

Easy IP で使用されるインタフェースの IP アドレスが変更され、Easy IP を使用しない NAT サーバマッピングの IP アドレスと競合する場合、Easy IP 設定は無効になります。競合する IP アドレスが別の IP アドレスに変更された場合、または Easy IP を使用しない NAT サーバマッピングが削除された場合、Easy IP 設定が有効になります。

負荷分散 NAT サーバマッピングを設定する場合は、内部サーバ上の同じサービスにアクセスするために、ユーザが同じパブリックアドレスとパブリックポートを使用していることを確認する必要があります。このため、次のマッピングの値 N が内部サーバグループのサーバ数以下であることを確認してください。

- 1 つのパブリックアドレスと N 個の連続するパブリックポート番号が、1 つの内部サーバグループにマッピングされます。
- N 個の連続するパブリックアドレスとパブリックポート番号が 1 つの内部サーバグループにマッピングされます。

同じプライオリティ値で設定された ACL ベースの NAT サーバマッピングは、ルールで ACL を使用して照合されます。

- 名前付き ACL を持つマッピングは、名前なし ACL を持つマッピングよりも優先順位が高くなります。
- 名前付き ACL を持つマッピングは、ACL 名のアルファベット順に一致します。
- 名前なし ACL を持つマッピングは、ACL 番号の降順で照合されます。

次の状況で内部サーバのコンフィグレーションロールバックを実行すると、ロールバックエラーのエラーメッセージが表示されます。

- カレントコンフィグレーションでは、NAT サーバマッピングの名前がシステムによって自動的に割り当てられます。
- 置換コンフィグレーションファイルに名前が存在しません。

カレントコンフィグレーションファイルと置換ファイルが比較され、不一致に関するエラーメッセージが表示されます。コンフィグレーションファイル内の NAT サーバマッピング設定が正常にインストールされたため、このエラーメッセージは無視できます。たとえば、NAT サーバマッピング設定は、カレントコンフィグレーションでは nat server global 112.1.1.1 inside 192.168.20.1、置換コンフィグレーションファイルでは nat server global 112.1.1.1 inside 192.168.20.1 rule ServerRule_num です。ロールバック操作の後、新しい NAT サーバ設定が正常にインストールされます。

例

#外部ユーザが内部 Web サーバ 10.110.10.10 から http://202.110.10.10:8080 にアクセスできるようにします。

<AC> system-view

[AC] interface vlan-interface 10

[AC-Vlan-interface10] nat server protocol tcp global 202.110.10.10 8080 inside 10.110.10.10 http

[AC-Vlan-interface10] quit

#ACL ベースの NAT サーバマッピングを設定して、サブネット 192.168.0.0/24 の IP アドレスを使用して 10.0.0.172 の内部サーバにアクセスできるようにします。

<AC> system-view

[AC] acl advanced 3000

[AC-acl-ipv4-adv-3000] rule 5 permit ip destination 192.168.0.0 0.0.0.255

[AC-acl-ipv4-adv-3000] quit

[AC] interface vlan-interface 10

[AC-Vlan-interface10] nat server global 3000 inside 10.0.0.172

関連コマンド

- **display nat all**
- **display nat server**
- **nat server-group**

13.1.45 nat server rule move

Syntax

nat server rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

View

Interface view

定義済みユーザロール

network-admin

パラメータ

nat-rule-name1: 移動する NAT ルールの名前を指定します。

after: ルール nat-rule-name 1 をルール nat-rule-name 2 の後の行 (参照ルールと呼ばれます) に移動します。参照規則の優先度の値は変更されません。移動されたルールの優先度の値は、参照ルールの優先度の値に 1 を加えた値と等しくなります。

before: ルール nat-rule-name 1 をルール nat-rule-name 2 の前の行に移動します。参照規則の優先度の値は変更されません。移動したルールの優先度値は、参照ルールの優先度値から 1 を引いた値と等しくなります。

nat-rule-name2: 移動する NAT 規則の参照規則として、NAT 規則の名前を指定します。

説明

nat server rule move コマンドは ACL ベースの NAT サーバルールのプライオリティを変更します。

このコマンドは、名前付き ACL ベースの NAT サーバルールにだけ適用できます。

ルールリストの前の方に表示されている NAT ルールは、パケットマッチングの優先順位が高くなります。

例

#ACL ベースの NAT サーバルール abc を、ACL ベースの NAT サーバルール def の前の行に移動します。

<AC> system-view

[AC] interface vlan-interface 10

[AC-Vlan-interface10] nat server rule move abc before def

関連コマンド

nat server

13.1.46 nat server-group

Syntax

nat server-group *group-id*

undo nat server-group *group-id*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id: 内部サーバグループに ID を割り当てます。この引数の値の範囲は 0 から 65535 です。

説明

nat server-group コマンドは内部サーバグループを作成してそのビューを移行するか、既存の内部サーバグループのビューを移行します。

undo nat server-group コマンドは内部サーバグループを削除します。

内部サーバグループには、inside ip コマンドで設定された複数のメンバーを含めることができます。

例

#内部サーバグループ 1 を作成します。

<AC> system-view

[AC] nat server-group 1

関連コマンド

- **display nat all**
- **display nat server-group**
- **inside ip**
- **nat server**

13.1.47 nat static enable

Syntax

nat static enable

undo nat static enable

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

説明

nat static enable コマンドはインタフェースでスタティック NAT を有効にします。

undo nat static enable コマンドはインタフェースでスタティック NAT を無効にします。

スタティック NAT マッピングがインタフェースで有効になるのは、そのインタフェースでスタティック NAT が有効になってからです。

例

#プライベート IP アドレス 192.168.1.1 とパブリック IP アドレス 2.2.2.2 の間の送信スタティック NAT マッピングを設定し、VLAN インタフェース 10 でスタティック NAT を有効にします。

<AC> system-view

[AC] nat static outbound 192.168.1.1 2.2.2.2

[AC] interface vlan-interface 10

[AC-Vlan-interface10] nat static enable

関連コマンド

- **display nat all**
- **display nat static**
- **nat static**
- **nat static net-to-net**

13.1.48 nat static inbound

Syntax

nat static inbound *global-ip local-ip* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**]

undo nat static inbound *global-ip local-ip*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

global-ip: パブリック IP アドレスを指定します。

local-ip: プライベート IP アドレスを指定します。

acl: 外部ネットワークにアクセスできる内部ホストを識別する ACL を指定します。

ipv4-acl-number: 2000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、all を指定することはできません。

reversible: 内部ネットワークからアクティブに開始された接続に対して、プライベート IP アドレスへの逆アドレス変換を有効にします。

rule *rule-name*: マッピングの名前を指定します。大文字と小文字が区別され、1~63 文字の文字列になります。バックスラッシュ (¥) 、スラッシュ (/) 、コロン (:) 、アスタリスク (*) 、疑問符 (?) 、左かぎかっこ (<) 、右かぎかっこ (>) 、縦棒 (|) 、引用符 (") 、またはアット記号 (@) です。このオプションを指定しない場合、マッピングに名前はありません。

priority *priority*: マッピングのプライオリティを 0~2147483647 の範囲で指定します。値が小さいほど、優先順位が高くなります。このオプションを指定しない場合、マッピングのプライオリティは同じタイプの NAT 規則の中で最も低くなります。

disable: 1 対 1 の受信スタティックマッピングを無効にします。このキーワードを指定しない場合、マッピングは有効になります。

counting: NAT カウントを有効にします。アドレスマッピングを使用するフローの数がカウントされます。

説明

nat static inbound コマンドは受信スタティック NAT の 1 対 1 マッピングを設定します。

undo nat static inbound コマンドは受信スタティック NAT の 1 対 1 マッピングを削除します。

外部ネットワークから内部ネットワークへのパケットの送信元 IP アドレスが global-ip と一致する場合、送信元 IP アドレスは local-ip に変換されます。内部ネットワークから外部ネットワークへのパケットの宛先 IP アドレスが local-ip と一致する場合、宛先 IP アドレスは global-ip に変換されます。

ACL を指定する場合は、次の制約事項および注意事項に従ってください。

- ACL を指定しない場合、すべての受信パケットの送信元アドレスとすべての送信パケットの宛先アドレスが変換されます。
- ACL を指定し、reversible キーワードを指定しない場合、ACL によって許可された受信パケットの送信元アドレスが変換されます。内部ネットワークからアクティブに開始された接続の宛先アドレスは、プライベート IP アドレスに変換されません。
- ACL と reversible キーワードの両方を指定すると、ACL によって許可された受信パケットの送信元アドレスが変換されます。内部ネットワークからプライベート IP アドレスへアクティブに開始された接続のパケットが ACL 逆マッチングによって許可される場合、宛先アドレスは変換されます。ACL リバースマッチングは次のように機能します。
  - パケットの送信元 IP アドレス/ポートと ACL 内の宛先 IP アドレス/ポートを比較します。
  - マッピングに従ってパケットの宛先 IP アドレスを変換し、変換された宛先 IP アドレス/ポートを ACL 内の送信元 IP アドレス/ポートと比較します。

スタティック NAT とダイナミック NAT の両方がインタフェースに設定されている場合、スタティック NAT はダイナミック NAT よりも優先されます。

nat static inbound コマンドと nat static inbound net-to-net コマンドを使用すると、複数のインバウンドスタティック NAT マッピングを設定できます。

同じプライオリティ値と ACL で設定されたインバウンドスタティック NAT の 1 対 1 マッピングは、マッピングの ACL を使用して照合されます。

- 名前付き ACL を持つマッピングは、名前なし ACL を持つマッピングよりも優先順位が高くなります。
- 名前付き ACL を持つマッピングは、ACL 名のアルファベット順に一致します。
- 名前なし ACL を持つマッピングは、ACL 番号の降順で照合されます。

例

#パブリック IP アドレス 2.2.2.2 とプライベート IP アドレス 192.168.1.1 の間のインバウンドスタティック NAT マッピングを設定します。

<AC> system-view

[AC] nat static inbound 2.2.2.2 192.168.1.1

関連コマンド

- **display nat all**
- **display nat static**
- **nat static enable**

13.1.49 nat static inbound net-to-net

Syntax

nat static inbound net-to-net *global-start-address global-end-address* **local** *local-network* { *mask-length* | *mask* } [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**]

undo nat static inbound net-to-net *global-start-address global-end-address* **local** *local-network* { *mask-length* | *mask* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

global-start-address global-end-address: 最大 255 個のアドレスを含むことができるパブリックアドレス範囲を指定します。global-end-address は global-start-address より小さくできません。同じ場合、パブリックアドレスは 1 つだけ指定されます。

local-network: プライベートネットワークアドレスを指定します。

mask-length: プライベートネットワークアドレスのマスク長を 8~31 の範囲で指定します。

mask: プライベートネットワークアドレスのマスクを指定します。

acl: 外部ネットワークにアクセスできる内部ホストを識別する ACL を指定します。

ipv4-acl-number: 2000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、all を指定することはできません。

reversible: 内部ネットワークからアクティブに開始された接続に対して、プライベート IP アドレスへの逆アドレス変換を有効にします。

rule *rule-name*: マッピングの名前を指定します。大文字と小文字が区別され、1~63 文字の文字列になります。バックスラッシュ (¥) 、スラッシュ (/) 、コロン (:) 、アスタリスク (*) 、疑問符 (?) 、左かぎかっこ (<) 、右かぎかっこ (>) 、縦棒 (|) 、引用符 (") 、またはアット記号 (@) です。このオプションを指定しない場合、マッピングに名前はありません。

priority *priority*: マッピングのプライオリティを 0~2147483647 の範囲で指定します。値が小さいほど、優先順位が高くなります。このオプションを指定しない場合、マッピングのプライオリティは同じタイプの NAT 規則の中で最も低くなります。

disable: net-to-net 受信スタティックマッピングを無効にします。このキーワードを指定しない場合、マッピングは有効になります。

counting: NAT カウントを有効にします。アドレスマッピングを使用するフローの数がカウントされます。

説明

nat static inbound net-to-net コマンドは受信スタティック NAT の net to net マッピングを設定します。

undo nat static inbound net-to-net コマンドは受信スタティック NAT の net to net マッピングを削除します。

開始アドレスと終了アドレスでパブリックネットワークを指定し、プライベートアドレスとマスクでプライベートネットワークを指定します。

外部ネットワークからのパケットの送信元アドレスがパブリックアドレス範囲と一致する場合、送信元アドレスはプライベートアドレス範囲内のプライベートアドレスに変換されます。内部ネットワークからのパケットの宛先アドレスがプライベートアドレス範囲と一致する場合、宛先アドレスはパブリックアドレス範囲内のパブリックアドレスに変換されます。

パブリック終了アドレスは、パブリック開始アドレスとプライベートネットワークマスクによって決定されるサブネット内の最大 IP アドレスより大きくすることはできません。たとえば、プライベートアドレスが 2.2.2.0 でマスクが 255.255.255.0、パブリック開始アドレスが 1.1.1.100 の場合、パブリック終了アドレスはサブネット 1.1.1.0/24 内で最大の IP アドレスである 1.1.1.255 より大きくすることはできません。

ACL を指定する場合は、次の制約事項および注意事項に従ってください。

- ACL を指定しない場合、すべての受信パケットの送信元アドレスとすべての送信パケットの宛先アドレスが変換されます。

- ACL を指定し、reversible キーワードを指定しない場合、ACL によって許可された受信パケットの送信元アドレスが変換されます。内部ネットワークからアクティブに開始された接続の宛先アドレスは、プライベート IP アドレスに変換されません。
- ACL と reversible キーワードの両方を指定すると、ACL によって許可された受信パケットの送信元アドレスが変換されます。内部ネットワークからプライベート IP アドレスへアクティブに開始された接続のパケットが ACL 逆マッチングによって許可される場合、宛先アドレスは変換されます。ACL リバースマッチングは次のように機能します。
  - □ パケットの送信元 IP アドレス/ポートと ACL 内の宛先 IP アドレス/ポートを比較します。
  - □ マッピングに従ってパケットの宛先 IP アドレスを変換し、変換された宛先 IP アドレス/ポートを ACL 内の送信元 IP アドレス/ポートと比較します。

スタティック NAT とダイナミック NAT の両方がインタフェースに設定されている場合、スタティック NAT はダイナミック NAT よりも優先されます。

nat static inbound コマンドと nat static inbound net-to-net コマンドを使用すると、複数のインバウンドスタティック NAT マッピングを設定できます。

同じプライオリティ値と ACL で設定されたインバウンドスタティック NAT のネット/ネットマッピングは、マッピングで ACL を使用して照合されます。

- 名前付き ACL を持つマッピングは、名前なし ACL を持つマッピングよりも優先順位が高くなります。
- 名前付き ACL を持つマッピングは、ACL 名のアルファベット順に一致します。
- 名前なし ACL を持つマッピングは、ACL 番号の降順で照合されます。

例

#パブリックネットワークアドレス 202.100.1.0/24 とプライベートネットワークアドレス 192.168.1.0/24 の間のインバウンドスタティック NAT を設定します。

<AC> system-view

[AC] nat static inbound net-to-net 202.100.1.1 202.100.1.255 local 192.168.1.0 24

関連コマンド

- **display nat all**
- **display nat static**
- **nat static enable**

13.1.50 nat static inbound rule move

Syntax

nat static inbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

View

System view

定義済みユーザロール

network-admin

パラメータ

nat-rule-name1: 移動する NAT ルールの名前を指定します。

after: ルール nat-rule-name 1 をルール nat-rule-name 2 の後の行 (参照ルールと呼ばれます) に移動します。参照規則の優先度の値は変更されません。移動されたルールの優先度の値は、参照ルールの優先度の値に 1 を加えた値と等しくなります。

before: ルール nat-rule-name 1 をルール nat-rule-name 2 の前の行に移動します。参照規則の優先度の値は変更されません。移動したルールの優先度値は、参照ルールの優先度値から 1 を引いた値と等しくなります。

nat-rule-name2: 移動する NAT 規則の参照規則として、NAT 規則の名前を指定します。

説明

nat static inbound rule move コマンドは 1 対 1 の受信スタティック NAT ルールのプライオリティを変更します。

このコマンドは、名前付き受信 1 対 1 スタティック NAT ルールにのみ適用されます。

ルールリストの前の方に表示されている NAT ルールは、パケットマッチングの優先順位が高くなります。

例

#インバウンド 1 対 1 スタティック NAT ルール abc を、インバウンド 1 対 1 スタティック NAT ルール def の前の行に移動します。

<AC> system-view

[AC] nat static inbound rule move abc before def

関連コマンド

nat static inbound

13.1.51 nat static outbound

Syntax

nat static outbound *local-ip global-ip* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**]

undo nat static outbound *local-ip global-ip*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

local-ip: プライベート IP アドレスを指定します。

global-ip: パブリック IP アドレスを指定します。

acl: 内部ホストがアクセスできる宛先 IP アドレスを定義する ACL を指定します。

ipv4-acl-number: 3000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、all を指定することはできません。

reversible: 外部ネットワークからアクティブに開始された接続の逆アドレス変換を、パブリック IP アドレスに有効にします。

rule *rule-name*: マッピングの名前を指定します。大文字と小文字が区別され、1~63 文字の文字列になります。バックスラッシュ (¥) 、スラッシュ (/) 、コロン (:) 、アスタリスク (*) 、疑問符 (?) 、左かぎかっこ (<) 、右かぎかっこ (>) 、縦棒 (|) 、引用符 (") 、またはアット記号 (@) です。このオプションを指定しない場合、マッピングに名前はありません。

priority *priority*: マッピングのプライオリティを 0~2147483647 の範囲で指定します。値が小さいほど、優先順位が高くなります。このオプションを指定しない場合、マッピングのプライオリティは同じタイプの NAT 規則の中で最も低くなります。

disable: 1 対 1 の送信スタティックマッピングを無効にします。このキーワードを指定しない場合、マッピングは有効になります。

counting: NAT カウントを有効にします。アドレスマッピングを使用するフローの数がカウントされます。

説明

nat static outbound コマンドは送信スタティック NAT の 1 対 1 マッピングを設定します。

undo nat static outbound コマンドは送信スタティック NAT の 1 対 1 マッピングを削除します。

送信パケットの送信元 IP アドレスが local-ip と一致する場合、IP アドレスは global-ip に変換されます。受信パケットの宛先 IP アドレスが global-ip と一致する場合、宛先 IP アドレスは local-ip に変換されます。

ACL を指定する場合は、次の制約事項および注意事項に従ってください。

- ACL を指定しない場合、すべての送信パケットの送信元アドレスとすべての受信パケットの宛先アドレスが変換されます。
- ACL を指定し、reversible キーワードを指定しない場合、ACL によって許可された送信パケットの送信元アドレスが変換されます。外部ネットワークからアクティブに開始された接続の宛先アドレスは、パブリック IP アドレスに変換されません。
- ACL と reversible キーワードの両方を指定すると、ACL によって許可された送信パケットの送信元アドレスが変換されます。外部ネットワークからパブリック IP アドレスに対してアクティブに開始された接続のパケットが ACL リバースマッチングによって許可される場合、宛先アドレスは変換されます。ACL リバースマッチングは次のように機能します。
  - パケットの送信元 IP アドレス/ポートと ACL 内の宛先 IP アドレス/ポートを比較します。
  - マッピングに従ってパケットの宛先 IP アドレスを変換し、変換された宛先 IP アドレス/ポートを ACL 内の送信元 IP アドレス/ポートと比較します。

スタティック NAT は、両方がインタフェースに設定されている場合、ダイナミック NAT よりも優先されます。

nat static outbound コマンドと nat static outbound net-to-net コマンドを使用すると、複数の送信スタティック NAT マッピングを設定できます。

同じプライオリティ値と ACL で設定された送信スタティック NAT の 1 対 1 マッピングは、マッピングの ACL を使用して照合されます。

- 名前付き ACL を持つマッピングは、名前なし ACL を持つマッピングよりも優先順位が高くなります。
- 名前付き ACL を持つマッピングは、ACL 名のアルファベット順に一致します。
- 名前なし ACL を持つマッピングは、ACL 番号の降順で照合されます。

例

#パブリック IP アドレス 2.2.2.2 とプライベート IP アドレス 192.168.1.1 の間の送信スタティック NAT マッピングを設定します。

<AC> system-view

[AC] nat static outbound 192.168.1.1 2.2.2.2

#外部へのスタティック NAT を設定し、内部ユーザ 192.168.1.1 がパブリック IP アドレス 2.2.2.2 を使用して外部ネットワーク 3.3.3.0/24 にアクセスできるようにします。

<AC> system-view

[AC] acl advanced 3001

[AC-acl-ipv4-adv-3001] rule permit ip destination 3.3.3.0 0.0.0.255

[AC-acl-ipv4-adv-3001] quit

[AC] nat static outbound 192.168.1.1 2.2.2.2 acl 3001

関連コマンド

- **display nat all**
- **display nat static**
- **nat static enable**

13.1.52 nat static outbound net-to-net

Syntax

nat static outbound net-to-net *local-start-address local-end-address* **global** *global-network* { *mask-length* | *mask* } [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**]

undo nat static outbound net-to-net *local-start-address local-end-address* **global** *global-network* { *mask-length* | *mask* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

local-start-address local-end-address: 最大 255 個のアドレスを含むことができるプライベートアドレス範囲を指定します。local-end-address は local-start-address より小さくできません。同じ場合は、プライベートアドレスを 1 つだけ指定します。

global-network: パブリックネットワークアドレスを指定します。

mask-length: パブリックネットワークアドレスのマスク長を 8~31 の範囲で指定します。

mask: パブリックネットワークアドレスのマスクを指定します。

acl: 内部ホストがアクセスできる宛先 IP アドレスを定義する ACL を指定します。

ipv4-acl-number: 2000~3999 の範囲で ACL 番号を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、all を指定することはできません。

reversible: 外部ネットワークからアクティブに開始された接続の逆アドレス変換を、パブリック IP アドレスに有効にします。

rule *rule-name*: マッピングの名前を指定します。大文字と小文字が区別され、1~63 文字の文字列になります。バックスラッシュ (¥) 、スラッシュ (/) 、コロン (:) 、アスタ

リスク (*) 、疑問符 (?) 、左かぎかっこ (<) 、右かぎかっこ (>) 、縦棒 (|) 、引用符 (") 、またはアット記号 (@) です。このオプションを指定しない場合、マッピングに名前はありません。

priority *priority*: マッピングのプライオリティを 0~2147483647 の範囲で指定します。値が小さいほど、優先順位が高くなります。このオプションを指定しない場合、マッピングのプライオリティは同じタイプの NAT 規則の中で最も低くなります。

disable: net-to-net 送信スタティックマッピングを無効にします。このキーワードを指定しない場合、マッピングは有効になります。

counting: NAT カウントを有効にします。アドレスマッピングを使用するフローの数がカウントされます。

説明

nat static outbound net-to-net コマンドは送信スタティック NAT の net-to-net マッピングを設定します。

undo nat static outbound net-to-net コマンドは送信スタティック NAT の net-to-net マッピングを削除します。

開始アドレスと終了アドレスでプライベートネットワークを指定し、パブリックアドレスとマスクでパブリックネットワークを指定します。

内部ネットワークからのパケットの送信元アドレスがプライベートアドレス範囲と一致する場合、送信元アドレスはパブリックアドレス範囲内のパブリックアドレスに変換されます。外部ネットワークからのパケットの宛先アドレスがパブリックアドレス範囲と一致する場合、宛先アドレスはプライベートアドレス範囲内のプライベートアドレスに変換されます。

プライベート終了アドレスは、プライベート開始アドレスとパブリックネットワークマスクによって決定されるサブネット内の最大 IP アドレスより大きくすることはできません。たとえば、パブリックアドレスは 2.2.2.0、マスクは 255.255.255.0、プライベート開始アドレスは 1.1.1.100 です。プライベートエンドアドレスは、サブネット 1.1.1.0/24 内で最大の IP アドレスである 1.1.1.255 を超えることはできません。

ACL を指定する場合は、次の制約事項および注意事項に従ってください。

- ACL を指定しない場合、すべての送信パケットの送信元アドレスとすべての受信パケットの宛先アドレスが変換されます。
- ACL を指定し、reversible キーワードを指定しない場合、ACL によって許可された送信パケットの送信元アドレスが変換されます。外部ネットワークからアクティブに開始された接続の宛先アドレスは、パブリック IP アドレスに変換されません。
- ACL と reversible キーワードの両方を指定すると、ACL によって許可された送信パケットの送信元アドレスが変換されます。外部ネットワークからパブリック IP アドレスに対してアクティブに開始された接続のパケットが ACL リバースマッチングによって許可される場合、宛先アドレスは変換されます。ACL リバースマッチングは次のように機能します。
  - パケットの送信元 IP アドレス/ポートと ACL 内の宛先 IP アドレス/ポートを比較します。

□ マッピングに従ってパケットの宛先 IP アドレスを変換し、変換された宛先 IP アドレス/ポートを ACL 内の送信元 IP アドレス/ポートと比較します。

スタティック NAT は、両方がインタフェースに設定されている場合、ダイナミック NAT よりも優先されます。

nat static outbound コマンドと nat static outbound net-to-net コマンドを使用すると、複数の送信スタティック NAT マッピングを設定できます。

同じプライオリティ値と ACL で設定された送信スタティック NAT のネット/ネットマッピングは、マッピングで ACL を使用して照合されます。

- 名前付き ACL を持つマッピングは、名前なし ACL を持つマッピングよりも優先順位が高くなります。
- 名前付き ACL を持つマッピングは、ACL 名のアルファベット順に一致します。
- 名前なし ACL を持つマッピングは、ACL 番号の降順で照合されます。

例

#プライベートネットワークアドレス 192.168.1.0/24 とパブリックネットワークアドレス 2.2.2.0/24 の間の送信スタティック NAT マッピングを設定します。

<AC> system-view

[AC] nat static outbound net-to-net 192.168.1.1 192.168.1.255 global 2.2.2.0 24

#送信スタティック NAT を設定します。サブネット 192.168.1.0/24 の内部ユーザが、サブネット 2.2.2.0/24 のパブリック IP アドレスを使用して外部サブネット 3.3.3.0/24 にアクセスできるようにします。

<AC> system-view

[AC] acl advanced 3001

[AC-acl-ipv4-adv-3001] rule permit ip destination 3.3.3.0 0.0.0.255

[AC-acl-ipv4-adv-3001] quit

[AC] nat static outbound net-to-net 192.168.1.1 192.168.1.255 global 2.2.2.0 24 acl 3001

関連コマンド

- **display nat all**
- **display nat static**
- **nat static enable**

13.1.53 nat static outbound rule move

Syntax

nat static outbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

View

System view

定義済みユーザロール

network-admin

パラメータ

nat-rule-name1: 移動する NAT ルールの名前を指定します。

after: ルール nat-rule-name 1 をルール nat-rule-name 2 の後の行 (参照ルールと呼ばれます) に移動します。参照規則の優先度の値は変更されません。移動されたルールの優先度の値は、参照ルールの優先度の値に 1 を加えた値と等しくなります。

before: ルール nat-rule-name 1 をルール nat-rule-name 2 の前の行に移動します。参照規則の優先度の値は変更されません。移動したルールの優先度値は、参照ルールの優先度値から 1 を引いた値と等しくなります。

nat-rule-name2: 移動する NAT 規則の参照規則として、NAT 規則の名前を指定します。

説明

nat static outbound rule move コマンドは送信 1 対 1 スタティック NAT ルールのプライオリティを変更します。

このコマンドは、名前付き送信 1 対 1 スタティック NAT ルールだけに適用されます。

ルールリストの前の方に表示されている NAT ルールは、パケットマッチングの優先順位が高くなります。

例

#送信 1 対 1 スタティック NAT ルール abc を、送信 1 対 1 スタティック NAT ルール def の前の行に移動します。

<AC> system-view

[AC] nat static outbound rule move abc before def

関連コマンド

nat static outbound

13.1.54 nat timestamp delete

Syntax

nat timestamp delete

undo nat timestamp delete

デフォルト

TCP SYN および SYN ACK パケットは、タイムスタンプを伝送します。

View

System view

定義済みユーザロール

network-admin

説明

nat timestamp delete コマンドは TCP SYN および SYN ACK パケットのタイムスタンプの削除を有効にします。

undo nat timestamp delete コマンドはデフォルト状態に戻します。

nat inbound または nat outbound を使用して PAT モードがインタフェースに設定され、tcp_timestamp および tcp_tw_recycle 関数が TCP サーバに設定されている場合、TCP 接続が確立されないことがあります。この問題を解決するには、tcp_tw_recycle 関数をシャットダウンするか、nat timestamp delete コマンドを設定します。

例

#パブリックネットワーク上の TCP SYN および SYN ACK パケットのタイムスタンプの削除を有効にします。

<AC> system-view

[AC] nat timestamp delete

関連コマンド

- **nat outbound**
- **nat inbound**

13.1.55 port-block

Syntax

port block block-size *block-size* [**extended-block-number** *extended-block-number*]

undo port block

デフォルト

設定なし

View

NAT address group view

定義済みユーザロール

network-admin

パラメータ

block-size *block-size*: ポートブロックサイズを指定します。block-size 引数の値の範囲は 1~65535 です。NAT アドレスグループでは、ポートブロックサイズをポート範囲内のポート数より大きくすることはできません。

extended-block-number *extended-block-number*: 拡張ポートブロックの数を 1~5 の範囲で指定します。プライベート IP アドレスがパブリックネットワークにアクセスし、選択されたポートブロック内のポートがすべて占有されている場合、NAT 444 ゲートウェイは、プライベート IP アドレスに対してポートブロックを 1 つずつ拡張します。

説明

port block コマンドは NAT アドレスグループのポートブロックパラメータを設定します。

undo port block コマンドはデフォルト状態に戻します。

ダイナミックポートブロックマッピングを設定するには、NAT アドレスグループにポートブロックパラメータが必要です。プライベート IP アドレスがパブリックネットワークへの接続を開始すると、NAT 444 ゲートウェイはパブリック IP アドレスとポートブロックを割り当て、マッピング用のエントリを作成します。プライベート IP アドレスからの後続の接続では、NAT 444 ゲートウェイはプライベート IP アドレスをマッピングされたパブリック IP アドレスに変換し、ポートを選択されたポートブロック内のポートに変換します。

例

#NAT アドレスグループ 2 のポートブロックサイズを 256 に、拡張ポートブロック数を 1 に設定します。

<AC> system-view

[AC] nat address-group 2

[AC-address-group-2] port-block block-size 256 extended-block-number 1

関連コマンド

nat address-group

13.1.56 port-range

Syntax

port-range *start-port-number end-port-number*

undo port-range

デフォルト

パブリック IP アドレスのポート範囲は 1~65535 です。

View

NAT address group view

定義済みユーザロール

network-admin

パラメータ

start-port-number end-port-number: ポート範囲の開始ポート番号と終了ポート番号を指定します。終了ポート番号は開始ポート番号より小さくできません。アプリケーションプロトコルの識別エラーを回避するに、開始ポート番号を 1024 以上に設定することを推奨します。

説明

port-range コマンドはパブリック IP アドレスのポート範囲を指定します。

undo port-range コマンドはデフォルト状態に戻します。

ポート範囲には、パブリック IP アドレスがアドレス変換に使用するすべてのポートを含める必要があります。

ポート範囲内のポート数は、ポートブロックサイズより小さくできません。

例

#NAT アドレスグループ 1 のポート範囲を 1024~65535 に指定します。

<AC> system-view

[AC] nat address-group 1

[AC-address-group-1] port-range 1024 65535

#NAT ポートブロックグループ 1 のポート範囲を 30001~65535 に指定します。

<AC> system-view

[AC] nat port-block-group 1

[AC-port-block-group-1] port-range 30001 65535

関連コマンド

- **nat address-group**
- **nat port-block-group**

13.1.57 reset nat count statistics

Syntax

reset nat count statistics { **all** | **dynamic** | **server** | **static** | **static-port-block** }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: NAT マッピングのすべてのカウント統計情報をクリアします。

dynamic: ダイナミック NAT マッピングのカウント統計情報をクリアします。

server: NAT サーバマッピングのカウント統計情報をクリアします。

static: スタティック NAT マッピングのカウント統計情報をクリアします。

static-port-block: NAT 444 マッピングのカウント統計情報をクリアします。

説明

reset nat count statistics コマンドは NAT カウント統計情報を削除します。

例

#スタティック NAT マッピングのすべてのカウント統計情報をクリアします。

<AC> reset nat count statistics all

関連コマンド

- **display nat inbound**
- **display nat outbound**
- **display nat outbound port-block-group**
- **display nat port-block**
- **display nat static**
- **display nat server**

13.1.58 reset nat session

Syntax

reset nat session

View

User view

定義済みユーザロール

network-admin

説明

reset nat session コマンドは NAT セッションを削除します。

NAT セッションをクリアすると、対応する NAT EIM テーブルと NO-PAT テーブルが同時にクリアされます。

例

すべての NAT セッションをクリアします。

<AC> reset nat session

関連コマンド

display nat session

QX-W2230AC アクセスコントローラ

コマンドマニュアル

6. ルーティングプロトコル

本マニュアルは以下に示す章で構成されています。

01-IP ルーティングの基本
02-スタティックルーティング

目次

このセクションのページは **6-x-x** です。

1 章 IP ルーティングの基本 1-1
1.1 IP ルーティングの概要設定コマンド 1-1
1.1.1 display ip routing-table 1-1
1.1.2 display ip routing-table acl 1-5
1.1.3 display ip routing-table ip-address 1-8
1.1.4 display ip routing-table prefix-list 1-10
1.1.5 display ip routing-table protocol 1-12
1.1.6 display ip routing-table statistics 1-14
1.1.7 reset ip routing-table statistics protocol 1-15

1章 IP ルーティングの基本

1.1 IPルーティングの概要設定コマンド

1.1.1 display ip routing-table

Syntax

display ip routing-table [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose: アクティブと非アクティブルートを含むルーティングテーブルの詳細情報を表示します。指定しない場合、アクティブルートの概要情報のみ表示します。

説明

display ip routing-table コマンドはルーティングテーブルの情報を表示します。

例

ルーティングテーブルのアクティブルートの概要情報を表示します。

<AC> display ip routing-table

```
Destinations : 12       Routes : 12

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
0.0.0.0/32          Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
192.168.1.0/24      Direct 0    0           192.168.1.40    Vlan11
192.168.1.0/32      Direct 0    0           192.168.1.40    Vlan11
192.168.1.40/32     Direct 0    0           127.0.0.1       InLoop0
192.168.1.255/32    Direct 0    0           192.168.1.40    Vlan11
224.0.0.0/4         Direct 0    0           0.0.0.0         NULL0
```

```
224.0.0.0/24        Direct 0    0           0.0.0.0        NULL0
255.255.255.255/32  Direct 0    0           127.0.0.1      InLoop0
```

表 1-1 コマンド出力

フィールド	説明
Destinations	宛先アドレスの数です。
Routes	ルート数です。
Destination/Mask	宛先アドレス/マスク長です。
Proto	ルートを指定したプロトコルです。
Pre	ルートの優先順位です。
Cost	ルートのコストです。
NextHop	ルートのネクストホップアドレスです。
Interface	ルートに従って転送されるパケットの出力インタフェースです。
Summary Count	ルート数です。

ルーティングテーブルのすべてのルートの詳細情報を表示します。

<AC> display ip routing-table verbose

```
Destinations : 13       Routes : 13

Destination: 0.0.0.0/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 08h34m37s
      Cost: 0             Preference: 0
     IpPre: N/A           QosLocalID: N/A
       Tag: 0                 State: Active NoAdv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0x2              OrigAs: 0
     NibID: 0x10000000         LastAs: 0
    AttrID: 0xffffffff       Neighbor: 0.0.0.0
     Flags: 0x1000c       OrigNextHop: 127.0.0.1
     Label: NULL          RealNextHop: 127.0.0.1
   BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid         Interface: InLoopBack0
```

```
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0         TrafficIndex: N/A
  Connector: N/A

Destination: 1.1.1.0/24
   Protocol: Static
 Process ID: 0
  SubProtID: 0x0                Age: 04h20m37s
       Cost: 0            Preference: 60
      IpPre: N/A          QosLocalID: N/A
        Tag: 0                State: Active Adv
  OrigTblID: 0x0            OrigVrf: default-vrf
    TableID: 0x2             OrigAs: 0
      NibID: 0x10000003       LastAs: 0
     AttrID: 0xffffffff      Neighbor: 0.0.0.0
      Flags: 0x1008c      OrigNextHop: 192.168.47.4
      Label: NULL         RealNextHop: 192.168.47.4
    BkLabel: NULL           BkNextHop: N/A
  Tunnel ID: Invalid        Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0         TrafficIndex: N/A
  Connector: N/A

...
```

表 1-2 コマンド出力

フィールド	説明
Destinations	宛先アドレスの数です。
Routes	ルート数です。
Destination	宛先アドレス/マスク長です。
Protocol	ルートを指定したプロトコルです。
SubProtID	ルーティングのサブプロトコルのIDです。
Age	ルーティングテーブルのルートが存在する時間です。
Cost	ルートのコストです。
Preference	ルートの優先順位です。
IpPre	IPプレシーデンスです。

フィールド	説明
QosLocalID	ローカルQoS IDです。
Tag	ルートタグです。
State	ルート状態です。 ● **Active**—アクティブなユニキャストルートです。 ● **Adv**—分配できるルートです。 ● **Inactive**—非アクティブルートです。 ● **NoAdv**—ルータが分配できないルートです。
OrigTblID	もとのルーティングテーブルIDです。
OrigVrf	ルートが所属しているもとのVPNインスタンスです。ルートがIPv4パブリックネットワークにある場合、**default-vrf**と表示します。
TableID	ルーティングテーブルのIDです。
OrigAs	もとのAS番号です。
NibID	ネクストホップのIDです。
LastAs	最新のAS番号です。
AttrID	属性IDです。
Neighbor	ルーティングプロトコルによって決定された隣接アドレスです。
Flags	ルートのフラグです。
OrigNextHop	ルートのネクストホップアドレスです。
RealNextHop	ルートの実際のネクストホップです。
BkLabel	バックアップラベルです。
BkNexthop	バックアップネクストホップです。
Interface	ルートに従って転送されるパケットの出力インタフェースです。
BkTunnel ID	バックアップトンネルIDです。
BkInterface	バックアップ出力インタフェースです。
FtnIndex	FTNエントリのインデックスです。

フィールド	説明
TrafficIndex	トラフィックのインデックスです。範囲は1～64です。 値が不正である場合、**N/A**と表示されます。
Connector	VPN IPv4ルートとともに、BGPピア間で交換されるBGP接続属性です。値はリモートPE装置のIPアドレスです。BGP接続属性はMD VPNで使用されます。BGP接続属性がサポートされていない場合、**N/A**と表示されます。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Summary Count	ルート数です。

1.1.2 display ip routing-table acl

Syntax

display ip routing-table acl *ipv4-acl-number* [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ipv4-acl-number: 標準 ACL を指定します。設定範囲は 2000～2999 です。

verbose: 標準 ACL によって許可されたすべてのルートの詳細情報を表示します。指定しない場合、標準 ACL によって許可されたアクティブルートの概要情報のみ表示します。

説明

display ip routing-table acl コマンドは指定された標準 ACL によって許可されたルートの情報を表示します。

指定された ACL が存在しない、あるいはルールが設定されていない場合、すべてのルートの情報を表示します。

例

標準 ACL 2000 を定義し、ルートのフィルタリングのルールを設定します。

<AC> system-view

[AC] acl basic 2000

[AC-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255

[AC-acl-ipv4-basic-2000] rule deny source any

標準 ACL 2000 によって許可されたアクティブルートの概要情報を表示します。

[AC-acl-basic-2000] display ip routing-table acl 2000

```
Summary count : 4

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
192.168.1.0/24      Direct 0    0           192.168.1.111   Vlan11
192.168.1.0/32      Direct 0    0           192.168.1.111   Vlan11
192.168.1.111/32    Direct 0    0           127.0.0.1       InLoop0
192.168.1.255/32    Direct 0    0           192.168.1.111   Vlan11
```

コマンド出力は表 1-1 を参照してください。

標準 ACL 2000 によって許可されたすべてのルートの詳細情報を表示します。

<AC> display ip routing-table acl 2000 verbose

```
Summary count : 4

Destination: 192.168.1.0/24
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x1                 Age: 04h20m37s
      Cost: 0             Preference: 0
     IpPre: N/A           QosLocalID: N/A
       Tag: 0                 State: Active Adv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0x2              OrigAs: 0
     NibID: 0x10000003         LastAs: 0
    AttrID: 0xffffffff       Neighbor: 0.0.0.0
     Flags: 0x10080       OrigNextHop: 192.168.1.111
     Label: NULL          RealNextHop: 192.168.1.111
   BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid         Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A

Destination: 192.168.1.0/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                 Age: 04h20m37s
      Cost: 0             Preference: 0
```

```
     IpPre: N/A           QosLocalID: N/A
       Tag: 0                State: Active NoAdv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0x2             OrigAs: 0
      NibID: 0x10000003       LastAs: 0
     AttrID: 0xffffffff      Neighbor: 0.0.0.0
      Flags: 0x1008c       OrigNextHop: 192.168.1.111
      Label: NULL         RealNextHop: 192.168.1.111
    BkLabel: NULL           BkNextHop: N/A
  Tunnel ID: Invalid         Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A

Destination: 192.168.1.111/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x1               Age: 04h20m37s
       Cost: 0             Preference: 0
     IpPre: N/A           QosLocalID: N/A
       Tag: 0                State: Active NoAdv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0x2             OrigAs: 0
      NibID: 0x10000000       LastAs: 0
     AttrID: 0xffffffff      Neighbor: 0.0.0.0
      Flags: 0x10004       OrigNextHop: 127.0.0.1
      Label: NULL         RealNextHop: 127.0.0.1
    BkLabel: NULL           BkNextHop: N/A
  Tunnel ID: Invalid         Interface: InLoopBack0
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A

Destination: 192.168.1.255/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0               Age: 04h20m37s
       Cost: 0             Preference: 0
     IpPre: N/A           QosLocalID: N/A
       Tag: 0                State: Active NoAdv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0x2             OrigAs: 0
      NibID: 0x10000003       LastAs: 0
```

```
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c       OrigNextHop: 192.168.1.111
      Label: NULL         RealNextHop: 192.168.1.111
    BkLabel: NULL           BkNextHop: N/A
  Tunnel ID: Invalid         Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A
```

コマンド出力は表 1-2 を参照してください。

1.1.3 display ip routing-table ip-address

Syntax

display ip routing-table *ip-address* [*mask-length* | *mask*] [**longer-match**] [**verbose**]

display ip routing-table *ip-address1* **to** *ip-address2* [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip-address: 宛先 IP アドレスを指定します。ドットで区切り、10 進数で指定します。

mask-length: マスク長を指定します。設定範囲は 0～32 です。

mask: IP アドレスマスクを指定します。ドットで区切り、10 進数で指定します。

longer-match: マスク長が最長のルートエントリを表示します。

ip-address1 **to** *ip-address2*: 宛先 IP アドレス範囲を指定します。

verbose: アクティブと非アクティブルートを含むルーティングテーブルの詳細情報を表示します。指定しない場合、アクティブルートの概要情報のみ表示します。

説明

display ip routing-table *ip-address* コマンドは指定した宛先アドレスのルート情報を表示します。

display ip routing-table *ip-address1* **to** *ip-address2* コマンドは宛先アドレス範囲のルート情報を表示します。

異なるパラメータを使用してコマンドを実行すると、異なる出力が得られます。

- **display ip routing-table** *ip-address*

- □ システムは、入力された宛先 IP アドレスと各アクティブルートエントリのサブネットマスクの AND 演算を行います。
- □ 各アクティブルートエントリの宛先 IP アドレスと対応するサブネットマスクの AND 演算を行います。

1 つのエントリに対する 2 つの演算結果が同じである場合、エントリが表示されます。

- **display ip routing-table** *ip-address mask*
  - □ システムは、入力された宛先 IP アドレスと入力されたサブネットマスクの AND 演算を行います。
  - □ 各アクティブルートエントリの宛先 IP アドレスと入力されたサブネットマスクの AND 演算を行います。

1 つのエントリに対する 2 つの演算結果が同じで、サブネットマスクが入力されたサブネットマスク以下の場合、このエントリが表示されます。

- **display ip routing-table** *ip-address* **longer-match**
  - □ システムは、入力された宛先 IP アドレスと各アクティブルートエントリのサブネットマスクの AND 演算を行います。
  - □ システムは、各アクティブルートエントリの宛先 IP アドレスと対応するサブネットマスクの AND 演算を行います。

複数のエントリに対する 2 つの演算結果が同じ場合、最もマスク長の長いエントリが表示されます。

- **display ip routing-table** *ip-address mask* **longer-match**
  - □ システムは、入力された宛先 IP アドレスと入力されたサブネットマスクの AND 演算を行います。
  - □ 各アクティブルートエントリの 宛先 IP アドレスと入力されたサブネットマスクの AND 演算を行います。

入力されたサブネットマスク以下のマスクを持つ複数のエントリに対する 2 つの演算結果が同じ場合、マスク長が最長のエントリが表示されます。

- **display ip routing-table** *ip-address1* **to** *ip-address2*

指定した範囲 *ip-address1*/32～*ip-address2*/32 の宛先アドレスのアクティブルートエントリを表示します。

例

宛先 IP アドレス 11.0.0.1 のルートエントリの概要情報を表示します。

<AC> display ip routing-table 11.0.0.1

```
Summary count : 3

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
11.0.0.0/8          Static 60   0           0.0.0.0         NULL0
11.0.0.0/16         Static 60   0           0.0.0.0         NULL0
11.0.0.0/24         Static 60   0           0.0.0.0         NULL0
```

宛先 IP アドレス 11.0.0.1 およびマスク長 20 のルートの概要情報を表示します。

<AC> display ip routing-table 11.0.0.1 20

```
Summary count : 2

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
11.0.0.0/8          Static 60   0           0.0.0.0         NULL0
11.0.0.0/16         Static 60   0           0.0.0.0         NULL0
```

宛先アドレス 11.0.0.1 のマスク長が最長のルートの概要情報を表示します。

<AC> display ip routing-table 11.0.0.1 longer-match

```
Summary count : 1

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
11.0.0.0/24         Static 60   0           0.0.0.0         NULL0
```

宛先アドレス 11.0.0.1、マスク長 20、マスク長が最長のルートの概要情報を表示します。

<AC> display ip routing-table 11.0.0.1 20 longer-match

```
Summary count : 1

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
11.0.0.0/16         Static 60   0           0.0.0.0         NULL0
```

宛先アドレス範囲 1.1.1.0～5.5.5.0 の宛先アドレスのルートの概要情報を表示します。

<AC> display ip routing-table 1.1.1.0 to 5.5.5.0

```
Summary count : 4

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
1.1.1.1/32          Direct 0    0           127.0.0.1       InLoop0
2.2.2.0/24          Direct 0    0           2.2.2.1         Vlan2
3.3.3.1/32          Direct 0    0           127.0.0.1       InLoop0
4.4.4.1/32          Direct 0    0           127.0.0.1       InLoop0
```

1.1.4 display ip routing-table prefix-list

Syntax

display ip routing-table prefix-list *prefix-list-name* [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

prefix-list-name: IP プレフィックスリストを指定します。設定範囲は 1～63 です。大文字、小文字を区別します。

verbose: IP プレフィックスリストによって許可されたすべてのルートの詳細情報を表示します。指定しない場合、IP プレフィックスリストによって許可されたアクティブルートの概要情報を表示します。

説明

display ip routing-table prefix-list コマンドはプレフィックスリストによって許可されたルートの情報を表示します。

指定した IP プレフィックスリストが存在しない場合、すべてのルートの情報を表示します。

例

ルート 1.1.1.0/24 を許可するプレフィックスリスト test を作成します。

<AC> system-view

[AC] ip prefix-list test permit 1.1.1.0 24

IP プレフィックスリストによって許可されたアクティブルートの概要情報を表示します。

[AC] display ip routing-table prefix-list test

```
Summary count : 1

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
1.1.1.0/24          Direct 0    0           1.1.1.2         Vlan11
```

コマンド出力は表 1-1 を参照してください。

IP プレフィックスリストによって許可されたすべてのルートの詳細情報を表示します。

[AC] display ip routing-table prefix-list test verbose

```
Summary count : 1

Destination: 1.1.1.0/24
  Protocol: Direct
```

```
 Process ID: 0
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                  State: Active Adv
 OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2               OrigAs: 0
      NibID: 0x10000003         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 1.1.1.2
      Label: NULL          RealNextHop: 1.1.1.2
    BkLabel: NULL            BkNextHop: N/A
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A
```

コマンド出力は表 1-2 を参照してください。

1.1.5 display ip routing-table protocol

Syntax

display ip routing-table protocol *protocol* [**inactive** | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

protocol: ルーティングプロトコルを指定します。

inactive: 非アクティブルートの情報を表示します。指定しない場合、アクティブルートと非アクティブルートの情報を表示します。

verbose: ルーティングテーブルの詳細情報を表示します。指定しない場合、ルーティングの概要情報を表示します。

説明

display ip routing-table protocol コマンドはプロトコルによって指定されたルートの情報を表示します。

例

ダイレクトルートの概要情報を表示します。

<AC> display ip routing-table protocol direct

```
Summary count : 9

Direct Routing Table Status : <Active>
Summary count : 9

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
0.0.0.0/32          Direct 0    0           127.0.0.1       InLoop0
2.2.2.0/24          Direct 0    0           2.2.2.1         Vlan2
2.2.2.0/32          Direct 0    0           2.2.2.1         Vlan2
2.2.2.2/32          Direct 0    0           127.0.0.1       InLoop0
2.2.2.255/32        Direct 0    0           2.2.2.1         Vlan2
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0

Direct Routing Table Status : <Inactive>
Summary count : 0
```

スタティックルートの概要情報を表示します。

<AC> display ip routing-table protocol static

```
Summary count : 1

Static Routing Table Status : <Active>
Summary count : 0

Static Routing Table Status : <Inactive>
Summary count : 1

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
1.2.3.0/24          Static 60   0           1.2.4.5         Vlan10
```

コマンド出力は表 1-1 を参照してください。

1.1.6 display ip routing-table statistics

Syntax

display ip routing-table statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ip routing-table statistics コマンドは IPv4 ルートの統計情報を表示します。

プロトコルによって指定されたすべてのルート、deleted と記載されたルート、アクティブルート数が含まれます。

例

パブリックネットワークの IPv4 ルートの統計情報を表示します。

<AC> display ip routing-table statistics

```
Total prefixes: 15       Active prefixes: 15

Proto      route      active     added      deleted
DIRECT     12         12         30         18
STATIC      3          3          5          2
RIP         0          0          0          0
OSPF        0          0          0          0
Total      15         15         35         20
```

表 1-3 コマンド出力

フィールド	説明
Proto	ルートを指定したプロトコルです。
route	プロトコルによって指定されたルート数です。
active	アクティブルート数です。
added	ルータが起動あるいはルーティングテーブルが最後に削除した後にルーティングテーブルに追加されたルート数です。
deleted	deletedと記載されたルート数です。一定期間後に削除されます。

フィールド	説明
Total	ルートの総数です。

1.1.7 reset ip routing-table statistics protocol

Syntax

reset ip routing-table statistics protocol { *protocol* | **all** }

View

User view

定義済みユーザロール

network-admin

パラメータ

protocol: ルーティングプロトコルのルートの統計情報を削除します。

all: すべての IPv4 ルーティングプロトコルのルートの統計情報を削除します。

説明

reset ip routing-table statistics protocol コマンドは IPv4 ルートの統計情報を削除します。

例

パブリックネットワークのすべての IPv4 ルートの統計情報を削除します。

<AC> reset ip routing-table statistics protocol all

目次

このセクションのページは **6-x-x** です。

2 章 スタティックルーティング 2-1
2.1 スタティックルーティング設定コマンド 2-1
2.1.1 delete static-routes all 2-1
2.1.2 ip route-static 2-2
2.1.3 ip route-static default-preference 2-3

2章 スタティックルーティング

2.1 スタティックルーティング設定コマンド

2.1.1 delete static-routes all

Syntax

delete static-routes all

View

System view

定義済みユーザロール

network-admin

説明

delete static-routes all コマンドはすべてのスタティックルートを削除します。

コマンドを実行すると、設定されているすべてのスタティックルートを削除する前に確認画面が表示されます。

1 つのスタティックルートを削除する場合、**undo ip route-static** コマンドを使用します。デフォルトルートを含むすべてのスタティックルートを削除する場合、**delete static-routes all** コマンドを使用します。

例

すべてのスタティックルートを削除します。

<AC> system-view

[AC] delete static-routes all

```
This will erase all IPv4 static routes and their configurations, you must
reconfigure all static routes.
Are you sure?[Y/N]:y
```

関連コマンド

ip route-static

2.1.2 ip route-static

Syntax

ip route-static *dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] [**tag** *tag-value*] [**description** *description-text*]

undo ip route-static { *dest-address* { *mask-length* | *mask* } [*interface-type interface-number* [*next-hop-address*] | *next-hop-address*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

dest-address: スタティックルートの宛先アドレスを指定します。ドットで区切り、10 進数で指定します。

mask-length: IP アドレスのマスク長を指定します。設定範囲は 0～32 です。

mask: IP アドレスのマスクを指定します。ドットで区切り、10 進数で指定します。

interface-type interface-number: 出力インタフェースのタイプと番号を指定します。詳細はオペレーションマニュアルのセクション 6 *ルーティングプロトコル“スタティックルーティング”* を参照してください。

next-hop-address: ネクストホップの IP アドレスを指定します。ドットで区切り、10 進数で指定します。詳細はオペレーションマニュアルのセクション 6 *ルーティングプロトコル “スタティックルーティング”* を参照してください。

permanent: 固定のスタティックルートを指定します。出力インタフェースがダウンしても、固定のスタティックルートはアクティブのままです。

track *track-entry-number*: 1～1024 の範囲の番号で指定されたトラックエントリにスタティックルートを紐付けます。Track に関する詳細はオペレーションマニュアルのセクション 10 *高可用性 “Track”* を参照してください。

preference *preference*: スタティックルートの優先順位を指定します。設定範囲は 1～255 です。デフォルトは 60 です。

tag *tag-value*: スタティックルートをマーキングするタグの値を設定します。設定範囲は 1～4294967295 です。デフォルトは 0 です。ルートのタグはルート制御に使用されます。

description *description-text*: スタティックルートの説明を設定します。設定範囲は 1～60 文字です。半角スペースのような記号を含むことができますがクエスチョンマーク(?)は含むことができません。

説明

ip route-static コマンドはスタティックルートを設定します。

undo ip route-static コマンドはスタティックルートを削除します。

宛先アドレスとマスクの両方が 0.0.0.0（あるいは 0）である場合、設定されたルートはデフォルトルートです。デフォルトルートはルーティングテーブルに一致するエントリがないパケットを転送するのに使用されます。

異なるルートの優先順位を設定するため、異なるルーティングポリシーを実装してください。たとえば、同一宛先の複数のルートの負荷分散を有効にする場合、ルートに同一の優先順位を割り当ててください。一方をバックアップルートとする場合、ルートに異なる優先順位を割り当ててください。

スタティックルートの出力インタフェースあるいはネクストホップアドレスを指定するとき、以下のガイドラインに従ってください。

- 出力インタフェースが Null 0 インタフェースである場合、ネクストホップアドレスは必要ありません。
- 出力インタフェースがポイント-ポイントインタフェースである場合、出力インタフェースのみを指定することができます。対向先のアドレスが変更してもルートの設定を変更する必要がありません。
- 出力インタフェースが複数のネクストホップを持つブロードキャストインタフェースである場合、ネクストホップアドレスを同時に指定してください。ブロードキャストインタフェースにはイーサネットインタフェースと VLAN インタフェースが含まれます。

例

宛先アドレスが 1.1.1.1/24、ネクストホップが 2.2.2.2、タグが 45、説明が for internet のスタティックルートを設定します。

<AC> system-view

[AC] ip route-static 1.1.1.1 24 2.2.2.2 tag 45 description for internet

2.1.3 ip route-static default-preference

Syntax

ip route-static default-preference *default-preference-value*

undo ip route-static default-preference

デフォルト

60

View

System view

定義済みユーザロール

network-admin

パラメータ

default-preference-value: スタティックルートのデフォルトの優先順位を設定します。設定範囲は 1～255 です。

説明

ip route-static default-preference コマンドはスタティックルートのデフォルトの優先順位を設定します。

undo ip route-static default-preference コマンドはデフォルトに戻します。

スタティックルートの優先順位を指定しない場合、デフォルトの優先順位が適用されます。

デフォルトの優先順位を再設定した場合、新しく追加されたスタティックルートが適用されます。

例

スタティックルートのデフォルトの優先順位を 120 に設定します。

<AC> system-view

[AC] ip route-static default-preference 120

QX-W2230AC アクセスコントローラ

コマンドマニュアル

7. IP マルチキャスト

本マニュアルは以下に示す章で構成されています。

01-IGMP スヌーピング

目次

このセクションのページは **7-x-x** です。

1 章 IGMP スヌーピング 1-1
1.1 IGMP スヌーピング設定コマンド 1-1
1.1.1 display igmp-snooping 1-1
1.1.2 display igmp-snooping group 1-3
1.1.3 display igmp-snooping router-port 1-5
1.1.4 display igmp-snooping static-group 1-6
1.1.5 display igmp-snooping static-router-port 1-8
1.1.6 display igmp-snooping statistics 1-9
1.1.7 display l2-multicast ip forwarding 1-11
1.1.8 display l2-multicast mac forwarding 1-12
1.1.9 dot1p-priority (IGMP-snooping view) 1-13
1.1.10 entry-limit (IGMP-snooping view) 1-14
1.1.11 fast-leave (IGMP-snooping view) 1-15
1.1.12 group-policy (IGMP-snooping view) 1-16
1.1.13 host-aging-time (IGMP-snooping view) 1-18
1.1.14 igmp-snooping 1-19
1.1.15 igmp-snooping dot1p-priority 1-20
1.1.16 igmp-snooping drop-unknown 1-21
1.1.17 igmp-snooping enable 1-22
1.1.18 igmp-snooping fast-leave 1-23
1.1.19 igmp-snooping general-query source-ip 1-24
1.1.20 igmp-snooping group-limit 1-25
1.1.21 igmp-snooping group-policy 1-26
1.1.22 igmp-snooping host-aging-time 1-27
1.1.23 igmp-snooping host-join 1-29
1.1.24 igmp-snooping last-member-query-interval 1-30
1.1.25 igmp-snooping leave source-ip 1-31
1.1.26 igmp-snooping max-response-time 1-32
1.1.27 igmp-snooping overflow-replace 1-33
1.1.28 igmp-snooping querier 1-35
1.1.29 igmp-snooping query-interval 1-35
1.1.30 igmp-snooping report source-ip 1-37
1.1.31 igmp-snooping router-aging-time 1-38
1.1.32 igmp-snooping special-query source-ip 1-39
1.1.33 igmp-snooping static-group 1-40
1.1.34 igmp-snooping static-router-port 1-41

1.1.35 igmp-snooping version 1-42
1.1.36 last-member-query-interval (IGMP-snooping view) 1-43
1.1.37 max-response-time (IGMP-snooping view) 1-44
1.1.38 overflow-replace (IGMP-snooping view) 1-45
1.1.39 report-aggregation (IGMP-snooping view) 1-46
1.1.40 reset igmp-snooping group 1-47
1.1.41 reset igmp-snooping router-port 1-48
1.1.42 reset igmp-snooping statistics 1-48
1.1.43 router-aging-time (IGMP-snooping view) 1-49

1章 IGMP スヌーピング

1.1 IGMPスヌーピング設定コマンド

1.1.1 display igmp-snooping

Syntax

display igmp-snooping [**global** | **vlan** *vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

global: グローバルの IGMP snooping の状態を表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

説明

display igmp-snooping コマンドは IGMP snooping の状態を表示します。

パラメータを指定しない場合、グローバルとすべての VLAN の IGMP snooping の状態を表示します。

例

グローバルとすべての VLAN の IGMP snooping の状態を表示します。

<AC> display igmp-snooping

```
IGMP snooping information: Global
 IGMP snooping: Enabled
 Drop-unknown: Disabled
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Report-aggregation: Enabled
 Dot1p-priority: --

IGMP snooping information: VLAN 1
```

```
 IGMP snooping: Enabled
 Drop-unknown: Disabled
 Version: 2
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Querier: Disabled
 Query-interval: 125s
 General-query source IP: 1.1.1.1
 Special-query source IP: 2.2.2.2
 Report source IP: 3.0.0.3
 Leave source IP: 1.0.0.1
 Dot1p-priority: 2

IGMP snooping information: VLAN 10
 IGMP snooping: Enabled
 Drop-unknown: Enabled
 Version: 3
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Querier: Disabled
 Query-interval: 125s
 General-query source IP: 1.1.1.1
 Special-query source IP: 2.2.2.2
 Report source IP: 3.0.0.3
 Leave source IP: 1.0.0.1
 Dot1p-priority: --
```

表 1-1 コマンド出力

フィールド	説明
IGMP snooping	IGMP snoopingの状態です。 • **Enabled**－有効です。 • **Disabled**－無効です。
Drop-unknown	未知のマルチキャストデータの廃棄機能の状態です。 • **Enabled**－有効です。 • **Disabled**－無効です。
Version	IGMP snoopingのバージョンです。

フィールド	説明
Host-aging-time	ダイナミックメンバポートのエージングタイマです。
Router-aging-time	ダイナミックルータポートのエージングタイマです。
Max-response-time	IGMP general クエリの最大応答時間です。
Last-member-query-interval	IGMP group-specific クエリの送信間隔です。
Report-aggregation	IGMP report抑制機能の状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Dot1p-priority	IGMPメッセージの802.1pプライオリティです。プライオリティが設定されていない場合、ハイフン（--）が表示されます。
Querier	IGMP snoopingクエリアの状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Query-interval	IGMP general クエリの間隔です。
General-query source IP	IGMP general クエリの送信元IPアドレスです。
Special-query source IP	IGMP group-specific クエリの送信元IPアドレスです。
Report source IP	IGMP reportsの送信元IPアドレスです。
Leave source IP	IGMP leaveメッセージの送信元IPアドレスです。

1.1.2 display igmp-snooping group

Syntax

display igmp-snooping group [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-address: マルチキャストグループの IP アドレスを指定します。設定範囲は 224.0.1.0～239.255.255.255 です。マルチキャストグループを指定しない場合、すべてのマルチキャストグループのダイナミック IGMP snooping グループエントリを表示します。

source-address: マルチキャストソースの IP アドレスを指定します。マルチキャストソースを指定しない場合、すべてのマルチキャストソースのダイナミック IGMP snooping グループエントリを表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のダイナミック IGMP snooping グループエントリを表示します。

verbose: ダイナミック IGMP snooping グループエントリに関する詳細情報を表示します。キーワードを指定しない場合、このコマンドはダイナミック IGMP snooping グループエントリに関する簡易情報を表示します。

説明

display igmp-snooping group コマンドはダイナミック IGMP snooping グループエントリを表示します。

例

VLAN 2 のダイナミック IGMP snooping グループエントリの詳細情報を表示します。

<AC> display igmp-snooping group vlan 2 verbose

```
Total 1 entries.

VLAN 2: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: local port
    FSM information: normal
    Host slots (0 in total):
    Host ports (1 in total):
      WLAN-BSS1/0/10                    (00:03:23)
```

表 1-2 コマンド出力

フィールド	説明
Total 1 entries	ダイナミックIGMP snoopingグループエントリの総数です。
VLAN 2: Total 1 entries	VLAN 2のダイナミックIGMP snoopingグループエントリの総数です。
(0.0.0.0, 224.1.1.1)	（S,G）エントリです。Sが**0.0.0.0**の場合、すべてのマルチキャストソースを示します。
Attribute	このフィールドは現在のソフトウェアバージョンではサポートされていません。 エントリ属性です。

フィールド	説明
	• **global port**—エントリにグローバルポートがあります。 • **local port**—エントリに指定された装置上のポートがあります。
FSM information	エントリの有限状態装置（Finite state machine）情報です。 • **delete**—エントリの属性が削除されています。 • **dummy**—エントリが新規で一時的なエントリです。 • **no info**—エントリが存在しません。 • **normal**—エントリが正しいエントリです。
Host slots (0 in total)	このフィールドは現在のソフトウェアバージョンではサポートされていません。 メンバIDとメンバ装置が指定されていないとき、指定されたメンバ装置、あるいはマスタ装置を除いたメンバ装置の総数です。
Host ports (1 in total)	メンバポートとメンバポートの総数です。
(00:03:23)	ダイナミックメンバポートの残りのエージングタイマです。

関連コマンド

reset igmp-snooping group

1.1.3 display igmp-snooping router-port

Syntax

display igmp-snooping router-port [**vlan** *vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のダイナミックルータポートの情報を表示します。

説明

display igmp-snooping router-port コマンドはダイナミックルータポートの情報を表示します。

例

VLAN 2 のダイナミックルータポートの情報を表示します。

<AC> display igmp-snooping router-port vlan 2

```
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    WLAN-BSS1/0/10                          (00:01:30)
    WLAN-BSS1/0/20                          (00:00:23)
```

表 1-3 コマンド出力

フィールド	説明
VLAN 2	VLAN IDです。
Router slots (0 in total)	このフィールドは現在のソフトウェアバージョンではサポートされていません。 メンバIDとメンバ装置が指定されていないとき、指定されたメンバ装置、あるいはマスタ装置を除いたメンバ装置の総数です。
Router ports (2 in total)	ダイナミックルータポートと、ダイナミックルータポートの総数です。
(00:01:30)	ダイナミックルータポートの残りのエージングタイマです。

関連コマンド

reset igmp-snooping router-port

1.1.4 display igmp-snooping static-group

Syntax

display igmp-snooping static-group [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-address: マルチキャストグループの IP アドレスを指定します。設定範囲は 224.0.1.0～239.255.255.255 です。マルチキャストグループを指定しない場合、すべてのマルチキャストグループのスタティック IGMP snooping グループエントリを表示します。

source-address: マルチキャストソースの IP アドレスを指定します。マルチキャストソースを指定しない場合、すべてのマルチキャストソースのスタティック IGMP snooping グループエントリを表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のスタティック IGMP snooping グループエントリを表示します。

verbose: スタティック IGMP スヌーピンググループエントリに関する詳細情報を表示します。キーワードを指定しない場合、このコマンドはスタティック IGMP スヌーピンググループエントリに関する簡易情報を表示します。

説明

display igmp-snooping static-group コマンドはスタティック IGMP snooping グループエントリを表示します。

例

VLAN 2 のスタティック IGMP snooping グループエントリの詳細情報を表示します。

<AC> display igmp-snooping static-group vlan 2 verbose

```
Total 1 entries.

VLAN 2: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: local port
    FSM information: normal
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/2
```

表 1-4 コマンド出力

フィールド	説明
Total 1 entries	スタティックIGMP snoopingグループエントリの総数です。
VLAN 2: Total 1 entries	VLAN 2のスタティックIGMP snoopingグループエントリの総数です。

フィールド	説明
(0.0.0.0, 224.1.1.1)	（S,G）エントリです。Sが**0.0.0.0**の場合、すべてのマルチキャストソースを示します。
Attribute	このフィールドは現在のソフトウェアバージョンではサポートされていません。 エントリ属性です。 ● **global port**—エントリにグローバルポートがあります。 ● **local port**—エントリに指定された装置上のポートがあります。
FSM information	エントリの有限状態装置（Finite state machine）情報です。 ● **delete**—エントリの属性が削除されています。 ● **dummy**—エントリが新規で一時的なエントリです。 ● **no info**—エントリが存在しません。 ● **normal**—エントリが正しいエントリです。
Host slots (0 in total)	このフィールドは現在のソフトウェアバージョンではサポートされていません。 メンバIDとメンバ装置が指定されていないとき、指定されたメンバ装置、あるいはマスタ装置を除いたメンバ装置の総数です。
Host ports (1 in total)	メンバポートとメンバポートの総数です。

1.1.5 display igmp-snooping static-router-port

Syntax

display igmp-snooping static-router-port [**vlan** *vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

説明

display igmp-snooping static-router-port コマンドはスタティックルータポートの情報を表示します。

例

VLAN 2 のスタティックルータポートの情報を表示します。

<AC> display igmp-snooping static-router-port vlan 2

```
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    GE1/0/1
    GE1/0/2
```

表 1-5 コマンド出力

フィールド	説明
VLAN 2	VLAN IDです。
Router slots (0 in total)	このフィールドは現在のソフトウェアバージョンではサポートされていません。 メンバIDとメンバ装置が指定されていないとき、指定されたメンバ装置、あるいはマスタ装置を除いたメンバ装置の総数です。
Router ports (2 in total)	スタティックルータポートとスタティックルータポートの総数です。

1.1.6 display igmp-snooping statistics

Syntax

display igmp-snooping statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display igmp-snooping statistics コマンドは IGMP snooping によって学習した IGMP メッセージと PIMv2 hello メッセージの統計情報を表示します。

例

IGMP snooping によって学習した IGMP メッセージと PIMv2 hello メッセージの統計情報を表示します。

<AC> display igmp-snooping statistics

```
Received IGMP general queries:  0
Received IGMPv1 reports:  0
Received IGMPv2 reports:  19
Received IGMP leaves:  0
Received IGMPv2 specific queries:  0
Sent    IGMPv2 specific queries:  0
Received IGMPv3 reports:  1
Received IGMPv3 reports with right and wrong records:  0
Received IGMPv3 specific queries:  0
Received IGMPv3 specific sg queries:  0
Sent    IGMPv3 specific queries:  0
Sent    IGMPv3 specific sg queries:  0
Received PIMv2 hello:  0
Received error IGMP messages:  19
```

表 1-6 コマンド出力

フィールド	説明
general queries	IGMP general クエリの数です。
specific queries	IGMP group-specific クエリの数です。
reports	IGMP reportの数です。
leaves	IGMP leaveメッセージの数です。
reports with right and wrong records	正常な記録、正常でない記録のIGMP reportの数です。
specific sg queries	IGMP group-and-source-specific クエリの数です。
PIMv2 hello	PIMv2 helloメッセージの数です。
error IGMP messages	エラーがあるIGMPメッセージの数です。

関連コマンド

reset igmp-snooping statistics

1.1.7 display l2-multicast ip forwarding

Syntax

display l2-multicast ip forwarding [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group *group-address*: マルチキャストグループの IP アドレスを指定します。マルチキャストグループを指定しない場合、すべてのマルチキャストグループのレイヤ 2 マルチキャストグループエントリを表示します。

source *source-address*: マルチキャストソースの IP アドレスを指定します。マルチキャストソースを指定しない場合、すべてのマルチキャストソースのレイヤ 2 IP マルチキャストグループエントリを表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のレイヤ 2 IP マルチキャストグループエントリを表示します。

説明

display l2-multicast ip forwarding コマンドはレイヤ 2 IP マルチキャストグループエントリを表示します。

例

VLAN 2 のレイヤ 2 IP マルチキャストグループエントリを表示します。

<AC> display l2-multicast ip forwarding vlan 2

```
Total 1 entries.

VLAN 2: Total 1 IP entries.
  (0.0.0.0, 224.1.1.1)
    Host slots (0 in total):
    Host ports (3 in total):
      GE1/0/1
      GE1/0/2
      GE1/0/3
```

表 1-7 コマンド出力

フィールド	説明
Total 1 entries	レイヤ2 IPマルチキャストグループエントリエントリの総数です。
VLAN 2: Total 1 IP entries	VLAN 2のレイヤ2 IPマルチキャストグループエントリの総数です。
(0.0.0.0, 224.1.1.1)	（S,G）エントリです。Sが**0.0.0.0**の場合、すべてのマルチキャストソースを示します。
Host ports (0 in total)	このフィールドは現在のソフトウェアバージョンではサポートされていません。 メンバIDとメンバポートをもつメンバ装置の総数です。メンバ装置が指定されていないとき、指定されたメンバ装置とマスタ装置は除きます。
Host ports (3 in total)	メンバポートとメンバポートの総数です。

1.1.8 display l2-multicast mac forwarding

Syntax

display l2-multicast mac forwarding [*mac-address*] [**vlan** *vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address: MAC アドレスで MAC マルチキャストグループを指定します。指定しない場合、すべての MAC マルチキャストグループのレイヤ 2 MAC マルチキャストグループエントリを表示します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のレイヤ 2 MAC マルチキャストグループエントリを表示します。

説明

display l2-multicast mac forwarding コマンドはレイヤ 2 MAC マルチキャストグループエントリを表示します。

例

VLAN 2 のレイヤ 2 MAC マルチキャストグループエントリを表示します。

<AC> display l2-multicast mac forwarding vlan 2

```
Total 1 MAC entries.

VLAN 2: Total 1 MAC entries.
  MAC group address: 0100-5e01-0101
    Host slots (0 in total):
    Host ports (3 in total):
      GE1/0/1
      GE1/0/2
      GE1/0/3
```

表 1-8 コマンド出力

フィールド	説明
Total 1 entries	レイヤ2 MACマルチキャストグループエントリの総数です。
VLAN 2: Total 1 entries	VLAN 2のレイヤ2 MACマルチキャストグループエントリの総数です。
MAC group address	MACマルチキャストグループのアドレスです。
Host ports (0 in total)	このフィールドは現在のソフトウェアバージョンではサポートされていません。 メンバIDとメンバポートをもつメンバ装置の総数です。メンバ装置が指定されていないとき、指定されたメンバ装置とマスタ装置は除きます。
Host ports (3 in total)	メンバポートとメンバポートの総数です。

1.1.9 dot1p-priority (IGMP-snooping view)

Syntax

dot1p-priority *priority-number*

undo dot1p-priority

デフォルト

IGMP メッセージの 802.1p 優先度はデフォルトで設定されていません。

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

priority: IGMP メッセージの 802.1p 優先度を指定します。設定範囲は 0～7 です。値が高いほど優先度が高くなります。

説明

dot1p-priority コマンドはグローバルで IGMP メッセージの 802.1p 優先度を設定します。

undo dot1p-priority コマンドはデフォルトに戻します。

このコマンドは **igmp-snooping dot1p-priority** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **dot1p-priority** コマンドはすべての VLAN に適用されます。
- **igmp-snooping dot1p-priority** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping dot1p-priority** コマンドは IGMP-snooping view の **dot1p-priority** コマンドより優先されます。

例

IGMP メッセージの 802.1p 優先度を 3 に設定します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] dot1p-priority 3

関連コマンド

igmp-snooping dot1p-priority

1.1.10 entry-limit (IGMP-snooping view)

Syntax

entry-limit *limit*

undo entry-limit

デフォルト

4294967295

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

limit: IGMP snooping グループエントリの最大数を指定します。設定範囲は 0～4294967295 です。

説明

entry-limit コマンドはグローバルでの IGMP snooping グループエントリの最大数を設定します。IGMP snooping グループエントリの最大数はダイナミックエントリとスタティックエントリを含みます。

undo entry-limit コマンドはデフォルトに戻します。

例

IGMP snooping グループエントリのグローバルの最大数を 512 に設定します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] entry-limit 512

1.1.11 fast-leave (IGMP-snooping view)

Syntax

fast-leave [**vlan** *vlan-list*]

undo fast-leave [**vlan** *vlan-list*]

デフォルト

無効

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、1 行のコマンドで 10 個まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

fast-leave コマンドはグローバルに fast-leave 処理機能を有効にします。

undo fast-leave コマンドはグローバルに fast-leave 処理機能を無効にします。

ポートが leave メッセージを受信したとき、装置はマルチキャストグループのグループエントリから迅速にポートを削除します。

このコマンドは **igmp-snooping fast-leave** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **fast-leave** コマンドはすべてのポートに適用されます。
- **igmp-snooping fast-leave** コマンドは現在のポートに適用されます。

ポートでは **igmp-snooping fast-leave** コマンドは IGMP-snooping view の **fast-leave** コマンドより優先されます。

例

VLAN 2 でグローバルに fast-leave 処理機能を有効にします。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] fast-leave vlan 2

関連コマンド

igmp-snooping fast-leave

1.1.12 group-policy (IGMP-snooping view)

Syntax

group-policy *acl-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

デフォルト

マルチキャストグループポリシーは設定されていません。受信ホストはすべてのマルチキャストグループに加入することができます。

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

acl-number: 標準 IPv4 ACL あるいは拡張 IPv4 ACL を指定します。設定範囲は 2000～3999 です。受信ホストは ACL が許可するマルチキャストグループのみ加入することができます。ACL が存在しない、あるいは ACL に正常なルールがないとき、受信ホストはマルチキャストグループに加入することができません。

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

group-policy コマンドは受信ホストが加入するマルチキャストグループを管理するため、グローバルでマルチキャストグループポリシーを設定します。

undo group-policy コマンドはグローバルのマルチキャストグループポリシーを削除します。

IPv4 ACL でルールを設定するとき、以下の制限とガイドラインに従ってください。

- 標準 IPv4 ACL の **source** *source-address source-wildcard* パラメータはマルチキャストグループアドレスを指定します。
- 拡張 IPv4 ACL の **source** *source-address source-wildcard* パラメータは IGMP report のマルチキャスト送信元アドレスを指定します。**destination** *dest-address dest-wildcard* パラメータはマルチキャストグループアドレスを指定します。

  以下の IGMP report に一致するように、マルチキャスト送信元アドレス **source** *source-address source-wildcard* を 0.0.0.0 に設定します。

  - IGMPv1、IGMPv2 の report
  - マルチキャスト送信元アドレスを送信しない IGMPv3 IS_EX、IGMPv3 TO_EX の report
- ACL ルールの **time-range** *time-range-name* パラメータ、**fragment** パラメータを除く他のオプションパラメータは無視します。

異なる VLAN のポートに異なる ACL のルールを設定することができます。同一 VLAN で複数の ACL を設定した場合、最後に行った ACL のルールが適用されます。

このコマンドは、ポートがダイナミックに参加したマルチキャストグループにのみ適用されます。

IGMP-snooping view のすべてのポートでグローバルにマルチキャストグループポリシーを設定することができます。また interface view のポートでマルチキャストグループポリシーを設定することができます。ポートでは **igmp-snooping group-policy** コマンドは IGMP-snooping view の **group-policy** コマンドより優先されます。

例

VLAN 2 のホストがマルチキャストグループ 225.1.1.1 のみ加入できるように VLAN 2 のマルチキャストグループポリシーをグローバルに設定します。

<AC> system-view

[AC] acl basic 2000

[AC-acl-ipv4-basic-2000] rule permit source 225.1.1.1 0

[AC-acl-ipv4-basic-2000] quit

[AC] igmp-snooping

[AC-igmp-snooping] group-policy 2000 vlan 2

関連コマンド

igmp-snooping group-policy

1.1.13 host-aging-time (IGMP-snooping view)

Syntax

host-aging-time *interval*

undo host-aging-time

デフォルト

260 秒

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

interval: ダイナミックメンバポートのエージングタイマを設定します。設定範囲は 1～8097894 秒です。

説明

host-aging-time コマンドはグローバルでダイナミックメンバポートのエージングタイマを設定します。

undo host-aging-time コマンドはデフォルトに戻します。

このコマンドは **igmp-snooping host-aging-time** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **host-aging-time** コマンドはすべての VLAN に適用されます。
- **igmp-snooping host-aging-time** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping host-aging-time** コマンドは IGMP-snooping view の **host-aging-time** コマンドより優先されます。

マルチキャストグループメンバを間違って削除しないようにするため、ダイナミックメンバポートのエージングタイマを、以下の式で計算された値よりも大きい値に設定してください。

[IGMP general クエリの間隔] ＋ [IGMP general クエリの最大応答時間]

ダイナミックメンバポートのエージングタイマを以下の式で計算した値に設定することを推奨します。

[IGMP general クエリの間隔] × 2 ＋ [IGMP general クエリの最大応答時間]

例

グローバルでダイナミックメンバポートのエージングタイマを 300 秒に設定します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] host-aging-time 300

関連コマンド

igmp-snooping host-aging-time

1.1.14 igmp-snooping

Syntax

igmp-snooping

undo igmp-snooping

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

igmp-snooping コマンドはグローバルで IGMP snooping を有効にし、IGMP-snooping view に移行します。

undo igmp-snooping コマンドはグローバルで IGMP snooping を無効にします。

例

グローバルで IGMP snooping を有効にし、IGMP-snooping view に移行します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping]

関連コマンド

igmp-snooping enable

1.1.15 igmp-snooping dot1p-priority

Syntax

igmp-snooping dot1p-priority *priority-number*

undo igmp-snooping dot1p-priority

デフォルト

IGMP メッセージの 802.1p 優先度はデフォルトで設定されていません。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

priority-number: IGMP メッセージの 802.1p 優先度を指定します。設定範囲は 0～7 です。値が高いほど優先度が高くなります。

説明

igmp-snooping dot1p-priority コマンドは VLAN の IGMP メッセージの 802.1p 優先度を設定します。

undo igmp-snooping dot1p-priority コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で IGMP snooping を有効にしてください。

このコマンドは **dot1p-priority** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **dot1p-priority** コマンドはすべての VLAN に適用されます。
- **igmp-snooping dot1p-priority** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping dot1p-priority** コマンドは IGMP-snooping view の **dot1p-priority** コマンドより優先されます。

例

VLAN 2 で IGMP snooping を有効にし、IGMP メッセージの 802.1p 優先度を 3 に設定します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] quit

[AC] vlan 2

[AC-vlan2] igmp-snooping enable

[AC-vlan2] igmp-snooping dot1p-priority 3

関連コマンド

- **dot1p-priority (IGMP-snooping view)**
- **igmp-snooping enable**

1.1.16 igmp-snooping drop-unknown

Syntax

igmp-snooping drop-unknown

undo igmp-snooping drop-unknown

デフォルト

VLAN の未知のマルチキャストデータの廃棄機能は無効です。未知のマルチキャストデータは VLAN にフラッディングされます。

View

VLAN view

定義済みユーザロール

network-admin

説明

igmp-snooping drop-unknown コマンドは VLAN の未知のマルチキャストデータの廃棄機能を有効にします。

undo igmp-snooping drop-unknown コマンドは VLAN の未知のマルチキャストデータの廃棄機能を無効にします。

このコマンドを実行する前に VLAN で IGMP snooping 機能を有効にしてください。

igmp-snooping drop-unknown コマンドと **drop-unknown** コマンドは互いに排他的です。同じ装置に設定することはできません。

例

IGMP snooping を有効にし、VLAN 2 の未知のマルチキャストデータの廃棄機能を有効にします。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] quit

[AC] vlan 2

[AC-vlan2] igmp-snooping enable

[AC-vlan2] igmp-snooping drop-unknown

関連コマンド

igmp-snooping enable

1.1.17 igmp-snooping enable

Syntax

igmp-snooping enable

undo igmp-snooping enable

デフォルト

無効

View

VLAN view

定義済みユーザロール

network-admin

説明

igmp-snooping enable コマンドは VLAN の IGMP snooping を有効にします。

undo igmp-snooping enable コマンドは VLAN の IGMP snooping を無効にします。

このコマンドを実行する前にグローバルで IGMP snooping 機能を有効にしてください。

VLAN view 内の VLAN もしくは、IGMP-snooping view で指定された VLAN に対して IGMP スヌーピングを有効にできます。VLAN view の設定は IGMP-snooping view の設定と同じ優先度を持ちます。最後に行われた設定が適用されます。

例

グローバルと VLAN 2 の IGMP snooping を有効にします。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] quit

[AC] vlan 2

[AC-vlan2] igmp-snooping enable

関連コマンド

igmp-snooping

1.1.18 igmp-snooping fast-leave

Syntax

igmp-snooping fast-leave [**vlan** *vlan-list*]

undo igmp-snooping fast-leave [**vlan** *vlan-list*]

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

igmp-snooping fast-leave コマンドはポートで fast-leave 処理機能を有効にします。

undo igmp-snooping fast-leave コマンドはポートで fast-leave 処理機能を無効にします。

この機能は、ポートが leave メッセージを受信したとき、装置がマルチキャストグループのグループエントリから迅速にポートを削除します。

このコマンドは IGMP-snooping view の **fast-leave** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **fast-leave** コマンドはすべてのポートに適用されます。
- **igmp-snooping fast-leave** コマンドは現在のポートに適用されます。

ポートでは **igmp-snooping fast-leave** コマンドは IGMP-snooping view の **fast-leave** コマンドより優先されます。

例

GigabitEthernet 1/0/1 の VLAN 2 で fast-leave 処理機能を有効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] igmp-snooping fast-leave vlan 2

関連コマンド

fast-leave (IGMP-snooping view)

1.1.19 igmp-snooping general-query source-ip

Syntax

igmp-snooping general-query source-ip *ip-address*

undo igmp-snooping general-query source-ip

デフォルト

IGMP general クエリの送信元 IP アドレスは現在の VLAN インタフェースの IP アドレスです。現在の VLAN インタフェースに IP アドレスがない場合、送信元 IP アドレスは 0.0.0.0 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ip-address: IGMP general クエリの送信元 IP アドレスを指定します。

説明

igmp-snooping general-query source-ip コマンドは IGMP general クエリの送信元 IP アドレスを設定します。

undo igmp-snooping general-query source-ip コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で IGMP snooping を有効にしてください。

例

VLAN 2 で IGMP snooping を有効にし、IGMP general クエリの送信元 IP アドレス 10.1.1.1 を設定します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] quit

[AC] vlan 2

[AC-vlan2] igmp-snooping enable

[AC-vlan2] igmp-snooping general-query source-ip 10.1.1.1

関連コマンド

igmp-snooping enable

1.1.20 igmp-snooping group-limit

Syntax

igmp-snooping group-limit *limit* [**vlan** *vlan-list*]

undo igmp-snooping group-limit [**vlan** *vlan-list*]

デフォルト

4294967295

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

limit: ポートが加入できるマルチキャストグループの最大数を設定します。設定範囲は 0～4294967295 です。

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

igmp-snooping group-limit コマンドはポートが加入できるマルチキャストグループの最大数を設定します。

undo igmp-snooping group-limit コマンドはデフォルトに戻します。

このコマンドはポートがダイナミックに加入するマルチキャストグループでのみ適用します。

例

VLAN 2 の GigabitEthernet 1/0/1 が加入できるマルチキャストグループの最大数を 10 に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] igmp-snooping group-limit 10 vlan 2

1.1.21 igmp-snooping group-policy

Syntax

igmp-snooping group-policy *acl-number* [**vlan** *vlan-list*]

undo igmp-snooping group-policy [**vlan** *vlan-list*]

デフォルト

ポートでマルチキャストグループポリシーは設定されていません。ポートに接続されたホストはすべてのマルチキャストグループに加入することができます。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

acl-number: 標準 IPv4 ACL あるいは拡張 IPv4 ACL を指定します。設定範囲は 2000～3999 です。受信ホストは ACL が許可するマルチキャストグループのみ加入することができます。ACL が存在しない、あるいは ACL に正常なルールがないとき、受信ホストはマルチキャストグループに加入することができません。

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

igmp-snooping group-policy コマンドは受信ホストが加入するマルチキャストグループを管理するため、ポートでマルチキャストグループポリシーを設定します。

undo igmp-snooping group-policy コマンドはポートのマルチキャストグループポリシーを削除します。

IPv4 ACL でルールを設定するとき、以下の制限とガイドラインに従ってください。

- 標準 IPv4 ACL の **source** *source-address source-wildcard* パラメータはマルチキャストグループアドレスを指定します。

- 拡張 IPv4 ACL の **source** *source-address source-wildcard* パラメータは IGMP report のマルチキャスト送信元アドレスを指定します。**destination** *dest-address dest-wildcard* パラメータはマルチキャストグループアドレスを指定します。

  以下の IGMP report に一致するように、マルチキャスト送信元アドレス **source** *source-address source-wildcard* を 0.0.0.0 に設定します。

  - IGMPv1、IGMPv2 の report
  - マルチキャスト送信元アドレスを送信しない IGMPv3 IS_EX、IGMPv3 TO_EX の report
- ACL ルールの **time-range** *time-range-name* パラメータ、**fragment** パラメータを除く他のオプションパラメータは無視します。

異なる VLAN のポートに異なる ACL のルールを設定することができます。同一 VLAN で複数の ACL を設定した場合、最後に行った ACL のルールが適用されます。

このコマンドはポートがダイナミックに加入するマルチキャストグループでのみ適用します。

IGMP-snooping view のすべてのポートでグローバルにマルチキャストグループポリシーを設定することができます。また interface view のポートでマルチキャストグループポリシーを設定することができます。ポートでは **igmp-snooping group-policy** コマンドは IGMP-snooping view の **group-policy** コマンドより優先されます。

例

ポートに接続されたホストがマルチキャストグループ 225.1.1.1 のみ加入できるように VLAN 2 の GigabitEthernet 1/0/1 でマルチキャストグループポリシーを設定します。

```
<AC> system-view
[AC] acl basic 2000
[AC-acl-ipv4-basic-2000] rule permit source 225.1.1.1 0
[AC-acl-ipv4-basic-2000] quit
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] igmp-snooping group-policy 2000 vlan 2
```

関連コマンド

group-policy (IGMP-snooping view)

1.1.22 igmp-snooping host-aging-time

Syntax

igmp-snooping host-aging-time *interval*

undo igmp-snooping host-aging-time

デフォルト

260 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

interval: VLAN のダイナミックメンバポートのエージングタイマを設定します。設定範囲は 1～8097894 秒です。

説明

igmp-snooping host-aging-time コマンドは VLAN のダイナミックメンバポートのエージングタイマを設定します。

undo igmp-snooping host-aging-time コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で IGMP snooping 機能を有効にしてください。

マルチキャストグループメンバを間違って削除しないようにするため、ダイナミックメンバポートのエージングタイマを、以下の式で計算された値よりも大きい値に設定してください。

[IGMP general クエリの間隔] ＋ [IGMP general クエリの最大応答時間]

ダイナミックメンバポートのエージングタイマを以下の式で計算した値に設定することを推奨します。

[IGMP general クエリの間隔] × 2 ＋ [IGMP general クエリの最大応答時間]

このコマンドは **host-aging-time** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **host-aging-time** コマンドはすべての VLAN に適用されます。
- **igmp-snooping host-aging-time** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping host-aging-time** コマンドは IGMP-snooping view の **host-aging-time** コマンドより優先されます。

例

VLAN 2 の IGMP snooping を有効にし、VLAN のダイナミックメンバポートのエージングタイマを 300 秒に設定します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] quit

[AC] vlan 2

[AC-vlan2] igmp-snooping enable

[AC-vlan2] igmp-snooping host-aging-time 300

関連コマンド

- **host-aging-time (IGMP-snooping view)**
- **igmp-snooping enable**

1.1.23 igmp-snooping host-join

Syntax

igmp-snooping host-join *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

undo igmp-snooping host-join { *group-address* [**source-ip** *source-address*] **vlan** *vlan-id* | **all** }

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

group-address: マルチキャストグループの IP アドレスを指定します。設定範囲は 224.0.1.0～239.255.255.255 です。

source-ip *source-address*: マルチキャストソースの IP アドレスを指定します。マルチキャストソースを指定した場合、ポートをマルチキャストソースとグループのシミュレーティッドメンバホストとして設定します。マルチキャストソースを指定しない場合、マルチキャストグループのポートをシミュレーティッドメンバホストとして設定します。このパラメータは IGMPv3 snooping が動作する装置で有効です。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

all: すべてのマルチキャストグループを指定します。

説明

igmp-snooping host-join コマンドはポートをマルチキャストグループのシミュレーティッドメンバホストとして設定します。

undo igmp-snooping host-join コマンドはシミュレーティッドメンバホストの設定を削除します。

IGMP version と、シミュレーティッドメンバホストが動作する IGMP snooping のバージョンは同一にしてください。スタティックメンバポートと異なり、シミュレーティッドメンバホストとして設定されたポートはダイナミックメンバポートのようにエージアウトします。

例

VLAN 2 のマルチキャストソースとマルチキャストグループの（1.1.1.1, 232.1.1.1）のシミュレーティッドメンバポートを GigabitEthernet 1/0/1 に設定します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] quit

[AC] vlan 2

[AC-vlan2] igmp-snooping enable

[AC-vlan2] igmp-snooping version 3

[AC-vlan2] quit

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] igmp-snooping host-join 232.1.1.1 source-ip 1.1.1.1 vlan 2

1.1.24 igmp-snooping last-member-query-interval

Syntax

igmp-snooping last-member-query-interval *interval*

undo igmp-snooping last-member-query-interval

デフォルト

1 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

interval: IGMP last member クエリ間隔を設定します。設定範囲は 1～25 秒です。

説明

igmp-snooping last-member-query-interval コマンドは VLAN の IGMP last member クエリ間隔を設定します。

undo igmp-snooping last-member-query-interval コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で IGMP snooping 機能を有効にしてください。

このコマンドは **last-member-query-interval** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **last-member-query-interval** コマンドはすべての VLAN に適用されます。
- **igmp-snooping last-member-query-interval** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping last-member-query-interval** コマンドは IGMP-snooping view の **last-member-query-interval** コマンドより優先されます。

例

VLAN 2 の IGMP snooping を有効にし、VLAN 2 の IGMP last member クエリ間隔を 3 秒に設定します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] quit

[AC] vlan 2

[AC-vlan2] igmp-snooping enable

[AC-vlan2] igmp-snooping last-member-query-interval 3

関連コマンド

- **igmp-snooping enable**
- **last-member-query-interval (IGMP-snooping view)**

1.1.25 igmp-snooping leave source-ip

Syntax

igmp-snooping leave source-ip *ip-address*

undo igmp-snooping leave source-ip

デフォルト

IGMP leave クエリの送信元 IP アドレスは現在の VLAN インタフェースの IP アドレスです。現在の VLAN インタフェースに IP アドレスがない場合、送信元 IP アドレスは 0.0.0.0 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ip-address: IGMP leave メッセージの送信元 IP アドレスを指定します。

説明

igmp-snooping leave source-ip コマンドは IGMP leave メッセージの送信元 IP アドレスを設定します。

undo igmp-snooping leave source-ip コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で IGMP snooping 機能を有効にしてください。

例

VLAN 2 で IGMP snooping を有効にし、IGMP leave メッセージの送信元 IP アドレスを 10.1.1.1 に設定します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] quit

[AC] vlan 2

[AC-vlan2] igmp-snooping enable

[AC-vlan2] igmp-snooping leave source-ip 10.1.1.1

関連コマンド

igmp-snooping enable

1.1.26 igmp-snooping max-response-time

Syntax

igmp-snooping max-response-time *interval*

undo igmp-snooping max-response-time

デフォルト

10 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

interval: IGMP general クエリの最大応答時間を設定します。設定範囲は 1～3174 秒です。

説明

igmp-snooping max-response-time コマンドは VLAN の IGMP general クエリの最大応答時間を設定します。

undo igmp-snooping max-response-time コマンドはデフォルトに戻します。

このコマンドを実行する前に VLAN で IGMP snooping 機能を有効にしてください。

マルチキャストグループメンバを間違って削除しないようにするため、IGMP general クエリの最大応答時間は IGMP general クエリよりも小さいに設定してください。

このコマンドは **max-response-time** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **max-response-time** コマンドはすべての VLAN に適用されます。
- **igmp-snooping max-response-time** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping max-response-time** コマンドは IGMP-snooping view の **max-response-time** コマンドより優先されます。

例

VLAN 2 の IGMP snooping を有効にし、VLAN 2 の IGMP general クエリの最大応答時間を 5 秒に設定します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] quit

[AC] vlan 2

[AC-vlan2] igmp-snooping enable

[AC-vlan2] igmp-snooping max-response-time 5

関連コマンド

- **igmp-snooping enable**
- **igmp-snooping query-interval**
- **max-response-time (IGMP-snooping view)**

1.1.27 igmp-snooping overflow-replace

Syntax

igmp-snooping overflow-replace [**vlan** *vlan-list*]

undo igmp-snooping overflow-replace [**vlan** *vlan-list*]

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

igmp-snooping overflow-replace コマンドはポートでマルチキャストグループ置き換え機能を有効にします。

undo igmp-snooping overflow-replace コマンドはポートでマルチキャストグループ置き換え機能を無効にします。

このコマンドはポートがダイナミックに加入するマルチキャストグループでのみ適用します。

このコマンドは **overflow-replace** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **overflow-replace** コマンドはすべてのポートに適用されます。
- **igmp-snooping overflow-replace** コマンドは現在のポートに適用されます。

ポートでは **igmp-snooping overflow-replace** コマンドは IGMP-snooping view の **overflow-replace** コマンドより優先されます。

例

GigabitEthernet 1/0/1 の VLAN2 でマルチキャストグループ置き換え機能を有効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] igmp-snooping overflow-replace vlan 2

関連コマンド

overflow-replace (IGMP-snooping view)

1.1.28 igmp-snooping querier

Syntax

igmp-snooping querier

undo igmp-snooping querier

デフォルト

無効

View

VLAN view

定義済みユーザロール

network-admin

説明

igmp-snooping querier コマンドは IGMP snooping クエリアを有効にします。

undo igmp-snooping querier コマンドは IGMP snooping クエリアを無効にします。

このコマンドを実行する前に、VLAN の IGMP snooping 機能を有効にしてください。

例

VLAN 2 の IGMP snooping を有効にし、IGMP snooping クエリアを有効にします。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] quit

[AC] vlan 2

[AC-vlan2] igmp-snooping enable

[AC-vlan2] igmp-snooping querier

関連コマンド

- **igmp-snooping enable**
- **subvlan (multicast VLAN view)**

1.1.29 igmp-snooping query-interval

Syntax

igmp-snooping query-interval *interval*

undo igmp-snooping query-interval

デフォルト

125 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

interval: IGMP general クエリの送信間隔を設定します。設定範囲は 2～31744 秒です。

説明

igmp-snooping query-interval コマンドは VLAN の IGMP general クエリ送信間隔を設定します。

undo igmp-snooping query-interval コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN の IGMP snooping 機能を有効にしてください。

間違ってマルチキャストグループメンバを削除しないように、IGMP general クエリの最大応答時間より IGMP general クエリの送信間隔を大きくしてください。

例

VLAN 2 の IGMP snooping を有効にし、IGMP general クエリ送信間隔を 20 秒に設定します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] quit

[AC] vlan 2

[AC-vlan2] igmp-snooping enable

[AC-vlan2] igmp-snooping query-interval 20

関連コマンド

- **igmp-snooping enable**
- **igmp-snooping max-response-time**
- **igmp-snooping querier**
- **max-response-time**

1.1.30 igmp-snooping report source-ip

Syntax

igmp-snooping report source-ip *ip-address*

undo igmp-snooping report source-ip

デフォルト

IGMP report の送信元 IP アドレスは、現在の VLAN インタフェースの IP アドレスです。現在の VLAN インタフェースに IP アドレスが設定されていない場合、送信元 IP アドレスは 0.0.0.0 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ip-address: IGMP report の送信元 IP アドレスを指定します。

説明

igmp-snooping report source-ip コマンドは IGMP report の送信元 IP アドレスを設定します。

undo igmp-snooping report source-ip コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN の IGMP snooping 機能を有効にしてください。

例

VLAN 2 で IGMP snooping を有効にし、IGMP report の送信元 IP アドレスを 10.1.1.1 に設定します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] quit

[AC] vlan 2

[AC-vlan2] igmp-snooping enable

[AC-vlan2] igmp-snooping report source-ip 10.1.1.1

関連コマンド

igmp-snooping enable

1.1.31 igmp-snooping router-aging-time

Syntax

igmp-snooping router-aging-time *interval*

undo igmp-snooping router-aging-time

デフォルト

260 秒

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

interval: VLAN のダイナミックルータポートのエージングタイマを設定します。設定範囲は 1～8097894 秒です。

説明

igmp-snooping router-aging-time コマンドは VLAN のダイナミックルータポートのエージングタイマを設定します。

undo igmp-snooping router-aging-time コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN の IGMP snooping 機能を有効にしてください。

このコマンドは **router-aging-time** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **router-aging-time** コマンドはすべての VLAN に適用されます。
- **igmp-snooping router-aging-time** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping router-aging-time** コマンドは IGMP-snooping view の **router-aging-time** コマンドより優先されます。

例

VLAN 2 の IGMP snooping を有効にし、ダイナミックルータポートのエージングタイマを 100 秒に設定します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] quit

[AC] vlan 2

[AC-vlan2] igmp-snooping enable

[AC-vlan2] igmp-snooping router-aging-time 100

関連コマンド

- **igmp-snooping enable**
- **router-aging-time (IGMP-snooping view)**

1.1.32 igmp-snooping special-query source-ip

Syntax

igmp-snooping special-query source-ip *ip-address*

undo igmp-snooping special-query source-ip

デフォルト

VLAN で IGMP group-specific クエリの送信元 IP アドレスは以下のいずれかとなります。

- VLAN の IGMP snooping クエリアが IGMP general クエリを受信したとき、IGMP group-specific クエリの送信元 IP アドレスは IGMP general クエリの送信元 IP アドレスです。
- VLAN の IGMP snooping クエリアが IGMP general クエリを受信していない場合、IGMP group-specific クエリの送信元 IP アドレスは現在の VLAN インタフェースの IP アドレスです。
- VLAN の IGMP snooping クエリアが IGMP general クエリを受信しておらず、現在の VLAN インタフェースに IP アドレスが設定されていない場合、送信元 IP アドレスは 0.0.0.0 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ip-address: IGMP group-specific クエリの送信元 IP アドレスを指定します。

説明

igmp-snooping special-query source-ip コマンドは IGMP group-specific クエリの送信元 IP アドレスを設定します。

undo igmp-snooping special-query source-ip コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN の IGMP snooping 機能を有効にしてください。

例

VLAN 2 の IGMP snooping を有効にし、IGMP group-specific クエリの送信元 IP アドレス 10.1.1.1 を設定します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] quit

[AC] vlan 2

[AC-vlan2] igmp-snooping enable

[AC-vlan2] igmp-snooping special-query source-ip 10.1.1.1

関連コマンド

igmp-snooping enable

1.1.33 igmp-snooping static-group

Syntax

igmp-snooping static-group *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

undo igmp-snooping static-group { *group-address* [**source-ip** *source-address*] **vlan** *vlan-id* | **all** }

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

group-address: マルチキャストグループの IP アドレスを指定します。設定範囲は 224.0.1.0～239.255.255.255 です。

source-ip *source-address*: マルチキャストソースの IP アドレスを指定します。マルチキャストソースを指定した場合、ポートをマルチキャストソースとグループのスタティックメンバポートとして設定します。マルチキャストソースを指定しない場合、ポートをマルチキャストグループのスタティックメンバポートとして設定します。このパラメータは IGMPv3 snooping が動作する装置で有効です。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

all: すべての VLAN を指定します。

説明

igmp-snooping static-group コマンドはマルチキャストグループのスタティックメンバポートを設定します。

undo igmp-snooping static-group コマンドはスタティックメンバポートを削除します。

例

VLAN 2 のマルチキャストソースとマルチキャストグループの（1.1.1.1, 225.0.0.1）のスタティックメンバポートを GigabitEthernet 1/0/1 に設定します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] quit

[AC] vlan 2

[AC-vlan2] igmp-snooping enable

[AC-vlan2] igmp-snooping version 3

[AC-vlan2] quit

[AC] interface Gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] igmp-snooping static-group 225.0.0.1 source-ip 1.1.1.1 vlan 2

1.1.34 igmp-snooping static-router-port

Syntax

igmp-snooping static-router-port vlan *vlan-id*

undo igmp-snooping static-router-port { **all** | **vlan** *vlan-id* }

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

all: すべての VLAN を指定します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。

説明

igmp-snooping static-router-port コマンドはスタティックルータポートを設定します。

undo igmp-snooping static-router-port コマンドはスタティックルータポートを削除します。

例

VLAN 2 の GigabitEthernet 1/0/1 をスタティックルータポートに設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] igmp-snooping static-router-port vlan 2

1.1.35 igmp-snooping version

Syntax

igmp-snooping version *version-number*

undo igmp-snooping version

デフォルト

2

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

version-number: IGMP snooping のバージョンを指定します。2 あるいは 3 です。

説明

igmp-snooping version コマンドは IGMP snooping のバージョンを指定します。

undo igmp-snooping version コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN の IGMP snooping 機能を有効にしてください。

VLAN view 内の VLAN もしくは、IGMP-snooping view で指定された VLAN に対してバージョンを指定できます。VLAN view の設定は IGMP-snooping view の設定と同じ優先度を持ちます。最後に行われた設定が適用されます。

例

VLAN 2 の IGMP snooping を有効にし、IGMP snooping のバージョンを 3 に指定します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] quit

[AC] vlan 2

[AC-vlan2] igmp-snooping enable

[AC-vlan2] igmp-snooping version 3

関連コマンド

igmp-snooping enable

1.1.36 last-member-query-interval (IGMP-snooping view)

Syntax

last-member-query-interval *interval*

undo last-member-query-interval

デフォルト

1 秒

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

interval: IGMP last member クエリ間隔を設定します。設定範囲は 1～25 秒です。

説明

last-member-query-interval コマンドはグローバルで IGMP last member クエリ間隔を設定します。

undo last-member-query-interval コマンドはデフォルトに戻します。

このコマンドは **igmp-snooping last-member-query-interval** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **last-member-query-interval** コマンドはすべての VLAN に適用されます。

- **igmp-snooping last-member-query-interval** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping last-member-query-interval** コマンドは IGMP-snooping view の **last-member-query-interval** コマンドより優先されます。

例

IGMP last member クエリ間隔を 3 秒に設定します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] last-member-query-interval 3

関連コマンド

igmp-snooping last-member-query-interval

1.1.37 max-response-time (IGMP-snooping view)

Syntax

max-response-time *interval*

undo max-response-time

デフォルト

10 秒

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

interval: IGMP general クエリの最大応答時間を設定します。設定範囲は 1～3174 秒です。

説明

max-response-time コマンドはグローバルで IGMP general クエリの最大応答時間を設定します。

undo max-response-time コマンドはデフォルトに戻します。

マルチキャストグループメンバを間違って削除しないようにするため、IGMP general クエリの最大応答時間は IGMP general クエリよりも小さいに設定してください。

このコマンドは **igmp-snooping max-response-time** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **max-response-time** コマンドはすべての VLAN に適用されます。
- **igmp-snooping max-response-time** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping max-response-time** コマンドは IGMP-snooping view の **max-response-time** コマンドより優先されます。

例

グローバルで IGMP general クエリの最大応答時間を 5 秒に設定します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] max-response-time 5

関連コマンド

- **igmp-snooping max-response-time**
- **igmp-snooping query-interval**

1.1.38 overflow-replace (IGMP-snooping view)

Syntax

overflow-replace [**vlan** *vlan-list*]

undo overflow-replace [**vlan** *vlan-list*]

デフォルト

無効

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*: VLAN を指定します。半角スペースで区切り、10 まで設定することができます。VLAN を範囲で指定する形式は *start-vlan-id* **to** *end-vlan-id* です。設定範囲は 1～4094 です。指定しない場合、すべての VLAN に適用します。

説明

overflow-replace コマンドはグローバルでマルチキャストグループ置き換え機能を有効にします。

undo overflow-replace コマンドはグローバルでマルチキャストグループ置き換え機能を無効にします。

このコマンドはポートがダイナミックに加入するマルチキャストグループでのみ適用します。

このコマンドは **igmp-snooping overflow-replace** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **overflow-replace** コマンドはすべてのポートに適用されます。
- **igmp-snooping overflow-replace** コマンドは現在のポートに適用されます。

ポートでは **igmp-snooping overflow-replace** コマンドは IGMP-snooping view の **overflow-replace** コマンドより優先されます。

例

VLAN2 でマルチキャストグループ置き換え機能を有効にします。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] overflow-replace vlan 2

関連コマンド

igmp-snooping overflow-replace

1.1.39 report-aggregation (IGMP-snooping view)

Syntax

report-aggregation

undo report-aggregation

デフォルト

有効

View

IGMP-snooping view

定義済みユーザロール

network-admin

説明

report-aggregation コマンドは IGMP report 抑制機能を有効にします。

undo report-aggregation コマンドは IGMP report 抑制機能を無効にします。

例

IGMP report 抑制機能を無効にします。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] undo report-aggregation

1.1.40 reset igmp-snooping group

Syntax

reset igmp-snooping group { *group-address* [*source-address*] | **all** } [**vlan** *vlan-id*]

View

User view

定義済みユーザロール

network-admin

パラメータ

group-address: マルチキャストグループの IP アドレスを指定します。設定範囲は 224.0.1.0～239.255.255.255 です。

source-address: マルチキャストソースの IP アドレスを指定します。指定しない場合、すべてのマルチキャストソースのダイナミック IGMP snooping グループエントリを削除します。

all: すべてのマルチキャストグループを指定します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のダイナミック IGMP snooping グループエントリを削除します。

説明

reset igmp-snooping group コマンドはダイナミック IGMP snooping グループエントリを削除します。

例

すべてのダイナミック IGMP snooping グループエントリを削除します。

<AC> reset igmp-snooping group all

関連コマンド

display igmp-snooping group

1.1.41 reset igmp-snooping router-port

Syntax

reset igmp-snooping router-port { **all** | **vlan** *vlan-id*]

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべての VLAN を指定します。

vlan *vlan-id*: VLAN の ID を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のダイナミックルータポートを削除します。

説明

reset igmp-snooping router-port コマンドはダイナミックルータポートの情報を削除します。

例

すべてのダイナミックルータポートの情報を削除します。

<AC> reset igmp-snooping router-port all

関連コマンド

display igmp-snooping router-port

1.1.42 reset igmp-snooping statistics

Syntax

reset igmp-snooping statistics

View

User view

定義済みユーザロール

network-admin

説明

reset igmp-snooping statistics コマンドは IGMP snooping によって学習した IGMP メッセージの統計情報を削除します。

例

IGMP snooping によって学習した IGMP メッセージの統計情報を削除します。

<AC> reset igmp-snooping statistics

関連コマンド

display igmp-snooping statistics

1.1.43 router-aging-time (IGMP-snooping view)

Syntax

router-aging-time *interval*

undo router-aging-time

デフォルト

260 秒

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

interval: ダイナミックルータポートのエージングタイマを設定します。設定範囲は 1～8097894 秒です。

説明

router-aging-time コマンドはグローバルでダイナミックルータポートのエージングタイマを設定します。

undo router-aging-time コマンドはデフォルトに戻します。

このコマンドは **igmp-snooping router-aging-time** コマンドと同一機能ですが、適用範囲が異なります。

- IGMP-snooping view の **router-aging-time** コマンドはすべての VLAN に適用されます。
- **igmp-snooping router-aging-time** コマンドは現在の VLAN に適用されます。

VLAN では **igmp-snooping router-aging-time** コマンドは IGMP-snooping view の **router-aging-time** コマンドより優先されます。

例

グローバルでダイナミックルータポートのエージングタイマを 100 秒に設定します。

<AC> system-view

[AC] igmp-snooping

[AC-igmp-snooping] router-aging-time 100

関連コマンド

igmp-snooping router-aging-time

QX-W2230AC アクセスコントローラ

コマンドマニュアル

8.ACL and QoS

本マニュアルは以下に示す章で構成されています。

01-ACL
02-QoS ポリシー
03-プライオリティマッピング
04-タイムレンジ

目次

このセクションのページは **8-x-x** です。

1 章 ACL 1-1
1.1 ACL 設定コマンド 1-1
1.1.1 acl 1-1
1.1.2 acl copy 1-4
1.1.3 description 1-5
1.1.4 display acl 1-6
1.1.5 packet-filter (Interface View) 1-7
1.1.6 packet-filter (service template view) 1-9
1.1.7 reset acl counter 1-10
1.1.8 rule (IPv4 advanced ACL view) 1-11
1.1.9 rule (IPv4 basic ACL view) 1-16
1.1.10 rule (Layer 2 ACL view) 1-18
1.1.11 rule (WLAN client ACL view) 1-20
1.1.12 rule (WLAN AP ACL view) 1-21
1.1.13 rule comment 1-23
1.1.14 step 1-24

1章 ACL

1.1 ACL設定コマンド

1.1.1 acl

🕮 メモ：

- **acl number** *acl-number* 形式での ACL 作成は、ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアからサポートしています。
- **acl number** *acl-number* 形式では、WLAN クライアントの ACL と WLAN AP の ACL を作成することはできません。WLAN クライアントの ACL を作成する場合は、”**acl wlan client**”の形式、WLAN AP の ACL を作成する場合は、”**acl wlan ap**”の形式で作成してください。

Syntax

acl number *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]

acl { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

acl mac { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

acl wlan client { *acl-number* | **name** *acl-name* }

acl wlan ap { *acl-number* | **name** *acl-name* }

undo acl { **all** | { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } }

undo acl mac { **all** | *acl-number* | **name** *acl-name* }

undo acl wlan client { *acl-number* | **all** | **name** *acl-name* }

undo acl wlan ap { *acl-number* | **all** | **name** *acl-name* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

basic: 標準 ACL を指定します。

advanced: 拡張 ACL を指定します。

mac: L2 ACL を指定します。

wlan client: WLAN クライアントの ACL タイプを指定します。

wlan ap: WLAN AP の ACL タイプを指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 100～199：WLAN クライアントの ACL です。
- 200～299：WLAN AP の ACL です。
- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。

name *acl-name*: ACL を識別しやすくするため、ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。混乱を避けるため、**all** は使用できません。

match-order: パケットを比較する ACL ルールの順番を設定します。

- **auto**: 深さ優先順序に従って ACL ルールを比較します。詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS “ACL”* を参照してください。
- **config**: ルール ID の昇順に従って ACL ルールを比較します。小さいルール ID は優先度が高くなります。ACL ルールの順序を指定しない場合、デフォルトで **config** が適用されます。

all: すべての ACL を指定します。

説明

acl コマンドは ACL を作成し、ACL の view に移行します。すでに ACL が作成されている場合、その view に移行します。

undo acl コマンドは指定された、あるいはすべての ACL を削除します。

ルールが含まれていない ACL のみ、比較順序を変更することができます。

ACL のルールが一致順序を含む、あるいは以下の一致基準が有効である場合、一致するパケットはソフトウェアベースのパケット転送を行います。

- 送信元および宛先 IP アドレス
- 送信元ポート、宛先ポート
- トランスポートレイヤプロトコル
- ICMP メッセージタイプ、メッセージコード、およびメッセージ名
- VPN インスタンス
- ロギング
- タイムレンジ

ソフトウェアベースのパケット転送は、転送エントリのため、コントロールプレーンにパケットを送信します。これは装置のパケット転送に影響します。

例

標準 IPv4 ACL 2000 を作成し、その view に移行します。

<AC> system-view

[AC] acl basic 2000

[AC-acl-ipv4-basic-2000]

ACL 名が flow の標準 IPv4 ACL を作成し、その view に移行します。

<AC> system-view

[AC] acl basic name flow

[AC-acl-ipv4-basic-flow]

拡張 IPv4 ACL 3000 を作成し、その view に移行します。

<AC> system-view

[AC] acl advanced 3000

[AC-acl-ipv4-adv-3000]

L2 ACL 4000 を作成し、その view に移行します。

<AC> system-view

[AC] acl mac 4000

[AC-acl-mac-4000]

ACL 名が flow の L2 ACL を作成し、その view に移行します。

<AC> system-view

[AC] acl mac name flow

[AC-acl-mac-flow]

WLAN クライアント ACL100 を作成し、その view に移行します。

<AC> system-view

[AC] acl wlan client 100

[AC-acl-client-100]

ACL 名が flow の WLAN クライアントを作成し、その view に移行します。

<AC> system-view

[AC] acl wlan client name flow

[AC-acl-client-flow]

WLAN AP ACL200 を作成し、その view に移行します。

<AC> system-view

[AC] acl wlan ap 200

[AC-acl-ap-200]

ACL 名が flow の WLAN AP を作成し、その view に移行します。

<AC> system-view

[AC] acl wlan ap name flow

[AC-acl-ap-flow]

関連コマンド

display acl

1.1.2 acl copy

Syntax

acl [**mac**] **copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

View

System view

定義済みユーザロール

network-admin

パラメータ

ipv6: IPv6 ACL を指定します。

mac: L2 ACL を指定します。

source-acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 100～199：WLAN クライアント ACL です。
- 200～299：WLAN AP ACL です。
- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。**mac** の指定が必要です。

name *source-acl-name*: ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。

dest-acl-number: 新しい ACL の番号を指定します。以下に設定範囲を示します。

- 100～199：WLAN クライアント ACL です。
- 200～299：WLAN AP ACL です。
- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。

name *dest-acl-name*: ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。混乱を避けるため、**all** は使用できません。

説明

acl copy コマンドは既存の ACL をコピーします。

新しい ACL は既存の ACL とカテゴリ、同一内容ですが、ACL 名と ACL 番号が異なります。

IPv4 ACL を指定する場合、**mac** パラメータを指定しないでください。

例

標準 IPv4 ACL 2001 をコピーし、標準 IPv4 ACL 2002 を作成します。

<AC> system-view

[AC] acl copy 2001 to 2002

ACL 名が test の標準 IPv4 ACL をコピーし、ACL 名が paste の標準 IPv4 ACL を作成します。

<AC> system-view

[AC] acl copy name test to name paste

1.1.3 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

IPv4 basic/advanced ACL view

Layer 2 ACL view

WLAN AP/client ACL view

定義済みユーザロール

network-admin

パラメータ

text: ACL の説明を設定します。設定範囲は 1～127 です。大文字、小文字は区別します。

説明

description コマンドは ACL の説明を設定します。

undo description コマンドは ACL の説明を削除します。

例

標準 IPv4 ACL 2000 の説明を設定します。

<AC> system-view

[AC] acl basic 2000

[AC-acl-ipv4-basic-2000] description This is an IPv4 basic ACL.

関連コマンド

display acl

1.1.4 display acl

Syntax

display acl [**mac** | **wlan**] { *acl-number* | **all** | **name** *acl-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac: L2 ACL を指定します。

wlan client: WLAN クライアント ACL と WLAN AP ACL を含む WLAN ACL を指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 100～199：WLAN クライアント ACL です。
- 200～299：WLAN AP ACL です。
- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。**mac** の指定が必要です。

all: すべての ACL を指定します。

name *acl-name*: ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。

説明

display acl コマンドは ACL の設定と一致する統計情報を表示します。

ACL ルールの順番が設定されたとき、このコマンドは **config** あるいは **auto** で表示します。

IPv4 ACL を指定する場合、**mac** パラメータ、あるいは **wlan** パラメータを指定しないでください。

例

標準 IPv4 ACL 2001 の設定と一致する統計情報を表示します。

<AC> display acl 2001

```
Basic IPv4 ACL 2001, 1 rules, match-order is auto,
This is an IPv4 basic ACL.
ACL's step is 5
 rule 5 permit source 1.1.1.1 0
 rule 5 comment This rule is used on GigabitEthernet 1/0/1.
```

表 1-1 コマンド出力

フィールド	説明
Basic IPv4 ACL 2001	ACLのカテゴリと番号です。フィールドの情報は標準IPv4 ACL 2000です。
1 rule	ACLは1つのルールがあることを示します。
match-order is auto	ACLの比較順序が**auto**です。深さ優先順序に従ってACLルールを比較します。比較順序が**config**である場合は表示されません。
This is an IPv4 basic ACL.	ACLの説明です。
ACL's step is 5	ルールのステップ数が5です。
rule 5 permit source 1.1.1.1 0	ルール5の内容です。IPアドレス1.1.1.1からのパケットを許可します。
rule 5 comment This rule is used on GigabitEthernet 1/0/1.	ACLルール5の説明です。

1.1.5 packet-filter (Interface View)

🕮 **メモ：**

- **packet-filter** コマンドは、ソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。
- Ethernet インタフェース、アグリゲートインタフェースに適用した ACL は、Layer2 通信パケットに対してのみ動作します。
- VLAN インタフェースに適用した ACL は、Layer3 通信パケットに対してのみ動作します。

Syntax

packet-filter [**mac**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

undo packet-filter [**mac**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

mac: レイヤ 2 ACL タイプを指定します。

acl-number: ACL を番号で指定します。使用可能な値の範囲は次のとおりです。

- 2000～2999 : 標準 IPv4 ACL です。
- 3000～3999 : 拡張 IPv4 ACL です。
- 4000～4999 : L2 ACL です。

name *acl-name*: ACL 名を指定します。設定範囲は 1～63 文字で、大文字と小文字を区別しません。

inbound: インタフェースで受信されるパケットをフィルタリングします。

outbound: インタフェースで送信されるパケットをフィルタリングします。

説明

packet-filter コマンドは、インタフェースに ACL を適用します。

undo packet-filter コマンドは、インタフェースから ACL を削除します。

IPv 4 ACL タイプを指定する場合、**mac** キーワードを指定しないでください。

この機能は、アグリゲートメンバーポートでは有効になりません。

インタフェースの同じ方向に、最大 32 の ACL を適用できます。

例

GigabitEthernet 1/0/1 に対し、受信したトラフィックをフィルタリングするため、IPv4 標準 ACL 2001 を適用します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] packet-filter 2001 inbound

関連コマンド

display acl

1.1.6 packet-filter (service template view)

🕮 メモ：

- **packet-filter** コマンドは、ソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。
- FIT または Anchor-FIT AP の無線にバインドしたサービステンプレートで動作させる場合、AC ではなく、FIT または Anchor-FIT AP 側に ACL を設定する必要があります。コンフィグレーションプロファイル機能、または **map-configuration** コマンドを使用して ACL を設定してください。

Syntax

packet-filter { *acl-number* **| name** *acl-name* **} { inbound | outbound }**

undo packet-filter { *acl-number* **| name** *acl-name* **} { inbound | outbound }**

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

acl-number: ACL を番号で指定します。使用可能な値の範囲は次のとおりです。

- 2000～2999： 標準 IPv4 ACL です。
- 3000～3999： 拡張 IPv4 ACL です。

name *acl-name*: ACL 名を指定します。設定範囲は 1～63 文字で、大文字と小文字を区別しません。

inbound: 受信されるパケットをフィルタリングします。

outbound: 送信されるパケットをフィルタリングします。

説明

packet-filter コマンドは、サービステンプレートに ACL を適用します。

undo packet-filter コマンドは、サービステンプレートから ACL を削除します。

サービステンプレートに適用される ACL は、送信元 IP アドレス、宛先 IP アドレス、送信元ポート番号、宛先ポート番号、およびパケットのプロトコルのみを照合できます。

サービステンプレートの同じ方向に適用できる ACL は 1 つだけです。

このコマンドは、サービステンプレートが無効の場合にのみ実行できます。

例

サービステンプレート service1 に対し、受信したトラフィックをフィルタリングするため、標準 IPv4 ACL 2001 を適用します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] packet-filter 2001 inbound

1.1.7 reset acl counter

Syntax

reset acl [**mac**] **counter** { *acl-number* | **all** | **name** *acl-name* }

View

User view

定義済みユーザロール

network-admin

パラメータ

mac: L2 ACL を指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。**mac** の指定が必要です。

all: すべての ACL の統計情報を削除します。

name *acl-name*: ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。

説明

reset acl counter コマンドは ACL の統計情報を削除します。

例

標準 IPv4 ACL 2001 の統計情報を削除します。

<AP> reset acl counter 2001

関連コマンド

display acl

1.1.8 rule (IPv4 advanced ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **destination** | **destination-port** | { **dscp** | { **precedence** | **tos** } * } | **fragment** | **icmp-type** | **source** | **source-port** | **time-range**] *

デフォルト

設定なし

View

IPv4 advanced ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

protocol: プロトコル番号あるいはプロトコル名を指定します。

- プロトコル番号の設定範囲は 0～255 です。
- プロトコル名は **gre** (47)、**icmp** (1)、**igmp** (2)、**ip**、**ipinip** (4)、**ospf** (89)、**tcp** (6)、**udp** (17)を指定できます。**ip** はすべてのプロトコルを指定します。表 1-26 にプロトコルの値に関わらず指定できるパラメータを示します。

表 1-2 拡張 IPv4 ACL ルールの一致基準と他のルールの情報

パラメータ	機能	説明
source { *source-address source-wildcard* | **any** }	送信元アドレスを定義します。	*source-address*と*source-wildcard*はドットで区切られた10進数表記の送信元IPアドレスとワイルドカードマスクを示します。すべてが0のワイルドカードはホストアドレスを示します。 **any**は、任意の送信元IPアドレスを示します。
destination { *dest-address dest-wildcard* | **any** }	宛先アドレスを定義します。	*dest-address*と*dest-wildcard*はドットで区切られた10進数表記の宛先IPアドレスとワイルドカードマスクを示します。すべてが0のワイルドカードはホストアドレスを示します。 **any**は、任意の宛先IPアドレスを示します。
precedence *precedence*	IPプレシーデンスの値を指定します。	プレシーデンスの値あるいはプレシーデンスの名前を指定します。番号の設定範囲は0～7です。名前は**routine** (0)、**priority** (1)、**immediate** (2)、**flash** (3)、**flash-override** (4)、**critical** (5)、**internet** (6)、**network** (7)が指定できます。
tos *tos*	ToSプレシーデンスを指定します。	プレシーデンスの値あるいはプレシーデンスの名前を指定します。番号の設定範囲は0～15です。名前は**max-reliability** (2)、**max-throughput** (4)、**min-delay** (8)、**min-monetary-cost** (1)、**normal** (0)が指定できます。
dscp *dscp*	DSCPプライオリティを指定します。	*dscp*プライオリティの値あるいはプライオリティの名前を指定します。番号の設定範囲は0～63です。名前は**af11** (10)、**af12** (12)、**af13** (14)、**af21** (18)、**af22** (20)、**af23** (22)、**af31** (26)、**af32** (28)、**af33** (30)、**af41** (34)、**af42** (36)、**af43** (38)、**cs1** (8)、**cs2** (16)、**cs3** (24)、**cs4** (32)、**cs5** (40)、**cs6** (48)、**cs7** (56)、**default** (0)、**ef** (46)が指定できます。
fragment	最初のフラグメントではないフラグメントを指定します。	指定しない場合、ルールはすべてのフラグメントと非フラグメントを適用します。

パラメータ	機能	説明
time-range *time-range-name*	ルールのタイムレンジを指定します。	*time-range-name*の設定範囲は1～32文字です。大文字、小文字を区別しません。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション8 *ACL and QoS* *"タイムレンジ"*を参照してください。

protocol が **tcp** (6)あるいは **udp** (17)である場合、設定するパラメータを表 1-37 に示します。

表 1-3 拡張 IPv4 ACL ルールの TCP/UDP 指定パラメータ

パラメータ	機能	説明
source-port *operator port1* [*port2*]	1つまたは複数のTCP/UDPの送信元ポート番号を指定します。	*operator*は**lt** (lower than)、**gt** (greater than)、**eq** (equal to)、**neq** (not equal to)、**range** (inclusive range)が指定できます。*port1*、*port2*はTCPあるいはUDPポート番号です。設定範囲は0～65535です。*port2*は*operator*が範囲であるときのみ必要です。 TCPポート番号は以下の名前で指定できます。**chargen** (19)、**bgp** (179)、**cmd** (514)、**daytime** (13)、**discard** (9)、**domain** (53)、**echo** (7)、**exec** (512)、**finger** (79)、**ftp** (21)、**ftp-data** (20)、**gopher** (70)、**hostname** (101)、**irc** (194)、**klogin** (543)、**kshell** (544)、**login** (513)、**lpd** (515)、**nntp** (119)、**pop2** (109)、**pop3** (110)、**smtp** (25)、**sunrpc** (111)、**tacacs** (49)、**talk** (517)、**telnet** (23)、**time** (37)、**uucp** (540)、**whois** (43)、**www** (80) UDPポート番号は以下の名前で指定できます **biff** (512)、**bootpc** (68)、**bootps** (67)、**discard** (9)、**dns** (53)、**dnsix** (90)、**echo** (7)、**mobilip-ag** (434)、**mobilip-mn** (435)、**nameserver** (42)、**netbios-dgm** (138)、**netbios-ns** (137)、**netbios-ssn** (139)、**ntp** (123)、**rip** (520)、**snmp** (161)、**snmptrap** (162)、**sunrpc** (111)、**syslog** (514)、**tacacs-ds** (65)、**talk** (517)、**tftp** (69)、**time** (37)、**who** (513)、**xdmcp** (177)
destination-port *operator port1* [*port2*]	1つまたは複数のTCP/UDPの宛先ポート番号を指定します。	
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* |	ACK、FIN、PSH、RST、SYN、URGを	TCP用のパラメータです。各値は0(フラグビットがセットされていません)または1(フラグ

パラメータ	機能	説明
rst *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	含む1つまたは複数のTCPフラグを指定します。	ビットがセットされています)が指定できます。ルールのTCPフラグはANDの関係です。たとえば、ack 0 psh 1が設定されたルールは、ACKフラグが設定されていないパケット、およびPSHフラグが設定されているパケットに一致します。
established	TCP接続の確立状態を示すフラグを指定します。	TCP用のパラメータです。ルールはACKあるいはRSTフラグがセットされているTCP接続パケットに一致します。

protocol が **icmp** (1)である場合、設定するパラメータを表 1-4 に示します。

表 1-4 拡張 IPv4 ACL ルールの ICMP 指定パラメータ

パラメータ	機能	説明
icmp-type { **icmp-type** *icmp-code* | *icmp-message* }	ICMPメッセージタイプとコードを指定します。	*icmp-type*の設定範囲は0～255です。*icmp-code*の設定範囲は0～255です。*icmp-message*はメッセージの名前を指定します。サポートされるICMPメッセージ名と対応するタイプとコードの値を表 1-5に示します。

表 1-5 拡張 IPv4 ACL ルールでサポートされる ICMP メッセージ名

ICMP メッセージ名	ICMP メッセージタイプ	ICMP メッセージコード
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2

ICMP メッセージ名	ICMP メッセージタイプ	ICMP メッセージコード
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

説明

rule コマンドは拡張 IPv4 ACL のルールを作成あるいは修正します。

undo rule コマンドは拡張 IPv4 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

- すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。
- パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

ACL のルールとルールの ID を表示する場合、**display acl all** コマンドを使用します。

例

アドレス 129.9.0.0/16 から 202.38.160.0/24 の宛先ポート 80 の TCP パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] acl advanced 3000

[AC-acl-ipv4-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0 0.0.0.255 destination-port eq 80

192.168.1.0/24 宛の ICMP パケットを除くすべての IP パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] acl advanced 3001

[AC-acl-ipv4-adv-3001] rule deny icmp destination 192.168.1.0 0.0.0.255

[AC-acl-ipv4-adv-3001] rule permit ip

FTP の送受信パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] acl advanced 3002

[AC-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp

[AC-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp-data

[AC-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp

[AC-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp-data

SNMP と SNMP trap の送受信パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] acl advanced 3003

[AC-acl-ipv4-adv-3003] rule permit udp source-port eq snmp

[AC-acl-ipv4-adv-3003] rule permit udp source-port eq snmptrap

[AC-acl-ipv4-adv-3003] rule permit udp destination-port eq snmp

[AC-acl-ipv4-adv-3003] rule permit udp destination-port eq snmptrap

関連コマンド

- **acl**
- **display acl**
- **step**
- **time-range**

1.1.9 rule (IPv4 basic ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**fragment** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *

undo rule *rule-id* [**fragment** | **source** | **time-range**] *

デフォルト

設定なし

View

IPv4 basic ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

fragment: 最初のフラグメントではないフラグメントを指定します。指定しない場合、ルールはすべてのフラグメントと非フラグメントを適用します。

source { *source-address source-wildcard* | **any** }: 送信元アドレスを定義します。*source-address* と *source-wildcard* はドットで区切られた 10 進数表記の送信元 IP アドレスとワイルドカードマスクを示します。すべてが 0 のワイルドカードはホストアドレスを示します。**any** は、任意の送信元 IP アドレスを示します。

time-range *time-range-name*: ルールのタイムレンジを指定します。*time-range-name* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS “タイムレンジ”* を参照してください。

説明

rule コマンドは標準 IPv4 ACL のルールを作成あるいは修正します。

undo rule コマンドは標準 IPv4 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

- すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。

- パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

ACL のルールとルールの ID を表示する場合、**display acl all** コマンドを使用します。

例

アドレス 10.0.0.0/8、172.17.0.0/16、192.168.1.0/24 を除く送信元 IP セグメントからのパケットを拒否する標準 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] acl basic 2000

[AC-acl-ipv4-basic-2000] rule permit source 10.0.0.0 0.255.255.255

[AC-acl-ipv4-basic-2000] rule permit source 172.17.0.0 0.0.255.255

[AC-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255

[AC-acl-ipv4-basic-2000] rule deny source any

関連コマンド

- **acl**
- **display acl**
- **step**
- **time-range**

1.1.10 rule (Layer 2 ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

undo rule *rule-id* [**time-range**]

デフォルト

設定なし

View

Layer 2 ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始

まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

cos *vlan-pri*: 802.1p プライオリティを定義します。

- プライオリティの設定範囲は 0～7 です。
- **best-effort** (0)、**background** (1)、**spare** (2)、**excellent-effort** (3)、**controlled-load** (4)、**video** (5)、**voice** (6)、**network-management** (7)の用語で定義することができます。

dest-mac *dest-address dest-mask*: 宛先 MAC アドレス範囲を定義します。*dest-address* と *dest-mask* は宛先 MAC アドレスとマスクを示します。マスクの形式は H-H-H です。

lsap *lsap-type lsap-type-mask*: LLC カプセル化の DSAP と SSAP フィールドを定義します。*lsap-type* は 16 進数表記でカプセル化フォーマットを示します。*lsap-type-mask* は 16 進数表記で LSAP マスクを示します。

type *protocol-type protocol-type-mask*: L2 の 1 つ以上のプロトコルを定義します。*protocol-type* は 16 進数表記で Ethernet_II と Ethernet_SNAP のプロトコルタイプを示します。*protocol-type-mask* は 16 進数表記でプロトコルタイプのマスクを示します。

source-mac *source-address source-mask*: 送信元 MAC アドレス範囲を定義します。*source-address* は送信元 MAC アドレスを示します。*sour-mask* はマスクを示します。マスクの形式は H-H-H です。

time-range *time-range-name*: ルールのタイムレンジを指定します。*time-range-name* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。最初の文字は英字を使用する必要があります。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS “タイムレンジ”* を参照してください。

説明

rule コマンドは L2 ACL のルールを作成あるいは修正します。

undo rule コマンドは L2 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

- すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。
- パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

L2 ACL のルールとルールの ID を表示する場合、**display acl all** コマンドを使用します。

例

L2 ACL 4000 のルールを作成します。ARP パケットを許可し、RARP パケットを拒否します。

<AC> system-view

[AC] acl mac 4000

[AC-acl-mac-4000] rule permit type 0806 ffff

[AC-acl-mac-4000] rule deny type 8035 ffff

関連コマンド

- **acl**
- **display acl**
- **step**
- **time-range**

1.1.11 rule (WLAN client ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**ssid** *ssid-name*]

undo rule *rule-id*

デフォルト

設定なし

View

WLAN client ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

ssid *ssid-name*: SSID の名前を指定します。設定範囲は 1～32 文字です。大文字と小文字を区別します。文字、数字、スペースが入力可能です。このオプションを指定しない場合、ルールはすべての SSID のパケットに適用されます。

説明

rule コマンドは WLAN クライアント ACL のルールを作成あるいは修正します。

undo rule コマンドは WLAN クライアント ACL ルールを削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

ACL のルールとルールの ID を表示する場合、**display acl all** コマンドを使用します。

例

WLAN クライアント ACL 111 のルールを作成します。SSID が **ME** のパケットを許可し、SSID が **HIM** のパケットを拒否します。

<AC> system-view

[AC] acl wlan client 111

[AC-acl-client-111] rule permit ssid ME

[AC-acl-client-111] rule deny ssid HIM

関連コマンド

- **acl wlan client**
- **display acl**
- **step**

1.1.12 rule (WLAN AP ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**mac** *mac-address mac-mask*] [**serial-id** *serial-id*]

undo rule *rule-id*

デフォルト

設定なし

View

WLAN AP ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

mac *mac-address mac-mask*: AP の MAC アドレスの範囲と一致するように指定します。*mac-address* は H-H-H 形式の MAC アドレスをあらわします。*mac-mask* は H-H-H 形式のマスクをあらわします。**mac** *mac-address mac-mask* を指定しない場合、ルールはすべての MAC アドレスに適用されます。

serial-id *serial-id*: AP のシリアル ID に一致するように指定します。設定範囲は 1～32 文字です。大文字と小文字を区別しません。このオプションを指定しない場合、ルールはすべてのシリアル ID に適用されます。

説明

rule コマンドは WLAN AP ACL のルールを作成あるいは修正します。

undo rule コマンドは WLAN AP ACL ルールを削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

ACL のルールとルールの ID を表示する場合、**display acl all** コマンドを使用します。

例

WLAN AP ACL 222 のルールを作成します。シリアル ID が 210235A42QB095000766 の AP を許可し、シリアル ID が 210235A42QB095000777 の AP を拒否します。

<AC> system-view

[AC] acl wlan ap 222

[AC-acl-ap-222] rule permit serial-id 210235A42QB095000766

[AC-acl-ap-222] rule deny serial-id 210235A42QB095000777

関連コマンド

- **acl wlan ap**
- **display acl**
- **step**

1.1.13 rule comment

Syntax

rule *rule-id* **comment** *text*

undo rule *rule-id* **comment**

デフォルト

設定なし

View

IPv4 basic/advanced ACL view

Layer 2 ACL view

WLAN AP/client ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ACL のルール ID を指定します。設定範囲は 0～65534 です。ACL のルールはすでに作成されている必要があります。

text: ACL のルールの説明を指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

rule comment コマンドは ACL のルールの説明を設定します。

undo rule comment コマンドは ACL のルールの説明を削除します。

例

標準 IPv4 ACL 2000 を作成し、ルールの説明を追加します。

<AC> system-view

[AC] acl basic 2000

[AC-acl-ipv4-basic-2000] rule 0 deny source 1.1.1.1 0

[AC-acl-ipv4-basic-2000] rule 0 comment This rule is used on Gigabitethernet 1/0/1.

関連コマンド

display acl

1.1.14 step

Syntax

step *step-value*

undo step

デフォルト

ACL のルール番号付けステップは 5 で、開始ルール ID は 0 です。

View

IPv4 basic/advanced ACL view

Layer 2 ACL view

WLAN AP/client ACL view

定義済みユーザロール

network-admin

パラメータ

step-value: ACL ルールのステップ数を指定します。設定範囲は 1～20 です。

説明

step コマンドは ACL ルールに自動的に番号を割り振るためのステップ数を設定します。

undo step コマンドはデフォルトに戻します。

ルールの番号づけステップはシステムが自動的にルール番号の増分を設定します。たとえば、デフォルトの ACL の番号づけステップは 5 です。ルールを作成するとき、ID を割り当てない場合、ルールの番号は 0、5、10、15、...と番号づけられます。番号づけのステップを広くする場合、2 つのルールの間に多くのルールを挿入することができます。ステップを変更したときはいつでも、ルールは 0 から再ナンバリングが行われます。たとえば、5 つのルールの番号 5、10、13、15、20 がつけられている場合、ステップを 5 から 2 に変更すると、ルールの番号は 0、2、4、6、8 に再ナンバリングされます。

例

標準 IPv4 ACL 2000 のステップ数を 2 に設定します。

<AC> system-view

[AC] acl basic 2000

[AC-acl-ipv4-basic-2000] step 2

関連コマンド

display acl

目次

このセクションのページは **8-x-x** です。

2 章 QoS ポリシー.....2-1
2.1 トラフィッククラス設定コマンド.....2-1
2.1.1 display traffic classifier.....2-1
2.1.2 if-match.....2-2
2.1.3 traffic classifier.....2-7
2.2 トラフィック動作設定コマンド.....2-8
2.2.1 car.....2-8
2.2.2 display traffic behavior.....2-9
2.2.3 filter.....2-11
2.2.4 remark dscp.....2-12
2.2.5 remark local-precedence.....2-14
2.2.6 traffic behavior.....2-14
2.3 QoS ポリシー設定コマンド.....2-15
2.3.1 classifier behavior.....2-15
2.3.2 display qos policy.....2-17
2.3.3 display qos policy interface.....2-18
2.3.4 qos apply policy (interface view).....2-20
2.3.5 qos apply policy global.....2-21
2.3.6 qos policy.....2-22

2章 QoS ポリシー

2.1 トラフィッククラス設定コマンド

2.1.1 display traffic classifier

Syntax

display traffic classifier user-defined [*classifier-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

user-defined: ユーザ定義のクラスを表示します。

classifier-name: トラフィッククラスを指定します。設定範囲は 1～31 文字です。指定しない場合、すべてのトラフィッククラスを表示します。

説明

display traffic classifier コマンドはトラフィッククラスを表示します。

例

ユーザ定義のすべてのトラフィッククラスを表示します。

<AC> display traffic classifier user-defined

```
User-defined classifier information:

 Classifier: 1 (ID 100)
   Operator: AND
   Rule(s) :
    If-match acl 2000

 Classifier: 2 (ID 101)
   Operator: AND
   Rule(s) :
    If-match not protocol ipv6
```

```
Classifier: 3 (ID 102)
  Operator: AND
  Rule(s) :
   -none-
```

表 2-1 コマンド出力

フィールド	説明
Classifier	トラフィッククラス名と一致条件です。
Operator	トラフィッククラスが一致したときの動作です。動作がANDであるとき、トラフィッククラスはすべての一致条件に一致するパケットにマッチします。動作がORであるとき、トラフィッククラスはいずれかの一致条件に一致するパケットにマッチします。
Rule(s)	一致条件です。

2.1.2 if-match

Syntax

if-match *match-criteria*

undo if-match *match-criteria*

デフォルト

設定なし

View

Traffic class view

定義済みユーザロール

network-admin

パラメータ

match-criteria: 一致条件を指定します。表 2-2 に使用可能な一致条件を示します。

表 2-2 使用可能な一致条件

オプション	説明
acl [**mac**] { *acl-number* | **name** *acl-name* }	ACLでマッチするように指定します。 *acl-number*は、ACL番号でACLを指定します。 ● IPv4 ACLの設定範囲は2000～3999です。 ● L2 ACLの設定範囲は4000～4999です。 *acl-name*は、ACL名でACLを指定します。設定範囲は1～63文字です。大文字、小文字を区別しません。文字列の最初は英字を指定します。混乱をさけるため**all**を使用してはいけません。
any	すべてのパケットにマッチするように指定します。
customer-dot1p *dot1p-value*&<1-8>	VLANタグ内の802.1p優先度の値に一致するように指定します。 *dot1p-value*は、設定範囲が0～7の802.1p優先度の値のリストです。&<1-8>を使用して最大8つの802.1p優先度の値を指定できます。
customer-vlan-id *vlan-id-list*	VLANタグ内のVLAN IDに一致するように指定します。 *vlan-id-list*は、10個までのVLANアイテムリストを指定します。各アイテムは、VLANもしくはVLANの範囲を*vlan-id1* **to** *vlan-id2*の形式で指定します。*vlan-id2*の値は*vlan-id1*の値以上にしてください。設定範囲は1～4094です。
destination-mac *mac-address*	指定した宛先MACアドレスのパケットにマッチするよう指定します。
dscp *dscp-value*&<1-8>	DSCP値あるいはキーワードでマッチするように指定します。*dscp-value*は、設定範囲が0～63のDSCP値のリストです。&<1-8>を使用して最大8つまでDSCP値を設定できます。*dscp-value*のキーワードを表 2-3に示します。
ip-precedence *ip-precedence-value*&<1-8>	パケットのIPプレシーデンスにマッチするよう指定します。*ip-precedence-value*は、設定範囲が0～7のIPプレシーデンス値のリストです。&<1-8>を使用して最大8つのIPプレシーデンス値を指定できます。
local-precedence local-*precedence-value*&<1-8>	ローカルプレシーデンスにマッチするよう指定します。 *precedence-value*は、設定範囲が0～7のIPプレシーデンス値のリストです。&<1-8>を使用して最大8つのローカルプレシーデンス値を指定できます。
protocol *protocol-name*	指定したプロトコルのパケットにマッチするように指定します。*protocol-name*はARP、BITTORRENT、IPが指定できます。
source-mac *mac-address*	指定した送信元MACアドレスのパケットにマッチするよう指定します。

表 2-3 DSCP のキーワードと値

キーワード	DSCP 値（バイナリ）	DSCP 値（10 進数）
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
default	000000	0
ef	101110	46

説明

if-match コマンドは一致条件を定義します。

undo if-match コマンドは一致条件を削除します。

複数の一致条件の **if-match** コマンドを作成する場合、クラスの演算子を OR に設定し、複数の **if-match** コマンドを使用して設定してください。

1 つの **if-match** コマンドで複数の条件を設定する場合、以下の制限とガイドラインに従ってください。

- 1 つの **if-match** コマンドで以下の一致条件を使用して最大 8 つまで指定することができます。
  - 802.1p プライオリティ
  - DSCP
  - IP プレシーデンス
  - ローカルプレシーデンス
  - VLAN ID
- 指定した値の 1 つが一致した場合、**if-match** コマンドに一致します。
- 1 つの **if-match** コマンドに設定された複数の条件を削除する場合、**undo if-match** コマンドで指定する値は **if-match** コマンドで指定された値と同一にする必要があります。設定した順番は異なっていても構いません。

ACL ベースの条件を設定する場合、以下の制限とガイドラインに従ってください。

- **if-match** コマンドに参照される ACL が存在しない場合、トラフィッククラスはハードウェアに適用することができません。
- 一致条件として同じ ACL を使用する **if-match** コマンドを 2 つ追加できます。1 つのコマンドで、名前で ACL を指定します。もう一方のコマンドで、番号で ACL を指定します。
- トラフィッククラスの ACL に拒否ルールが含まれている場合、**if-match** ステートメントは無視されます。
  - トラフィッククラスのオペレータが OR である場合、マッチングプロセスは次の if-match ステートメントで続行されます。
  - トラフィッククラスのオペレータが AND である場合、マッチングプロセスは次のトラフィッククラスで続行されます。

送信元 MAC アドレスと宛先 MAC アドレスの一致条件はイーサネットインタフェースにのみ適用されます。

例

宛先 MAC アドレスが 0050-ba27-bed3 のパケットのマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<AC> system-view

[AC] traffic classifier class1

[AC-classifier-class1] if-match destination-mac 0050-ba27-bed3

送信元 MAC アドレスが 0050-ba27-bed2 のパケットのマッチングを行うように、トラフィッククラス class2 に一致条件を定義します。

<AC> system-view

[AC] traffic classifier class2

[AC-classifier-class2] if-match source-mac 0050-ba27-bed2

VLAN タグの 802.1p プライオリティ 3 のパケットとマッチングを行うように、トラフィッククラス class1 の一致条件を定義します。

<AC> system-view

[AC] traffic classifier class1

[AC-classifier-class1] if-match customer-dot1p 3

拡張 ACL 3101 のマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<AC> system-view

[AC] traffic classifier class1

[AC-classifier-class1] if-match acl 3101

ACL 名が flow の ACL のマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<AC> system-view

[AC] traffic classifier class1

[AC-classifier-class1] if-match acl name flow

すべてのパケットのマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<AC> system-view

[AC] traffic classifier class1

[AC-classifier-class1] if-match any

DSCP が 1、6、9 のパケットのマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<AC> system-view

[AC] traffic classifier class1

[AC-classifier-class1] if-match dscp 1 6 9

IP プレシーデンスが 1、6 のパケットのマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<AC> system-view

[AC] traffic classifier class1

[AC-classifier-class1] if-match ip-precedence 1 6

ローカルプレシーデンスが 1、6 のパケットのマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<AC> system-view

[AC] traffic classifier class1

[AC-classifier-class1] if-match local-precedence 1 6

IP パケットのマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<AC> system-view

[AC] traffic classifier class1

[AC-classifier-class1] if-match protocol ip

VLAN タグの VLAN ID が 1、6、9 のパケットのマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<AC> system-view

[AC] traffic classifier class1

[AC-classifier-class1] if-match customer-vlan-id 1 6 9

2.1.3 traffic classifier

Syntax

traffic classifier *classifier-name* [**operator** { **and** | **or** }]

undo traffic classifier *classifier-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

classifier-name: トラフィッククラスを指定します。大文字と小文字を区別します。設定範囲は 1～31 文字です。

operator: トラフィッククラスの論理積 AND あるいは論理和 OR を指定するオペレータを設定します。デフォルトは論理積 AND です。

and: 論理積 AND を指定します。トラフィッククラスはすべての条件に一致したパケットのみマッチングします。

or: 論理和 OR を指定します。トラフィッククラスはいずれかの条件に一致したパケットのみマッチングします。

説明

traffic classifier コマンドはトラフィッククラスを作成し、traffic class view に移行します。

undo traffic classifier コマンドはトラフィッククラスを削除します。

例

トラフィッククラス class1 を作成します。

<AC> system-view

[AC] traffic classifier class1

[AC-classifier-class1]

関連コマンド

display traffic classifier

2.2 トラフィック動作設定コマンド

2.2.1 car

Syntax

car cir *committed-information-rate* [cbs *committed-burst-size*] [green *action* | red *action* | yellow *action*] *

undo car

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

cir *committed-information-rate*: CIR（認定情報レート）を kbps 単位で指定します。設定範囲は 8～10000000 です。

cbs *committed-burst-size*: CBS（認定バーストサイズ）を byte 単位で指定します。設定範囲は 1000～1000000000 です。

green *action*: CIR に対応するパケットに対して実施されるアクションを指定します。デフォルトはパケットを転送します。

red *action*: CIR に対応しないパケットに対して実施されるアクションを指定します。デフォルトはパケットを廃棄します。

yellow *action*: PIR に対応し、CIR に対応しないパケットに対して実施されるアクションを指定します。デフォルトはパケットを転送します。このオプションは、現在のソフトウェアバージョンではサポートされていません。

action: パケットに対して実施されるアクションを指定します。

- **discard**: パケットを廃棄します。
- **pass**: パケットを転送します。

説明

car コマンドはトラフィック動作に CAR アクションを設定します。

undo car コマンドはトラフィック動作から CAR アクションを削除します。

同一のトラフィック動作に **car** コマンドを複数設定した場合、最後に行った設定が適用されます。

例

トラフィック動作に CAR アクションを設定します。

<AC> system-view

[AC] traffic behavior database

[AC-behavior-database] car cir 200 cbs 51200 green pass

2.2.2 display traffic behavior

Syntax

display traffic behavior user-defined [*behavior-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

user-defined: ユーザ定義のトラフィック動作を表示します。

behavior-name: トラフィック動作を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。指定しない場合、すべてのトラフィック動作を表示します。

説明

display traffic behavior コマンドはトラフィック動作を表示します。

例

すべてのユーザ定義のトラフィック動作を表示します。

<AC> display traffic behavior user-defined

```
User-defined behavior information:

  Behavior: 1 (ID 100)
    Filter enable: Permit
    Marking:
      Remark dscp 3
    Committed Access Rate:
      CIR 112 (kbps), CBS 5120 (Bytes), EBS 0 (Bytes)
      Green action  : pass
      Yellow action : pass
      Red action    : discard
```

システム定義のトラフィック動作を表示します。

<AC> display traffic behavior system-defined

```
System-defined behavior information:

  Behavior: be (ID 0)
    -none-

  Behavior: af (ID 1)
    -none-

  Behavior: ef (ID 2)
    -none-

  Behavior: be-flow-based (ID 3)
    -none-
```

表 2-4 コマンド出力

フィールド	説明
Behavior	トラフィック動作の名前と内容です。
Marking	プライオリティマーキングの情報です。

フィールド	説明
Remark dscp	DSCP値をパケットに設定するアクションです。
Committed Access Rate	CARアクションの情報です。
Green action	greenパケットを適用するアクションです。
Yellow action	yellowパケットを適用するアクションです。 このフィールドは現在のソフトウェアバージョンではサポートされていません。
Red action	redパケットを適用するアクションです。
Filter enable	トラフィックフィルタリングアクションです。
none	トラフィック動作の設定はありません。

2.2.3 filter

Syntax

filter { **deny** | **permit** }

undo filter

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

deny: パケットを廃棄します。

permit: パケットを転送します。

説明

filter コマンドはトラフィック動作にトラフィックフィルタリングを設定します。

undo filter コマンドはトラフィック動作からトラフィックフィルタリングを削除します。

例

トラフィック動作 database にパケットを廃棄するトラフィックフィルタリングを設定します。

<AC> system-view

[AC] traffic behavior database

[AC-behavior-database] filter deny

2.2.4 remark dscp

Syntax

remark dscp *dscp-value*

undo remark dscp

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

green: green パケットを指定します。

red: red パケットを指定します。

yellow: yellow パケットを指定します。

dscp-value: DSCP 値あるいは DSCP のキーワードを指定します。DSCP 値の設定範囲は 0～63 です。DSCP のキーワードを表 2-5 に示します。

表 2-5 DSCP のキーワードと値

キーワード	DSCP 値（バイナリ）	DSCP 値（10 進数）
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18

キーワード	DSCP 値（バイナリ）	DSCP 値（10 進数）
default	000000	0
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
ef	101110	46

説明

remark dscp コマンドはトラフィック動作に DSCP マーキングアクションを設定します。

undo remark dscp コマンドは DSCP マーキングアクションを削除します。

例

トラフィック動作の DSCP を 6 にするアクションを設定します。

<AC> system-view

[AC] traffic behavior database

[AC-behavior-database] remark dscp 6

2.2.5 remark local-precedence

Syntax

remark local-precedence *local-precedence-value*

undo remark local-precedence

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザロール

network-admin

パラメータ

local-precedence-value: パケットに設定するローカルプレシーデンスを指定します。設定範囲は 0～7 です。

説明

remark local-precedence コマンドはトラフィック動作にローカルプレシーデンスアクションを設定します。

undo remark local-precedence コマンドはアクションを削除します。

例

トラフィック動作にローカルプレシーデンスを 2 にするアクションを設定します。

<AC> system-view

[AC] traffic behavior database

[AC-behavior-database] remark local-precedence 2

2.2.6 traffic behavior

Syntax

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

behavior-name: トラフィック動作を設定します。大文字と小文字を区別します。設定範囲は 1～31 です。

説明

traffic behavior コマンドはトラフィック動作を作成し、traffic behavior view に移行します。すでにトラフィック動作がある場合、その view に移行します。

undo traffic behavior コマンドはトラフィック動作を削除します。

例

トラフィック動作 behavior1 を作成します。

<AC> system-view

[AC] traffic behavior behavior1

[AC-behavior-behavior1]

関連コマンド

display traffic behavior

2.3 QoSポリシー設定コマンド

2.3.1 classifier behavior

Syntax

classifier *classifier-name* **behavior** *behavior-name* [**insert-before** *before-classifier-name*]

undo classifier *classifier-name*

デフォルト

設定なし

View

QoS policy view

定義済みユーザロール

network-admin

パラメータ

classifier-name: トラフィッククラスを指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

behavior-name: トラフィック動作を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

insert-before *before-classifier-name*: QoS ポリシー内の既存のトラフィッククラスの前に、新規のトラフィッククラスを挿入します。*before-classifier-name* で既存のトラフィッククラスの名前を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。**insert-before** *before-classifier-name* パラメータを指定しない場合、新規のトラフィッククラスは QoS ポリシーの最後に挿入されます。

説明

classifier behavior コマンドはトラフィック動作を QoS ポリシーのトラフィッククラスに関連づけます。

undo classifier コマンドは QoS ポリシーからトラフィッククラスを削除します。

QoS ポリシーのトラフィッククラスは 1 つのトラフィック動作にのみ関連づけることができます。

指定したトラフィッククラスあるいはトラフィック動作が存在しない場合、システムは null のトラフィッククラスまたはトラフィック動作を作成します。

undo classifier default-class コマンドは以下の動作を実行します。

- システム定義のクラス **default-class** に対する既存のクラス動作の紐付けを削除します。
- システム定義のクラス **default-class** を、システム定義の動作 **be** に紐付けます。

例

トラフィック動作 test を QoS ポリシーuser1 のトラフィッククラス database に関連づけます。

<AC> system-view

[AC] qos policy user1

[AC-qospolicy-user1] classifier database behavior test

トラフィック動作 test を QoS ポリシーuser1 のトラフィッククラス database に関連づけ、トラフィッククラス database を既存のトラフィッククラス class-a の前に挿入します。

<AC> system-view

[AC] qos policy user1

[AC-qospolicy-user1] classifier database behavior test insert-before class-a

関連コマンド

qos policy

2.3.2 display qos policy

Syntax

display qos policy user-defined [*policy-name* [**classifier** *classifier-name*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

user-defined: ユーザ定義の QoS ポリシーを表示します。

policy-name: QoS ポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。指定しない場合、すべてのユーザ定義の QoS ポリシーを表示します。

classifier *classifier-name*: トラフィッククラス名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。指定しない場合、すべてのトラフィッククラスを表示します。

説明

display qos policy コマンドは QoS ポリシーを表示します。

例

すべてのユーザ定義の QoS ポリシーを表示します。

<AC> display qos policy user-defined

```
User-defined QoS policy information:

Policy: 1 (ID 100)
 Classifier: 1 (ID 100)
   Behavior: 1
    Marking:
      Remark dscp 3
```

```
    Committed Access Rate:
      CIR 112 (kbps), CBS 5120 (Bytes), EBS 0 (Bytes)
      Green action  : pass
      Yellow action : pass
      Red action    : discard
  Classifier: 3 (ID 102)
    Behavior: 3
     -none-
```

コマンド出力は表 2-1、表 2-4 を参照してください。

2.3.3 display qos policy interface

Syntax

display qos policy interface [*interface-type interface-number*] [**inbound** | **outbound**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。インタフェースを指定しない場合、このコマンドは各インタフェースの QoS ポリシーの情報を表示します。

inbound: 受信トラフィックに適用された QoS ポリシーを表示します。

outbound: 送信トラフィックに適用された QoS ポリシーを表示します。

説明

display qos policy interface コマンドはインタフェースに適用された QoS ポリシーを表示します。

方向を指定しない場合、**inbound** と **inbound** の両方のトラフィックの QoS ポリシーを表示します。

VT インタフェースを指定する場合、VT インタフェースの各 VA インタフェースに適用された QoS ポリシーを表示します。VT インタフェースに関する QoS の情報は表示しません。

例

GigabitEthernet 1/0/1 の受信方向のトラフィックに適用された QoS ポリシーを表示します。

<AC> display qos policy interface gigabitethernet 1/0/1 inbound

```
Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: 1
   Classifier: 1
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 5120 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets) 0 (Bytes)
        Yellow packets: 0 (Packets) 0 (Bytes)
        Red packets   : 0 (Packets) 0 (Bytes)
   Classifier: 2
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match not protocol ipv6
     Behavior: 2
      Filter enable: Permit
      Marking:
        Remark mpls-exp 4
   Classifier: 3
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
```

```
 Dropped  : 0/0 (pps/bps)
Operator: AND
Rule(s) :
 -none-
Behavior: 3
 -none-
```

表 2-6 コマンド出力

フィールド	説明
Direction	インタフェースに適用されたQoSポリシーの方向です。
Matched	パケットに一致した数です。
Forwarded	統計収集期間以内に正常に転送された一致しているパケットの平均レートです。
Dropped	統計収集期間以内に廃棄された一致しているパケットの平均レートです。
Green packets	greenパケットのトラフィックの統計情報です。
Yellow packets	yellowパケットのトラフィックの統計情報です。 このフィールドは現在のソフトウェアバージョンではサポートされていません。
Red packets	redパケットのトラフィックの統計情報です。

その他のコマンド出力は表 2-1、表 2-4 を参照してください。

2.3.4 qos apply policy (interface view)

Syntax

qos apply policy *policy-name* { **inbound** | **outbound** }

undo qos apply policy *policy-name* { **inbound** | **outbound** }

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

policy-name: QoS ポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

inbound: すべてのインタフェースの受信トラフィックに適用された QoS ポリシーを適用します。

outbound: すべてのインタフェースの送信トラフィックに適用された QoS ポリシーを適用します。

説明

qos apply policy コマンドはインタフェースに QoS ポリシーを適用します。

undo qos apply policy コマンドは QoS ポリシーを削除します。

例

GigabitEthernet 1/0/1 の送信トラフィックに適用された QoS ポリシーUSER1 を適用します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] qos apply policy USER1 outbound

2.3.5 qos apply policy global

Syntax

qos apply policy *policy-name* **global** { **inbound** | **outbound** }

undo qos apply policy *policy-name* **global** { **inbound** | **outbound** }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-name: QoS ポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

inbound: すべてのインタフェースの受信パケットに適用された QoS ポリシーを適用します。

outbound: すべてのインタフェースの送信パケットに適用された QoS ポリシーを適用します。

説明

qos apply policy global コマンドはグローバルに QoS ポリシーを適用します。

undo qos apply policy global コマンドはグローバルに適用された QoS ポリシーを削除します。

グローバルに適用された QoS ポリシーは、QoS ポリシーが適用された方向に依存し、すべての受信トラフィックあるいはすべての送信トラフィックに適用します。

例

グローバルの受信トラフィックに適用された汎用 QoS ポリシー**user1** を適用します。

<AC> system-view

[AC] qos apply policy user1 global inbound

2.3.6 qos policy

Syntax

qos policy *policy-name*

undo qos policy *policy-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-name: QoS ポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

説明

qos policy コマンドは QoS ポリシーを作成し、QoS policy view に移行します。QoS ポリシーがすでに存在する場合、その view に移行します。

undo qos policy コマンドは QoS ポリシーを削除します。

undo qos policy コマンドでオブジェクトに適用されているポリシーを削除するには、最初にオブジェクトからポリシーを削除してください。

例

QoS ポリシーuser1 を作成します。

<AC> system-view

[AC] qos policy user1

[AC-qospolicy-user1]

関連コマンド

- **classifier behavior**
- **qos apply policy**

目次

このセクションのページは **8-x-x** です。

3 章 プライオリティマッピング 3-1
3.1 プライオリティマッピング設定コマンド 3-1
3.1.1 display qos map-table 3-1
3.1.2 import 3-2
3.1.3 qos map-table 3-3
3.2 ポートプライオリティ設定コマンド 3-4
3.2.1 qos priority 3-4
3.3 プライオリティトラステッドモード設定コマンド 3-5
3.3.1 display qos trust interface 3-5
3.3.2 qos trust 3-6

3章 プライオリティマッピング

3.1 プライオリティマッピング設定コマンド

3.1.1 display qos map-table

Syntax

display qos map-table [**dot11e-lp | dot1p-lp | dscp-lp | lp-dot11e | lp-dot1p | lp-dscp**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

装置は表 3-1 に示すプライオリティマッピングを適用します。

表 3-1 プライオリティマッピング

プライオリティマッピング	説明
dot11e-lp	802.11e-localプライオリティマッピングです。
dot1p-lp	802.1p-localプライオリティマッピングです。
dscp-lp	DSCP-localプライオリティマッピングです。
lp-dot11e	Local-802.11eプライオリティマッピングです。
lp-dot1p	Local-802.1pプライオリティマッピングです。
lp-dscp	Local-DSCPプライオリティマッピングです。

説明

display qos map-table コマンドはプライオリティマッピングの設定を表示します。

プライオリティマップを指定しない場合、すべてのプライオリティマッピングの設定を表示します。

例

802.1p-local プライオリティマッピングの設定を表示します。

<AC> display qos map-table dot1p-lp

```
MAP-TABLE NAME: dot1p-lp   TYPE: pre-define
IMPORT  :  EXPORT
   0    :    2
   1    :    0
   2    :    1
   3    :    3
   4    :    4
   5    :    5
   6    :    6
   7    :    7
```

表 3-2 コマンド出力

フィールド	説明
MAP-TABLE NAME	プライオリティマッピングの名前です。
TYPE	プライオリティマッピングのタイプです。
IMPORT	プライオリティマッピングの入力値です。
EXPORT	プライオリティマッピングの出力値です。

3.1.2 import

Syntax

import *import-value-list* **export** *export-value*

undo import { *import-value-list* | **all** }

デフォルト

デフォルトのプライオリティマッピングが使用されます。詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS* *“付録”* を参照してください。

View

Priority map view

定義済みユーザロール

network-admin

パラメータ

import-value-list: 入力値のリストを指定します。

export-value: 出力値を指定します。

all: プライオリティマッピングのすべてのマッピングをデフォルトに戻します。

説明

import コマンドはプライオリティマッピングのマッピングを設定します。

undo import コマンドはプライオリティマッピングの指定した、あるいはすべてのマッピングをデフォルトに戻します。

例

802.1p-drop プライオリティマッピングを設定し、802.1p のプライオリティ 4 およびプライオリティ 5 を、ドロッププライオリティ 1 にマッピングします。

<AC> system-view

[AC] qos map-table dot1p-dp

[AC-maptbl-dot1p-dp] import 4 5 export 1

関連コマンド

display qos map-table

3.1.3 qos map-table

Syntax

qos map-table { **dot11e-lp | dot1p-lp | dscp-lp | lp-dot11e | lp-dot1p | lp-dscp** }

View

System view

定義済みユーザロール

network-admin

パラメータ

パラメータの説明は表 3-1 を参照してください。

説明

qos map-table コマンドは指定した priority map view に移行します。

例

802.1p-local priority map view に移行します。

<AC> system-view

[AC] qos map-table dot1p-lp

[AC-maptbl-dot1p-lp]

関連コマンド

- **display qos map-table**
- **import**

3.2 ポートプライオリティ設定コマンド

3.2.1 qos priority

Syntax

qos priority *priority-value*

undo qos priority

デフォルト

0

View

Interface view

定義済みユーザロール

network-admin

パラメータ

priority-value: ポートプライオリティの値を指定します。設定範囲は 0～7 です。

説明

qos priority コマンドはインタフェースのポートプライオリティを変更します。

undo qos priority コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 のポートプライオリティを 2 に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] qos priority 2

関連コマンド

display qos trust interface

3.3 プライオリティトラステッドモード設定コマンド

3.3.1 display qos trust interface

Syntax

display qos trust interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースのプライオリティのトラステッドモードとポートプライオリティの情報を表示します。

説明

display qos trust interface コマンドはインタフェースのプライオリティのトラステッドモードとポートプライオリティの情報を表示します。

例

GigabitEthernet 1/0/1 のプライオリティのトラステッドモードとポートプライオリティの情報を表示します。

<AC> display qos trust interface gigabitethernet 1/0/1

```
Interface: GigabitEthernet1/0/1
Port priority information
  Port priority: 4
  Port dot1p priority: -
  Port dscp priority: -
  Port priority trust type: dot1p
```

表 3-3 コマンド出力

フィールド	説明
Interface	インタフェースのタイプと番号です。
Port priority	インタフェースのポートプライオリティのセットです。

フィールド	説明
Port dot1p priority	ポートの802.1pプライオリティです。
Port dscp priority	ポートのDSCPプライオリティです。
Port priority trust type	インタフェースのプライオリティトラステッドモードです。**dot1p**、**dscp**、**none**があります。

3.3.2 qos trust

Syntax

qos trust { **dot1p** | **dscp** }

undo qos trust

デフォルト

インタフェースはパケットのプライオリティを信用しません。802.1p プライオリティとしてポートプライオリティを使用します。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

dot1p: プライオリティマッピングの受信パケットの 802.1p プライオリティを使用します。

dscp: プライオリティマッピングの受信パケットの DSCP を使用します。

説明

qos trust コマンドはインタフェースのプライオリティトラステッドモードを設定します。

undo qos trust コマンドはデフォルトのプライオリティのトラステッドモードに戻します。

例

GigabitEthernet 1/0/1 のプライオリティトラステッドモードを 802.1p プライオリティに設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] qos trust dot1p

関連コマンド

display qos trust interface

目次

このセクションのページは **8-x-x** です。

4 章 タイムレンジ 4-1
4.1 タイムレンジ設定コマンド 4-1
4.1.1 display time-range 4-1
4.1.2 time-range 4-2

4章 タイムレンジ

4.1 タイムレンジ設定コマンド

4.1.1 display time-range

Syntax

display time-range { *time-range-name* | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

time-range-name: タイムレンジの名前を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別しません。文字列の最初は英字を指定します。

all: 既存のすべてのタイムレンジの設定と状態を表示します。

説明

display time-range コマンドはタイムレンジの設定と状態を表示します。

例

タイムレンジ 14 の設定と状態を表示します。

<AC> display time-range t4

```
Current time is 09:40:55 5/26/2015 Tuesday

Time-range : t4 (Inactive)
 10:00 to 12:00 Mon
 14:00 to 16:00 Wed
 from 00:00 1/1/2014 to 00:00 1/1/2015
 from 00:00 6/1/2015 to 00:00 7/1/2015
```

表 4-1 コマンド出力

フィールド	説明
Current time	現在のシステム時間です。

フィールド	説明
Time-range	タイムレンジの設定と状態です。タイムレンジ名、状態（activeあるいはinactive）、開始時間、終了時間が含まれます。

4.1.2 time-range

Syntax

time-range *time-range-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }

undo time-range *time-range-name* [*start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

time-range-name: タイムレンジの名前を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別しません。文字列の最初は英字を指定します。混乱をさけるため **all** を使用してはいけません。

start-time **to** *end-time*: 周期的なタイムレンジを指定します。*start-time* と *end-time* の形式は hh:mm です。24 時間時計です。*start-time* の設定範囲は 00:00～23:59 です。*end-time* の設定範囲は 00:00～24:00 です。*end-time* は *start-time* よりも大きい値にする必要があります。

days: 周期的なタイムレンジの日時あるいは曜日を指定します。複数の値を指定する場合、スペースで区切ります。値は重複することができません。値は以下のいずれかを指定することができます。

- 0～6：それぞれ日曜日、月曜日、火曜日、水曜日、木曜日、金曜日、土曜日の設定範囲を指定します。
- **Sun**、**Mon**、**Tue**、**Wed**、**Thu**、**Fri**、**Sat**：曜日を指定します。
- **working-day**：月曜日～金曜日の営業日を指定します。
- **off-day**：土曜日、日曜日の非営業日を指定します。
- **daily**：一週間の日付を指定します。

from *time1 date1*: 絶対的なタイムレンジの開始時間と開始日を指定します。*time1* は時間を指定します。形式は hh:mm です。24 時間時計です。設定範囲は 00:00～23:59 です。*date1* は日付を指定します。形式は MM/DD/YYYY あるいは YYYY/MM/DD です。MM は 1～12 の月、*DD* は各月の日付、*YYYY* は 1970～2100 の年です。このパラメータを指定しない場合、開始時間と開始日はシステムで有効なもっとも早い時間の 01/01/1970 00:00 AM となります。

to *time2 date2*: 絶対的なタイムレンジの終了時間と終了日を指定します。*time2* は時間を指定します。形式は hh:mm です。24 時間時計です。設定範囲は 00:00～24:00 です。*date2* は日付を指定します。形式は MM/DD/YYYY あるいは YYYY/MM/DD です。MM は 1～12 の月、*DD* は各月の日付、*YYYY* は 1970～2100 の年です。このパラメータを指定しない場合、終了時間と終了日はシステムで有効なもっとも遅い時間の 12/31/2100 24:00 PM となります。

説明

time-range コマンドはタイムレンジを作成あるいは修正します。

undo time-range コマンドはタイムレンジあるいはタイムレンジのパラメータを削除します。

タイムレンジ名が既に存在する場合、タイムレンジのパラメータを追加します。

タイムレンジの複数のパラメータを作成することができます。各時間のパラメータは以下の形式の 1 つを指定することができます。

- *start-time* **to** *end-time days* の形式の周期的なパラメータを指定します。周期的なパラメータは日付あるいは曜日を周期的に繰り返します。
- *from time1 date1* **to** *time2 date2* の形式の絶対的なパラメータを指定します。一度限りで繰り返しません。
- *start-time* **to** *end-time days* **from** *time1 date1* **to** *time2 date2* の形式の組み合わせを指定します。指定した期間内で日付あるいは曜日を周期的に繰り返します。たとえば、2015 年 1 月 1 日～12 月 31 日の月曜日の 8:00～12:00 の営業時間のタイムレンジ test を指定する場合、**time-range test 08:00 to 12:00 mon from 00:00 01/01/2015 to 23:59 12/31/2015** コマンドを使用します。

周期的なパラメータを最大 32、絶対的なパラメータを最大 12 の、最大 1024 のタイムレンジを作成することができます。タイムレンジのアクティブな期間を以下のように計算します。

1) すべての周期的なタイムレンジを組み合わせます。
2) すべての絶対的なタイムレンジを組み合わせます。
3) タイムレンジのアクティブな期間として 2 つの記述の AND を行います。

例

周期的なタイムレンジ t1 を作成し、営業時間の 8:00～18:00 をアクティブな期間に設定します。

<AC> system-view

[AC] time-range t1 08:00 to 18:00 working-day

絶対的なタイムレンジ t2 を作成し、2015 年のすべてをアクティブな期間に設定します。

<AC> system-view

[AC] time-range t2 from 00:00 1/1/2015 to 24:00 12/31/2015

組み合わせのタイムレンジ t3 を作成し、2015 年の土曜日と日曜日の 8:00～12:00 をアクティブな期間に設定します。

<AC> system-view

[AC] time-range t3 08:00 to 12:00 off-day from 00:00 1/1/2015 to 24:00 12/31/2015

組み合わせのタイムレンジ t4 を作成し、2015 年の 1 月～6 月の月曜日の 10:00～12:00 と水曜日の 14:00～16:00 をアクティブな期間に設定します。

<AC> system-view

[AC] time-range t4 10:00 to 12:00 1 from 00:00 1/1/2015 to 24:00 1/31/2015

[AC] time-range t4 14:00 to 16:00 3 from 00:00 6/1/2015 to 24:00 6/30/2015

関連コマンド

display time-range

QX-W2230AC アクセスコントローラ

コマンドマニュアル

9. セキュリティ

本マニュアルは以下に示す章で構成されています。

01-AAA
02-802.1X
03-MAC アドレス認証
04-パスワード管理
05-公開鍵
06-SSH
07-PKI
08-SSL
09-接続制限の設定
10-IP ソースガード
11-ARP アタックプロテクション
12-ユーザアイソレーション
13-TCP フラグメントアタックプロテクション
14-ユーザプロファイル

目次

このセクションのページは **9-x-x** です。

1 章 AAA 1-1
1.1 AAA 設定コマンド 1-1
1.1.1 aaa session-limit 1-1
1.1.2 accounting default 1-2
1.1.3 accounting lan-access 1-3
1.1.4 accounting login 1-4
1.1.5 authentication default 1-6
1.1.6 authentication lan-access 1-7
1.1.7 authentication login 1-8
1.1.8 authorization command 1-9
1.1.9 authorization default 1-11
1.1.10 authorization lan-access 1-12
1.1.11 authorization login 1-13
1.1.12 display domain 1-15
1.1.13 domain 1-20
1.1.14 domain default enable 1-21
1.1.15 nas-id 1-22
1.1.16 state (ISP domain view) 1-23
1.2 ローカルユーザ設定コマンド 1-24
1.2.1 access-limit 1-24
1.2.2 authorization-attribute (local user view/user group view) 1-25
1.2.3 bind-attribute 1-27
1.2.4 description 1-28
1.2.5 display local-user 1-29
1.2.6 display user-group 1-34
1.2.7 group 1-36
1.2.8 local-user 1-37
1.2.9 password 1-38
1.2.10 service-type (local user view) 1-40
1.2.11 state (local user view) 1-41
1.2.12 user-group 1-42
1.3 RADIUS 設定コマンド 1-43
1.3.1 accounting-on enable 1-43
1.3.2 data-flow-format (RADIUS scheme view) 1-45
1.3.3 display radius scheme 1-46
1.3.4 display radius statistics 1-49

1.3.5 key (RADIUS scheme view) 1-51
1.3.6 nas-ip (RADIUS scheme view) 1-52
1.3.7 primary accounting (RADIUS scheme view) 1-54
1.3.8 primary authentication (RADIUS scheme view) 1-55
1.3.9 radius dscp 1-57
1.3.10 radius nas-ip 1-57
1.3.11 radius scheme 1-59
1.3.12 reset radius statistics 1-60
1.3.13 retry 1-60
1.3.14 retry realtime-accounting 1-62
1.3.15 secondary accounting (RADIUS scheme view) 1-63
1.3.16 secondary authentication (RADIUS scheme view) 1-65
1.3.17 snmp-agent trap enable radius 1-67
1.3.18 state primary 1-68
1.3.19 state secondary 1-69
1.3.20 timer quiet (RADIUS scheme view) 1-70
1.3.21 timer realtime-accounting (RADIUS scheme view) 1-71
1.3.22 timer response-timeout (RADIUS scheme view) 1-73
1.3.23 user-name-format (RADIUS scheme view) 1-74

1章 AAA

1.1 AAA設定コマンド

1.1.1 aaa session-limit

Syntax

aaa session-limit { **ftp** | **http** | **https | ssh** | **telnet** } *max-sessions*

undo aaa session-limit { **ftp** | **http** | **https | ssh** | **telnet** }

デフォルト

32

View

System view

定義済みユーザロール

network-admin

パラメータ

ftp: FTP ユーザを指定します。

http: HTTP ユーザを指定します。

https: HTTPS ユーザを指定します。

ssh: SSH ユーザを指定します。

telnet: Telnet ユーザを指定します。

max-sessions: 装置に同時に接続可能な最大接続数を指定します。FTP、SSH、Telnet の設定範囲は 1～32 です。HTTP、HTTPS の設定範囲は 1～64 です。

説明

aaa session-limit コマンドは装置に同時に接続可能な最大接続数を指定します。

undo aaa session-limit コマンドはデフォルトに戻します。

ユーザタイプの最大同時接続数が上限に到達したのち、システムは後続のユーザタイプの接続を拒否します。

例

FTP ユーザの最大同時接続数を 4 に設定します。

<AC> system-view

[AC] aaa session-limit ftp 4

1.1.2 accounting default

Syntax

accounting default { **local** [**none**] **| none | radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting default

デフォルト

local

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカルアカウンティングを実行します。

none: アカウンティングを実行しません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

accounting default コマンドは ISP ドメインのデフォルトアカウンティング方式を指定します。

undo accounting default コマンドはデフォルトに戻します。

デフォルトアカウンティング方式は、この方式をサポートするすべてのユーザで使用されます。特定のアカウンティング方式は設定されません。

ローカルアカウンティングは、ローカルユーザ接続の数を監視し、制御するためにのみ使用されます。アカウンティング機能が一般的に提供する統計機能を提供していません。

1 つのプライマリデフォルトアカウンティング方式と複数のバックアップのアカウンティング方式を指定することができます。

プライマリアカウンティングが無効であるとき、装置は、順番にバックアップのアカウンティング方式を使用します。たとえば、**accounting default radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリデフォルト RADIUS アカウンティング方式と 2 つのバックアップの方式（ローカルアカウンティング方式とアカウンティングがない方式）を指定します。装置はデフォルトで RADIUS アカウンティング方式を実行し、RADIUS サーバが無効であるときローカルアカウンティング方式を実行します。

RADIUS アカウンティング方式とローカルアカウンティング方式の両方が無効であるとき、装置はアカウンティング方式を実行しません。

例

ISP ドメイン test のデフォルトアカウンティング方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルとして設定します。

<AC> system-view

[AC] domain test

[AC-isp-test] accounting default radius-scheme rd local

関連コマンド

- **local-user**
- **radius scheme**

1.1.3 accounting lan-access

Syntax

accounting lan-access { **local** [**none**] **| none | radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting lan-access

デフォルト

LAN ユーザのアカウンティング方式はデフォルトアカウンティング方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカルアカウンティングを実行します。

none: アカウンティングを実行しません。

radius-scheme *radius-scheme-name*: RADIUS スキームを指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

accounting lan-access コマンドは LAN ユーザのアカウンティング方式を設定します。

undo accounting lan-access コマンドはデフォルトに戻します。

1 つのプライマリアカウンティング方式と複数のバックアップのアカウンティング方式を指定することができます。

プライマリアカウンティングが無効であるとき、装置は、順番にバックアップのアカウンティング方式を使用します。たとえば、**accounting lan-access radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリ RADIUS アカウンティング方式と 2 つのバックアップ方式（ローカルアカウンティング方式とアカウンティングがない方式）を指定します。装置はデフォルトで RADIUS アカウンティング方式を実行し、RADIUS サーバが無効であるときローカルアカウンティング方式を実行します。RADIUS アカウンティング方式とローカルアカウンティング方式の両方が無効であるとき、装置はアカウンティング方式を実行しません。

例

ISP ドメイン test の LAN ユーザのローカルアカウンティング方式を設定します。

<AC> system-view

[AC] domain test

[AC-isp-test] accounting lan-access local

LAN ユーザの ISP ドメイン test のアカウンティング方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルに設定します。

<AC> system-view

[AC] domain test

[AC-isp-test] accounting lan-access radius-scheme rd local

関連コマンド

- **accounting default**
- **local-user**
- **radius scheme**

1.1.4 accounting login

Syntax

accounting login { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting login

デフォルト

ログインユーザの ISP ドメインのアカウンティング方式はデフォルトアカウンティング方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカルアカウンティングを実行します。

none: アカウンティングを実行しません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

accounting login コマンドはログインユーザのアカウンティング方式を指定します。

undo accounting login コマンドはデフォルトに戻します。

FTP、SFTP ユーザのアカウンティングはサポートしていません。

1 つのプライマリアカウンティング方式と複数のバックアップのアカウンティング方式を指定することができます。

プライマリアカウンティングが無効であるとき、装置は、順番にバックアップのアカウンティング方式を使用します。たとえば、**accounting login radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリデフォルト RADIUS アカウンティング方式と 2 つのバックアップ方式（ローカルアカウンティング方式とアカウンティングがない方式）を指定します。装置はデフォルトで RADIUS アカウンティング方式を実行し、RADIUS サーバが無効であるときローカルアカウンティング方式を実行します。RADIUS アカウンティング方式とローカルアカウンティング方式の両方が無効であるとき、装置はアカウンティング方式を実行しません。

例

ISP ドメイン test のログインユーザのローカルアカウンティングを設定します。

<AC> system-view

[AC] domain test

[AC-isp-test] accounting login local

ログインユーザの ISP ドメイン test のアカウンティング方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルに設定します。

<AC> system-view

[AC] domain test

[AC-isp-test] accounting login radius-scheme rd local

関連コマンド

- **accounting default**
- **local-user**
- **radius scheme**

1.1.5 authentication default

Syntax

authentication default { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication default

デフォルト

local

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカル認証を実行します。

none: 認証を実行しません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

authentication default コマンドは ISP ドメインのデフォルト認証方式を指定します。

undo authentication default コマンドはデフォルトに戻します。

デフォルト認証方式は、この方式をサポートするすべてのユーザで使用されます。特定の認証方式は設定されません。

1 つのプライマリデフォルト認証方式と複数のバックアップの認証方式を指定することができます。

プライマリ認証が無効であるとき、装置は、順番にバックアップの認証方式を使用します。たとえば、**authentication default radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリデフォルト RADIUS 認証方式と 2 つのバックアップの方式（ローカル認証方式と認証がない方式）を指定します。装置はデフォルトで RADIUS 認証方式

を実行し、RADIUS サーバが無効であるときローカル認証方式を実行します。RADIUS 認証方式とローカル認証方式の両方が無効であるとき、装置は認証を実行しません。

例

ISP ドメイン test のデフォルト認証方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルとして設定します。

<AC> system-view

[AC] domain test

[AC-isp-test] authentication default radius-scheme rd local

関連コマンド

- **local-user**
- **radius scheme**

1.1.6 authentication lan-access

Syntax

authentication lan-access { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication lan-access

デフォルト

LAN ユーザの認証方式はデフォルト認証方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカル認証を実行します。

none: 認証を実行しません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

authentication lan-access コマンドは LAN ユーザの認証方式を設定します。

undo authentication lan-access コマンドはデフォルトに戻します。

1 つのプライマリ認証方式と複数のバックアップの認証方式を指定することができます。

プライマリ認証が無効であるとき、装置は、順番にバックアップの認証方式を使用します。たとえば、**authentication lan-access radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリアカウンティング方式を RADIUS として指定し、アカウンティング方式をローカルとなしとして順番に指定します。装置はデフォルトで RADIUS 認証方式を実行し、RADIUS サーバが無効であるときローカル認証方式を実行します。RADIUS 認証方式とローカル認証方式の両方が無効であるとき、装置は認証を実行しません。

例

ISP ドメイン test の LAN ユーザのローカル認証方式を設定します。

<AC> system-view

[AC] domain test

[AC-isp-test] authentication lan-access local

LAN ユーザの ISP ドメイン test の認証方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルに設定します。

<AC> system-view

[AC] domain test

[AC-isp-test] authentication lan-access radius-scheme rd local

関連コマンド

- **authentication default**
- **local-user**
- **radius scheme**

1.1.7 authentication login

Syntax

authentication login { **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication login

デフォルト

ログインユーザの ISP ドメインの認証方式はデフォルト認証方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカル認証を実行します。

none: 認証を実行しません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

authentication login コマンドはログインユーザの認証方式を指定します。

undo authentication login コマンドはデフォルトに戻します。

1 つのプライマリ認証方式と複数のバックアップの認証方式を指定することができます。

プライマリ認証が無効であるとき、装置は、順番にバックアップの認証方式を使用します。たとえば、**authentication login radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリデフォルト RADIUS 認証方式と 2 つのバックアップ方式（ローカル認証方式と認証がない方式）を指定します。装置はデフォルトで RADIUS 認証方式を実行し、RADIUS サーバが無効であるときローカル認証方式を実行します。RADIUS 認証方式とローカル認証方式の両方が無効であるとき、装置は認証を実行しません。

例

ISP ドメイン test のログインユーザのローカル認証を設定します。

<AC> system-view

[AC] domain test

[AC-isp-test] authentication login local

ログインユーザの ISP ドメイン test の認証方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルに設定します。

<AC> system-view

[AC] domain test

[AC-isp-test] authentication login radius-scheme rd local

関連コマンド

- **authentication default**
- **local-user**
- **radius scheme**

1.1.8 authorization command

Syntax

authorization command { **local** [**none**] | **none** }

undo authorization command

デフォルト

ISP ドメインのコマンド許可（認可）方式はデフォルト許可方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカル許可を実行します。

none: 許可を実行しません。許可サーバは、入力されたコマンドがユーザロールで許可されているかどうかを確認しません。ユーザロールがコマンドを許可している場合、コマンドが正常に実行されます。

説明

authorization command コマンドはコマンドの許可方式を指定します。

undo authorization command コマンドはデフォルトに戻します。

入力された各コマンドが許可されているかどうか確認するため、コマンド許可は、許可サーバを使用しログインユーザが入力可能なコマンドのみを実行できるように制限します。

ローカルコマンド許可が設定されているとき、装置は入力された各コマンドとユーザの設定を比較します。ユーザの許可されたユーザロールによって許可されるときのみ、コマンドが実行されます。

実行できるコマンドは、ユーザロールのアクセス許可と許可サーバのコマンド許可の両方で管理されます。アクセス許可の管理は、許可されたユーザロールが入力されたコマンドにアクセスできるかどうかを管理しますが、ユーザロールがこれらのコマンドに許可を取得したかどうかを管理しません。コマンドがアクセス許可によって許可されるが、コマンド許可で許可されていない場合、コマンドは実行できません。

1 つのプライマリコマンド許可方式と複数のバックアップのコマンド許可方式を指定することができます。

デフォルト許可方式が無効であるとき、装置は、順番にバックアップの許可方式を使用します。たとえば、**authorization command local none** コマンドはプライマリデフォルトローカル許可方式と 1 つのバックアップ方式（認証がない方式）を指定します。装置はデフォルトでローカル許可方式を実行し、ローカル許可方式が無効であるとき装置は許可を実行しません。

例

ISP ドメイン test の LAN ユーザのローカルコマンド許可方式を設定します。

<AC> system-view

[AC] domain test

[AC-isp-test] authorization command local

関連コマンド

local-user

1.1.9 authorization default

Syntax

authorization default { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization default

デフォルト

local

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカル許可を実行します。

none: 許可を実行しません。ユーザが認証にパスしたのち、以下のデフォルト許可情報を適用します。

- ログインユーザがネットワークにアクセスできません。
- ログインユーザはユーザロール Level-0 に割り当てられています。ログインユーザは Telnet、FTP、SFTP、端末ユーザです。端末ユーザはコンソールポートを使用して装置にアクセスできます。
- FTP、SFTP ユーザが作業ディレクトリとして設定した NAS のルートディレクトリを持っていますが、ユーザはルートディレクトリへのアクセス権限がありません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

authorization default コマンドは ISP ドメインのデフォルト許可方式を指定します。

undo authorization default コマンドはデフォルトに戻します。

デフォルト許可方式は、この方式をサポートするすべてのユーザで使用されます。特定の許可方式は設定されません。

ISP ドメインの認証方式と許可方式が同じ RADIUS スキームを使用するときのみ RADIUS 許可が適用されます。

1 つのプライマリデフォルト許可方式と複数のバックアップの許可方式を指定することができます。

プライマリ許可が無効であるとき、装置は、順番にバックアップの許可方式を使用します。たとえば、**authorization default radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリデフォルト RADIUS 許可方式と 2 つのバックアップの方式（ローカル許可方式と許可がない方式）を指定します。装置はデフォルトで RADIUS 許可方式を実行し、RADIUS サーバが無効であるときローカル許可方式を実行します。RADIUS 許可方式とローカル許可方式の両方が無効であるとき、装置は許可を実行しません。

例

ISP ドメイン test のデフォルト許可方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルとして設定します。

<AC> system-view

[AC] domain test

[AC-isp-test] authorization default radius-scheme rd local

関連コマンド

- **local-user**
- **radius scheme**

1.1.10 authorization lan-access

Syntax

authorization lan-access { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization lan-access

デフォルト

LAN ユーザの許可方式はデフォルト許可方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカル許可を実行します。

none: 許可を実行しません。認証された LAN ユーザは直接ネットワークにアクセスします。

radius-scheme *radius-scheme-name*: RADIUS スキームを指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

authorization lan-access コマンドは LAN ユーザの許可方式を設定します。

undo authorization lan-access コマンドはデフォルトに戻します。

ISP ドメインの認証方式と許可方式が同じ RADIUS スキームを使用するときのみ RADIUS 許可が適用されます。

1 つのプライマリ許可方式と複数のバックアップの許可方式を指定することができます。

プライマリ許可が無効であるとき、装置は、順番にバックアップの許可方式を使用します。たとえば、**authorization lan-access radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリ RADIUS 許可方式と 2 つのバックアップ方式（ローカル許可方式と許可がない方式）を指定します。装置はデフォルトで RADIUS 許可方式を実行し、RADIUS サーバが無効であるときローカル許可方式を実行します。RADIUS 許可方式とローカル許可方式の両方が無効であるとき、装置は許可を実行しません。

例

ISP ドメイン test の LAN ユーザのローカル許可方式を設定します。

<AC> system-view

[AC] domain test

[AC-isp-test] authorization lan-access local

LAN ユーザの ISP ドメイン test の許可方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルに設定します。

<AC> system-view

[AC] domain test

[AC-isp-test] authorization lan-access radius-scheme rd local

関連コマンド

- **authorization default**
- **local-user**
- **radius scheme**

1.1.11 authorization login

Syntax

authorization login { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization login

デフォルト

ログインユーザの ISP ドメインの許可方式はデフォルト許可方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカル許可を実行します。

none: 許可を実行しません。ユーザが認証にパスしたのち、以下のデフォルト許可情報を適用します。

- ログインユーザはユーザロール Level-0 に割り当てられています。ログインユーザは Telnet、FTP、SFTP、端末ユーザです。端末ユーザはコンソールポートを使用して装置にアクセスできます。
- FTP、SFTP ユーザが作業ディレクトリとして設定した NAS のルートディレクトリを持っていますが、ユーザはルートディレクトリへのアクセス権限がありません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

authorization login コマンドはログインユーザの許可方式を指定します。

undo authorization login コマンドはデフォルトに戻します。

ISP ドメインの認証方式と許可方式が同じ RADIUS スキームを使用するときのみ RADIUS 許可が適用されます。

1 つのプライマリ許可方式と複数のバックアップの許可方式を指定することができます。

プライマリ許可が無効であるとき、装置は、順番にバックアップの許可方式を使用します。たとえば、**authorization login radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリデフォルト RADIUS 許可方式と 2 つのバックアップ方式（ローカル許可方式と許可がない方式）を指定します。装置はデフォルトで RADIUS 許可方式を実行し、RADIUS サーバが無効であるときローカル許可方式を実行します。RADIUS 許可方式とローカル許可方式の両方が無効であるとき、装置は許可を実行しません。

例

ISP ドメイン test のログインユーザのローカル許可を設定します。

<AC> system-view

[AC] domain test

[AC-isp-test] authorization login local

ログインユーザの ISP ドメイン test の許可方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルに設定します。

<AC> system-view

[AC] domain test

[AC-isp-test] authorization login radius-scheme rd local

関連コマンド

- **authorization default**
- **local-user**
- **radius scheme**

1.1.12 display domain

Syntax

display domain [*isp-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

isp-name: ISP ドメイン名を指定します。設定範囲は 1～255 です。大文字、小文字を区別しません。ISP ドメインを指定しない場合、すべての ISP ドメインの設定を表示します。

説明

display domain コマンドは ISP ドメインの設定を表示します。

例

すべての ISP ドメインの設定を表示します。

<AC> display domain

```
Total 2 domains

Domain: system
  State: Active
  Default authentication scheme:  Local
```

```
  Default authorization  scheme:  Local
  Default accounting    scheme:  Local
  Accounting start failure action: Online
  Accounting update failure action: Online
  Accounting quota out action: Offline
  Service type: HSI
  Session time: Exclude idle time
  DHCPv6-follow-IPv6CP timeout: 60 seconds
  Authorization attributes :
    Idle-cut: Disabled
    Session timeout: Disabled
    IGMP access number: 4
    MLD access number:  4

Domain: dm
  State: Active
  Login   authentication scheme:  RADIUS=rad
  Login   authorization  scheme:  RADIUS=rad
  Super   authentication scheme:  RADIUS=rad
  PPP    accounting    scheme:  RADIUS=r1, (RADIUS=r2), Local
  Command authorization  scheme:  Local
  LAN access authentication scheme:  RADIUS=r4
  Portal  authentication scheme:  LDAP=ldp
  Default authentication scheme:  LDAP=rad, Local, None
  Default authorization  scheme:  Local
  Default accounting    scheme:  None
  Accounting start failure action: Online
  Accounting update failure action: Online
  Accounting quota out action: Offline
  ITA service poilcy: ita1
  Service type: HSI
  Session time: Include idle time
  User basic service IP type: IPv4 IPv6 IPv6-PD
  DHCPv6-follow-IPv6CP timeout: 60 seconds
  Authorization attributes :
    Idle-cut : Enabled
      Idle timeout: 2 minutes
      Flow: 10240 bytes
    Session timeout: 34 minutes
    IP pool: appy
    User profile: test
    ACL number: 3000
    User group: ugg
```

```
    IPv6 prefix: 1::1/34
    IPv6 pool: ipv6pool
    Primary DNS server: 6.6.6.6
    Secondary DNS server: 3.6.2.3
    URL: http://portal
    IGMP access number: 12
    MLD access number: 35

Default domain name: system
```

表 1-1 コマンド出力

フィールド	説明
Domain	ISP ドメイン名です。
State	ISP ドメインの状態です。
Default authentication scheme	デフォルト認証方式です。
Default authorization scheme	デフォルト許可方式です。
Default accounting scheme	デフォルトアカウンティング方式です。
Accounting start failure action	アカウンティング開始の失敗となるユーザのアクセス制御です。 ● **Online**–ユーザがオンライン状態のままとなることを許可します。 ● **Offline**–ユーザをログオフします。
Accounting update failure max-times	ドメインの各ユーザによって、許可されたアカウンティングアップデートが連続して失敗する最大数です。
Accounting update failure action	すべてのアカウンティングアップデート試行に失敗したユーザのアクセス制御です。 ● **Online**–ユーザがオンライン状態のままとなることを許可します。 ● **Offline**–ユーザをログオフします。
Accounting quota out action	データ割り当てを使い果たしたユーザの制御です。 ● **Online**–ユーザがオンライン状態のままとなることを許可します。 ● **Offline**–ユーザをログオフします。
ITA service policy	ISP ドメインに適用されるITAポリシーです。
Service type	ISP ドメインのサービスタイプです。HIS、STB、VoIPがあります。

フィールド	説明
Session time	接続失敗あるいは誤動作によって、ユーザがオフラインとなったため、オンライン時間がサーバに送信されました。 • **Include idle time**–オンライン時間にアイドルカット期間が含まれます。 • **Exclude idle time**–オンライン時間にアイドルカット期間が含まれません。
User basic service IP type	PPPoEユーザが基本サービスを使用するために使用するIPアドレスの種類です。 • **IPv4**. • **IPv6**. • **IPv6-PD**.
DHCPv6-follow-IPv6CP timeout	PPPoEユーザのIPv6CPネゴシエーションが開始した後、DHCPv6要求タイムアウトタイマです。単位は秒です。
Login authentication scheme	ログインユーザに対する認証方法です。
Login authorization scheme	ログインユーザに対する許可方法です。
Login accounting scheme	ログインユーザに対するアカウンティング方法です。
Authorization attributes	ISPドメインのユーザの許可属性です。
Idle-cut	アイドルカット機能の状態です。 • **Enabled**–アイドルカット機能が有効です。装置は、アイドルタイムアウト期間内で最小のトラフィック要求を満たさないユーザをログオフします。 • **Disabled**–アイドルカット機能が無効です。デフォルトのアイドルカット状態です。
Idle timeout	アイドルタイムアウト期間です。単位は分です。
Flow	アイドルタイムアウト期間内にログインユーザが生成しなければならない最小トラフィックです。単位はbyteです。
Session timeout	ユーザのセッションタイムアウトタイマ（分）です。
IP pool	ユーザで許可されたIPv4アドレスプール名です。
User profile	許可ユーザプロファイル名です。
ACL number	ユーザの許可ACLです。
User group	ユーザの許可ユーザグループです。
IPv6 prefix	ユーザで許可されたIPv6アドレスのプレフィックスです。

フィールド	説明
IPv6 pool	ユーザで許可されたIPv6アドレスプール名です。
Primary DNS server	ユーザのプライマリDNSサーバのIPアドレスです。
Secondary DNS server	ユーザのセカンダリDNSサーバのIPアドレスです。
URL	ユーザのリダイレクトURLです。
IGMP max access number	IPv4ユーザが同時に加入できるIGMPグループの最大数です。
MLD max access number	IPv6ユーザが同時に加入できるMLDグループの最大数です。
RADIUS	RADIUSスキームです。
Local	ローカルスキームです。
None	認証、許可、アカウンティングがありません。
Super authentication scheme	装置に再接続を行わず別のユーザロールを取得する認証方式です。
PPP authentication scheme	PPPユーザの認証方法です。
PPP authorization scheme	PPPユーザの許可方法です。
PPP accounting scheme	PPPユーザのアカウンティング方法です。
Command authorization scheme	コマンドライン認証方法です。
LAN access authentication scheme	LANユーザの認証方法です。
LAN access authorization scheme	LANユーザの許可方法です。
LAN access accounting scheme	LANユーザのアカウンティング方法です。
Portal authentication scheme	portalユーザの認証方法です。
Portal authorization scheme	portalユーザの許可方法です。
Portal accounting scheme	portalユーザのアカウンティング方法です。
IKE authentication scheme	IKE拡張認証方法です。
IKE authorization scheme	IKE拡張認証の承認方法です。

1.1.13 domain

Syntax

domain *isp-name*

undo domain *isp-name*

デフォルト

system

View

System view

定義済みユーザロール

network-admin

パラメータ

isp-name: ISP ドメイン名を指定します。設定範囲は 1～255 です。大文字、小文字を区別しません。

次の記号は使用できません。スラッシュ（/），バックスラッシュ、垂直バー（|）、コーテーションマーク（"）、コロン（:）、アスタリスク（*）、クエスチョンマーク（?）、小なり記号（<）、大なり記号（>）、アットマーク（@）

次のドメイン名は使用できません。(d)、(de)(def)、(defa)、(defau)、(defaul)、(default)、(i)、(if)、(if-)、(if-u)、(if-un)、(if-unk)、(if-unkn)、(if-unkno)、(if-unknow)、(if-unknown)

説明

domain コマンドは ISP ドメインを作成し、ISP domain view に移行します。ISP ドメインが既に存在する場合、その view に移行します。

undo domain コマンドは ISP ドメインを削除します。

作成されたとき、すべての ISP ドメインはアクティブ状態です。

システムには予約済み ISP ドメイン system があり、修正できますが削除することはできません。

デフォルト ISP ドメインは、削除することができません。**undo domain** コマンドを使用する前に、**undo domain default enable** コマンドを使用して、デフォルトでない ISP ドメインを変更してください。

ドメイン名を含むユーザ名は、異なるタイプのユーザの最大長を超過しないように短いユーザ名を使用してください。

例

ISP ドメイン test を作成し、ISP domain view に移行します。

<AC> system-view

[AC] domain test

[AC-isp-test]

関連コマンド

- **display domain**
- **domain default enable**
- **domain if-unknown**
- **state (ISP domain view)**

1.1.14 domain default enable

Syntax

domain default enable *isp-name*

undo domain default enable

デフォルト

system

View

System view

定義済みユーザロール

network-admin

パラメータ

isp-name: ISP ドメイン名を指定します。設定範囲は 1～255 です。大文字、小文字を区別しません。ISP ドメインは既に存在している必要があります。

説明

domain default enable コマンドはデフォルト ISP ドメインを指定します。ドメイン名が付加されないユーザは、デフォルトドメインであるとみなします。

undo domain default enable コマンドはデフォルトに戻します。

デフォルトの ISP ドメインは 1 つしかありません。

デフォルトの ISP ドメインは、削除することができません。**undo domain** コマンドを使用する前に、**undo domain default enable** コマンドを使用して、デフォルトでない ISP ドメインを変更してください。

例

ISP ドメイン test を作成し、デフォルト ISP ドメインとして設定します。

<AC> system-view

[AC] domain test

[AC-isp-test] quit

[AC] domain default enable test

関連コマンド

- **display domain**
- **domain**

1.1.15 nas-id

🕮 **メモ：**

nas-id コマンドはソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

nas-id *nas-identifier*

undo nas-id

デフォルト

設定なし

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

nas-identifier: NAS-ID の文字列を指定します。この引数は大文字と小文字を区別する 1～31 文字の文字列です。

説明

nas-id コマンドはネットワークアクセスサーバ識別子（NAS ID）を設定します。

undo nas-id コマンドはデフォルトに戻します。

RADIUS 認証中、装置は NAS-ID を使用して RADIUS パケットの NAS-Identifier 属性を設定し、RADIUS サーバがユーザのアクセス場所を識別できるようにします。

装置は、次の優先順位で NAS-ID を選択します。

1.サービステンプレートを無線にバインドする時に指定した NAS-ID パラメータ

2.AP View の設定

3. AP group View の設定

4. wlan global-configuration View の設定

5. ISP ドメイン View の設定

NAS-ID が設定されていない場合、装置はデバイス名を NAS-ID として使用します。

例

ISP ドメイン test の NAS-ID を test に設定します。

<AC> system-view

[AC] domain test

[AC-isp-test] nas-id test

1.1.16 state (ISP domain view)

Syntax

state { **active** | **block** }

undo state

デフォルト

active

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

active: ISP ドメインをアクティブ状態にし、ISP ドメイン内のユーザがネットワークサービスを要求できるようにします。

block: ISP ドメインをブロック状態にし、ISP ドメイン内のユーザがネットワークサービスを要求できないようにします。

説明

state コマンドは ISP ドメインの状態を設定します。

undo state コマンドはデフォルトに戻します。

ISP ドメインをブロック状態にすると、このドメイン内のオフラインのユーザは、ネットワークサービスを要求できなくなります。オンラインユーザには影響しません。

例

ISP ドメイン test をブロック状態にします。

<AC> system-view

[AC] domain test

[AC-isp-test] state block

関連コマンド

display domain

1.2 ローカルユーザ設定コマンド

1.2.1 access-limit

Syntax

access-limit *max-user-number*

undo access-limit

デフォルト

ローカルユーザを使用して同時に接続するユーザ数に制限はありません。

View

Local user view

定義済みユーザロール

network-admin

パラメータ

max-user-number: 同時に接続するユーザの最大数です。設定範囲は 1～1024 です。

説明

access-limit コマンドはローカルユーザを使用して同時に接続するユーザの最大数を設定します。

undo access-limit コマンドはデフォルトに戻します。

ローカルユーザでローカルアカウンティングが設定されているときのみ適用されます。

FTP、SFTP ユーザはアカウンティングをサポートしていないため、FTP、SFTP ユーザには適用されません。

例

ローカルユーザ **abc** を使用して同時に接続するユーザの最大数 5 を設定します。

<AC> system-view

[AC] local-user abc

[AC-luser-manage-abc] access-limit 5

関連コマンド

display local-user

1.2.2 authorization-attribute (local user view/user group view)

Syntax

authorization-attribute { **acl** *acl-number* | **idle-cut** *minutes* | **user-profile** *profile-name* | **user-role** *role-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } *

undo authorization-attribute { **acl** | **idle-cut** | **session-timeout** | **user-profile** | **user-role** *role-name* | **vlan** | **work-directory** } *

デフォルト

FTP、SFTP ユーザは作業ディレクトリとして NAS のルートディレクトリを設定します。しかし、ユーザはルートディレクトリへのアクセス許可がありません。

network-admin あるいは level-15 のユーザによって作成されたローカルユーザは network-operator のユーザロールが割り当てられています。

View

Local user view

User group view

定義済みユーザロール

network-admin

パラメータ

acl *acl-number*: 許可 ACL を指定します。設定範囲は 2000～4999 です。認証をパスした後、ローカルユーザは ACL で指定されたネットワークリソースにアクセスすることができます。

idle-cut *minute*: アイドルタイムアウト時間を設定します。設定範囲は 1～120 分です。指定されるアイドル時間を超過したアイドル中のオンラインユーザはログアウトされます。

user-profile *profile-name*: 許可ユーザプロファイルを指定します。設定範囲は 1～31 です。大文字、小文字を区別します。ユーザプロファイル名は英字、数字、アンダーライン（_）のみ使用することができます。ユーザプロファイルは認証されたユーザの動作を制限します。

user-role *role-name*: 許可されたユーザロールを指定します。設定範囲は 1～63 です。大文字、小文字を区別します。ユーザに 64 のユーザロールを指定することができます。このオプションは local user view でのみ有効で、user group view では無効です。

vlan *vlan-id*: 許可 VLAN を指定します。設定範囲は 1～4094 です。認証にパスし、VLAN が許可されたのち、ローカルユーザは VLAN のリソースのみアクセスすることができます。

work-directory *directory-name*: FTP、SFTP ユーザの作業ディレクトリを指定します。設定範囲は 1～255 です。大文字、小文字を区別しません。このディレクトリは既に存在している必要があります。デフォルトで FTP、SFTP ユーザは装置のルートディレクトリにアクセスすることができます。

説明

authorization-attribute コマンドはローカルユーザまたはユーザグループの許可属性を設定します。ローカルユーザ、またはローカルユーザのユーザグループが認証を通過すると、装置はユーザにそれらの属性を割り当てます。

undo authorization-attribute コマンドはデフォルトに戻します。

アプリケーション環境と目的に従って許可属性を設定してください。ユーザのサービスタイプに依存して許可属性をサポートします。

LAN ユーザの場合、許可属性は ACL、ユーザプロファイル、VLAN のみが適用できます。

SSH、Telnet、端末ユーザの場合、許可属性はアイドルカット、ユーザロール、作業ディレクトリが適用できます。

HTTP、HTTPS ユーザの場合、許可属性はユーザロールが適用できます。

FTP ユーザの場合、許可属性はユーザロール、アイドルカット、ユーザロール、作業ディレクトリが適用できます。

ローカルユーザのほかのタイプは適用されません。

ユーザグループで設定された許可属性は、グループのすべてのローカルユーザに影響します。設定と管理の効率を上げるためにローカルユーザをグループ化することができます。local user view に設定する許可属性は、user group view に設定する同属性より優先されます。

ユーザが許可されたユーザロールのみ適用させるため、あらかじめ定義されたユーザロールを削除するために **undo authorization-attribute user-role** コマンドを使用してください。

例

ネットワークアクセスユーザ abc の許可される VLAN を VLAN 2 として設定します。

<AC> system-view

[AC] local-user abc class network

[AC-luser-network-abc] authorization-attribute vlan 2

ユーザグループ abc の許可される VLAN を VLAN3 として設定します。

<AC> system-view

[AC] user-group abc

[AC-ugroup-abc] authorization-attribute vlan 3

関連コマンド

- **display local-user**
- **display user-group**

1.2.3 bind-attribute

Syntax

bind-attribute { **ip** *ip-address* | **location interface** *interface-type interface-number* | **mac** *mac-address* | **vlan** *vlan-id* } *

undo bind-attribute { **ip** | **location** | **mac** | **vlan** } *

デフォルト

設定なし

View

Local user view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: ユーザの IP アドレスを指定します。このオプションは 802.1X ユーザのみ適用可能です。

location interface *interface-type interface-number*: ユーザのインタフェースを指定します。*interface-type* はインタフェースタイプ、*interface-number* はインタフェース番号を示します。認証にパスするため、ユーザはインタフェースを通してネットワークにアクセスする必要があります。このオプションは LAN、portal、PPP ユーザのみ適用可能です。

mac *mac-address*: ユーザの MAC アドレスを指定します。形式は H-H-H です。このオプションは LAN、portal、PPP ユーザのみ適用可能です。

vlan *vlan-id*: ユーザが所属する VLAN を指定します。設定範囲は 1～4094 です。このオプションは LAN、portal、PPP ユーザのみ適用可能です。

説明

bind-attribute コマンドはローカルユーザのバインディング属性を設定します。

undo bind-attribute コマンドはローカルユーザのバインディング属性を削除します。

ユーザのローカル認証を実行するため、装置はユーザの属性と設定されたバインディング属性を一致させます。ユーザが属性に一致しない、あるいは必要な属性が不足している場合、ユーザは認証に失敗します。

バインディング属性のチェックはすべてのアクセスサービスに適用します。

アクセスサービスにもとづいたユーザのバインディング属性を設定してください。装置はユーザのパケットから取得したすべての属性を確認します。たとえば、802.1X 認証はパケット内のユーザの IP アドレスを含むため、802.1X ユーザの IP アドレスのバインディング属性を設定することができます。しかし MAC アドレス認証は IP アドレスを使用しないため、MAC アドレス認証ユーザの IP アドレスのバインディング属性を設定することはできません。

バインディングするインタフェースタイプはローカルユーザの要件に合わせる必要があります。ユーザのサービスタイプにもとづいてインタフェースの割り当てを設定してください。

- ユーザが 802.1X ユーザの場合、802.1X が有効なレイヤ 2 Ethernet インタフェースを指定してください。
- ユーザが MAC アドレス認証ユーザの場合、MAC アドレス認証が有効なレイヤ 2 Ethernet インタフェースを指定してください。

例

ネットワークアクセスユーザ abc に IP アドレス 3.3.3.3 を割り当てます。

<AC> system-view

[AC] local-user abc class network

[AC-luser-network-abc] bind-attribute ip 3.3.3.3

関連コマンド

display local-user

1.2.4 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

Network access user view

定義済みユーザロール

network-admin

パラメータ

text: ネットワークアクセスユーザの説明を指定します。大文字と小文字を区別する 1 から 255 文字の文字列です。

説明

description コマンドはネットワークアクセスユーザの説明を設定します。

undo description はデフォルトに戻します。

description コマンドはネットワークアクセスユーザにだけ設定可能です。装置管理ユーザには設定できません。

例

ネットワークアクセスユーザ 123 の説明として Manager of MSC company を設定します。

<AC> system-view

[AC] local-user 123 class network

[AC-luser-network-123] description Manager of MSC company

関連コマンド

display local-user

1.2.5 display local-user

Syntax

display local-user [**class** { **manage** | **network** } | **idle-cut** { **disable** | **enable** } | **service-type** { **ftp** | **http** | **lan-access** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name* **class** { **manage** | **network** } | **vlan** *vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

class: ローカルユーザタイプを指定します。

- **manage**: 装置管理ユーザを指定します。
- **network**: ネットワークアクセスユーザを指定します。

idle-cut { **disable** | **enable** }: アイドルカット機能が有効、または無効になっているローカルユーザを指定します。

service-type: サービスの指定タイプを使用するローカルユーザを指定します。

- **ftp**: FTP ユーザを指定します。
- **http**: HTTP ユーザを指定します。
- **lan-access**: 802.1x ユーザなど、イーサネット経由でネットワークにアクセスするユーザを指定します。
- **ssh**: SSH ユーザを指定します。
- **telnet**: Telnet ユーザを指定します。
- **terminal**: コンソールポートを使用してログインする端末ユーザを指定します。

state { **active** | **block** }: アクティブまたはブロック状態にあるローカルユーザを指定します。アクティブ状態のローカルユーザは、ネットワークサービスにアクセスできます。ブロック状態のローカルユーザは認証、許可、アカウンティングサービスに要求することができません。

user-name *user-name*: 指定されたユーザ名を使用したすべてのローカルユーザを指定します。設定範囲は 1～55 です。大文字、小文字を区別します。ドメイン名を含めることはできません。

vlan *vlan-id*: VLAN のすべてのローカルユーザを指定します。設定範囲は 1～4094 です。

説明

display local-user コマンドはローカルユーザの設定、オンラインユーザの統計情報を表示します。

パラメータを指定しない場合、すべてのローカルユーザの情報を表示します。

例

すべてのローカルユーザの情報を表示します。

<AC> display local-user

```
Total 3 local users matched.


Device management user root:
 State:                Active
 Service type:          SSH/Telnet/Terminal
 Access limit:          Enabled         Max access number: 3
 Current access number:   1
 User group:            system
 Bind attributes:
 Authorization attributes:
  Work directory:        cfa0:
  User role list:        network-admin
```

```
 Password control configurations:
  Password aging:         Enabled (3 days)
Network access user jj:
 State:                 Active
 Service type:           Lan-access
 User group:             system
 Bind attributes:
  IP address:            2.2.2.2
  Location bound:         GigabitEthernet1/0/1
  MAC address:           0001-0001-0001
  VLAN ID:               2
  Calling number:         2:2
 Authorization attributes:
  Idle timeout:          33 minutes
  Work directory:         cfa0:
  ACL number:            2000
  User profile:          pp
  User role list:         network-operator, level-0, level-3
  SSL VPN policy group:    spg
Network access guest user user1:
  State:                  Active
  Service type:            LAN access/Portal
  User group:             guest1
  Full name:              Jack
  Company:                cc
  Email:                  Jack@cc.com
  Phone:                  131129237
  Description:             A guest from company cc
  Sponsor full name:        Sam
  Sponsor department:       security
  Sponsor email:           Sam@aa.com
  Validity period:
    Start date and time:    2015/04/01-08:00:00
    Expiration date and time:2015/04/03-18:00:00
```

表 1-2 コマンド出力

フィールド	説明
State	ローカルユーザの状態（アクティブまたはブロック）です。
Service type	ローカルユーザが使用可能なサービスタイプです。
Access limit	同時にログインできる接続数を制限しているかどうかを示します。

フィールド	説明
Max access number	ローカルユーザ名を使用して同時にログインする最大接続数です。
Current access number	ローカルユーザ名を使用して同時にログインしている現在の接続数です。
User group	ローカルユーザのグループです。
Bind attributes	ローカルユーザのバインディング属性です。
IP address	ローカルユーザのIPアドレスです。
Location bound	ローカルユーザのバインディングポートです。
MAC address	ローカルユーザのMACアドレスです。
VLAN ID	ローカルユーザのバインディングVLANです。
Calling number	ISDNユーザのコーリング番号です。
Authorization attributes	ローカルユーザの許可属性です。
Idle timeout	ユーザのアイドルタイムアウト時間です。単位は分です。
Callback number	ローカルユーザの許可PPPコールバック番号です。
Work directory	ユーザがアクセスできるFTP、SFTPのディレクトリです。
ACL number	ローカルユーザの許可ACLです。
VLAN ID	ローカルユーザの許可VLANです。
User profile	ローカルユーザの許可ユーザプロファイルです。
User role list	ローカルユーザの許可ロールです。
SSL VPN policy group	ローカルユーザで許可されたSSL VPNポリシーグループです。
IP address	ローカルユーザで許可されたIPv4アドレスです。
IPv6 address	ローカルユーザで許可されたIPv6アドレスです。
IPv6 prefix	ローカルユーザで許可されたIPv6アドレスプレフィックスです。
IPv6 pool	ローカルユーザで許可されたIPv6アドレスプールです。
Primary DNS server	ローカルユーザに対するプライマリDNSサーバのIPアドレスです。

フィールド	説明
Secondary DNS server	ローカルユーザに対するセカンダリDNSサーバのIPアドレスです。
URL	ローカルユーザのリダイレクトURLです。
Password control configurations	ローカルユーザで設定されるパスワード管理属性です。 このフィールドは現在のソフトウェアのバージョンではサポートされません。
Password aging	このフィールドはパスワードエージングが有効な場合のみ出現します。エージングタイマは括弧で表示されます。 このフィールドは現在のソフトウェアのバージョンではサポートされません。
Password length	このフィールドはパスワード長管理が有効な場合のみ出現します。最小のパスワード長は括弧で表示されます。 このフィールドは現在のソフトウェアのバージョンではサポートされません。
Password composition	パスワードの構成のポリシーです。 • パスワードが含まれる文字タイプの最小数です。 • パスワードの各タイプの最小文字数です。 このフィールドは現在のソフトウェアのバージョンではサポートされません。
Password complexity	パスワードの複雑性のポリシーです。 • パスワードにユーザ名あるいはユーザ名の逆の順番を使用しているかどうかを表示します。 • パスワードに文字が3回以上連続して続いているかどうかを表示します。 このフィールドは現在のソフトウェアのバージョンではサポートされません。
Maximum login attempts	連続してログインに失敗した最大数です。 このフィールドは現在のソフトウェアのバージョンではサポートされません。
Action for exceeding login attempts	ログイン試行後に、ログインに失敗したユーザへの動作です。 このフィールドは現在のソフトウェアのバージョンではサポートされません。
Full name	ローカルゲスト名です。
Company	ローカルゲストのカンパニー名です。
Email	ローカルゲストのEメールアドレスです。
Phone	ローカルアドレスの電話番号です。

フィールド	説明
Description	ネットワークアクセスユーザの説明です。
Sponsor full name	ゲストスポンサー名です。
Sponsor department	ゲストスポンサーの部門です。
Sponsor email	ゲストスポンサーのEメールアドレスです。
Validity period	ネットワークアクセスユーザの有効期間です。
Start date and time	ネットワークアクセスユーザが適用された日時です。
Expiration date and time	ネットワークアクセスユーザの有効期限が終了する日時です。

1.2.6 display user-group

Syntax

display user-group { **all** | **name** *group-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべてのユーザグループを指定します。

name *group-name*: ユーザグループ名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

display user-group コマンドはユーザグループの設定を表示します。

例

すべてのユーザグループの設定を表示します。

<AC> display user-group all

```
Total 2 user groups matched.
User group system:
  Authorization attributes:
```

```
    Work directory:         cfa0:
User group jj:
  Authorization attributes:
    Idle timeout:           2 minutes
    Callback number:         2:2
    Work directory:         cfa0:/
    ACL number:            2000
    VLAN ID:               2
  User profile:           pp
  SSL VPN policy group:    policygroup1
  Password control configurations:
    Password aging:         Enabled (2 days)
```

表 1-3 コマンド出力

フィールド	説明
Authorization attributes	ユーザグループの認可属性です。
Idle timeout	アイドルタイムアウト時間です。単位は分です。
Callback number	許可PPPコールバック番号です。
Work directory	グループのユーザがアクセスできるFTP、SFTPのディレクトリです。
ACL number	許可ACLです。
VLAN ID	許可VLANです。
User profile	許可ユーザプロファイルです。
IPv6 prefix	ユーザグループで許可されたIPv6アドレスプレフィックスです。
IPv6 pool	ユーザグループで許可されたIPv6アドレスプールです。
Primary DNS server	ユーザグループで許可されたプライマリDNSサーバのIPアドレスです。
Secondary DNS server	ユーザグループで許可されたセカンダリDNSサーバのIPアドレスです。
URL	ユーザグループのリダイレクトURLです。
Password control configurations	設定されたユーザグループのパスワード管理属性です。
Password aging	このフィールドはパスワードエージングが有効な場合のみ出現します。エージングタイマは括弧で表示されます。
Password length	このフィールドはパスワード長管理が有効な場合のみ出現します。最小のパスワード長は括弧で表示されます。

フィールド	説明
Password composition	パスワードの構成のポリシーです。 • パスワードが含まれる文字タイプの最小数です。 • パスワードの各タイプの最小文字数です。
Password complexity	パスワードの複雑性のポリシーです。 • パスワードにユーザ名あるいはユーザ名の逆の順番を使用しているかどうかを表示します。 • パスワードに文字が3回以上連続して続いているかどうかを表示します。
Maximum login attempts	連続してログインに失敗した同時接続最大数です。
Action for exceeding login attempts	ログイン試行後に、ログインに失敗したユーザへの動作です。

1.2.7 group

Syntax

group *group-name*

undo group

デフォルト

ローカルユーザはグループ system に所属しています。

View

Local user view

定義済みユーザロール

network-admin

パラメータ

group-name: ユーザグループ名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

group コマンドはユーザグループにローカルユーザを割り当てます。

undo group コマンドはデフォルトに戻します。

例

ユーザグループ abc に装置管理ユーザ 111 を割り当てます。

<AC> system-view

[AC] local-user 111 class manage

[AC-luser-manage-111] group abc

関連コマンド

display local-user

1.2.8 local-user

Syntax

local-user *user-name* [**class** { **manage** | **network** }]

undo local-user { *user-name* **class** { **manage** | **network** } | **all** [**service-type** { **ftp** | **http** | **https | lan-access** | **ssh** | **telnet** | **terminal** } | **class** { **manage** | **network** }] }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

user-name *user-name*: ローカルユーザ名を指定します。設定範囲は 1～55 です。大文字、小文字を区別します。

- ドメイン名を含めることはできません。
- スラッシュ（/），バックスラッシュ、垂直バー（|）、コロン（:）、アスタリスク（*）、クエスチョンマーク（?）、小なり記号（<）、大なり記号（>）、アットマーク（@）
- （a）、（al）、（all）は使用できません。

class: ローカルユーザタイプを指定します。指定しない場合、装置管理ユーザを指定します。

- **manage**: 装置管理ユーザを指定します。装置管理ユーザは FTP、HTTP、Telnet、SSH、端末サービスを使用することができます。
- **network**: ネットワークのリソースにアクセスするネットワークアクセスユーザを指定します。ネットワークアクセスユーザは LAN アクセスサービスを使用することができます。

all: すべてのユーザを指定します。

service-type: サービスの指定タイプを使用するローカルユーザを指定します。

- **ftp**: FTP ユーザを指定します。
- **http**: HTTP ユーザを指定します。
- **https**: HTTPS ユーザを指定します。
- **lan-access**: 802.1x ユーザなど、イーサネット経由でネットワークにアクセスするユーザを指定します。
- **ssh**: SSH ユーザを指定します。
- **telnet**: Telnet ユーザを指定します。
- **terminal**: コンソールポートを使用してログインする端末ユーザを指定します。

説明

local-user コマンドはローカルユーザを追加し、local user view に移行します。

undo local-user コマンドはローカルユーザを削除します。

例

装置管理ユーザ user1 を追加し、local user view に移行します。

<AC> system-view

[AC] local-user user1 class manage

[AC-luser-manage-user1]

ネットワークアクセスユーザ user2 を追加し、local user view に移行します。

<AC> system-view

[AC] local-user user2 class network

[AC-luser-network-user2]

関連コマンド

- **display local-user**
- **service-type**（local user view）

1.2.9 password

Syntax

ネットワークアクセスユーザ：

password { **cipher** | **simple** } *string*

undo password

装置管理ユーザ：

password [{ **hash** | **simple** } *string*]

undo password

デフォルト

ローカルユーザのパスワードは設定されていません。正しいユーザ名を入力し、属性の確認を行った後、認証にパスできます。

View

Local user view

定義済みユーザロール

network-admin

パラメータ

cipher: 暗号テキストのパスワードを設定します。

hash: ハッシュパスワードを設定します。

simple: プレーンテキストのパスワードを設定します。セキュリティのため、プレーンテキストで設定されたパスワードを含めたすべてのパスワードは、暗号化されて保存されます。

string: パスワードを指定します。大文字、小文字を区別します。

- 暗号テキストの設定範囲は 1～117 文字です。
- ハッシュテキストのパスワードは 1～110 文字です。
- プレーンテキストのパスワードは 1～63 文字です。

🕮 **メモ：**

7.2.27 を含む以降のソフトウェアでは、以下の要件を満たす *string* にしてください。

- 10 文字以上。
- アルファベット、数字、記号のうち 2 種類以上を含む。
- ユーザ名またはユーザ名の逆の文字を含まない。

7.2.21 を含む以前のソフトウェアで要件を満たしていないパスワードを設定し、7.2.27 を含む以降のソフトウェアにバージョンアップをした場合、古いパスワードのまま利用することもできますが、ログイン時にパスワードの強化が要求されます。

説明

password コマンドはローカルユーザのパスワードを設定します。

undo password コマンドはローカルユーザのパスワードを削除します。

パラメータを指定しない場合、インタラクティブモードに移行し、プレーンパスワードを設定するようにメッセージが表示されます。装置管理ユーザのみインタラクティブモードでのパスワードの設定がサポートされています。ユーザが正しいユーザ名を入力し、属性の確認にパスした場合、パスワードによるプロテクトの設定が行われていないユーザは認証をパスします。セキュリティのため、各ローカルユーザのパスワードを設定してください。

装置管理ユーザはプレーンテキストパスワードとハッシュパスワードをサポートします。ネットワークアクセスユーザはプレーンテキストパスワードと暗号テキストパスワードをサポートします。

例

装置管理ユーザ user1 のパスワード 123456TESTplat&!をプレーンテキストで設定します。

<AC> system-view

[AC] local-user user1 class manage

[AC-luser-manage-user1] password simple 123456TESTplat&!

装置管理ユーザ test のパスワードをインタラクティブモードで設定します。

<AC> system-view

[AC] local-user test class manage

[AC-luser-manage-test] password

```
Password:
Confirm :
```

ネットワークアクセスユーザ user2 のパスワード 123456TESTplat&!をプレーンテキストで設定します。

<AC> system-view

[AC] local-user user2 class network

[AC-luser-network-user2] password simple 123456TESTuser&!

関連コマンド

display local-user

1.2.10 service-type (local user view)

Syntax

service-type { **ftp** | **lan-access** | { **http** | **https** | **portal** | **ssh** | **telnet** | **terminal** } * }

undo service-type { **ftp** | **lan-access** | { **http** | **https** | **portal** | **ssh** | **telnet** | **terminal** } * }

デフォルト

ローカルユーザは許可されておらず、サービスを使用することができません。

View

Local user view

定義済みユーザロール

network-admin

パラメータ

ftp: ユーザが FTP サービスを使用することを許可します。許可されたディレクトリは **authorization-attribute work-directory** コマンドで変更することができます。

http: HTTP サービスを使用することを許可します。

https: HTTPS サービスを使用することを許可します。

lan-access: ユーザが LAN アクセスサービスを使用することを許可します。一般的にユーザは 802.1X ユーザのようなイーサネットユーザです。

portal: ユーザがポータル認証サービスを使用することを許可します。

ssh: ユーザが SSH サービスを使用することを許可します。

telnet: ユーザが Telnet サービスを使用することを許可します。

terminal: ユーザが端末サービスを使用し、コンソールポートからログインすることを許可します。

説明

service-type コマンドはローカルユーザが使用するサービスタイプを指定します。

undo service-type コマンドはローカルユーザが使用するサービスタイプを削除します。

複数のサービスタイプをユーザに割り当てることができます。

例

装置管理ユーザ user1 が Telnet、FTP サービスを使用することを許可します。

<AC> system-view

[AC] local-user user1 class manage

[AC-luser-manage-user1] service-type telnet

[AC-luser-manage-user1] service-type ftp

関連コマンド

display local-user

1.2.11 state (local user view)

Syntax

state { **active** | **block** }

undo state

デフォルト

active

View

Local user view

定義済みユーザロール

network-admin

パラメータ

active: 現在のローカルユーザをアクティブ状態にし、現在のローカルユーザがネットワークサービスを要求できるようにします。

block: 現在のローカルユーザをブロック状態にします。ブロックされたローカルユーザはネットワークサービスを要求できなくなります。

説明

state コマンドはローカルユーザの状態を設定します。

undo state コマンドはデフォルトに戻します。

例

装置管理ユーザ user1 をブロック状態にします。

<AC> system-view

[AC] local-user user1 class manage

[AC-luser-manage-user1] state block

関連コマンド

display local-user

1.2.12 user-group

Syntax

user-group *group-name*

undo user-group *group-name*

デフォルト

システム定義のユーザグループが存在します。グループ名は **system** です。

View

System view

定義済みユーザロール

network-admin

パラメータ

group-name: ユーザグループ名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

user-group コマンドはユーザグループを作成し、user group view に移行します。ユーザグループが既に存在する場合、その view に移行します。

undo user-group コマンドはユーザグループを削除します。

ユーザグループはローカルユーザのグループで構成され、ローカルユーザの属性を設定します。グループ内でローカルユーザのユーザ属性の一元管理を実装するために、ユーザグループでローカルユーザの属性を設定することができます。ローカルユーザが存在するユーザグループは削除できません。

システム定義のユーザグループ **system** の設定は変更できますが、ユーザグループは削除できません。

例

ユーザグループ abc を作成し、user group view に移行します。

<AC> system-view

[AC] user-group abc

[AC-ugroup-abc]

関連コマンド

display user-group

1.3 RADIUS設定コマンド

1.3.1 accounting-on enable

Syntax

accounting-on enable [**interval** *interval* | **send** *send-times*] *

undo accounting-on enable

デフォルト

無効

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

interval *interval*: accounting-on パケットを再送する間隔を設定します。設定範囲は 1～15 秒です。デフォルトは 3 秒です。

send *send-times*: accounting-on パケットを送信する試行回数を指定します。設定範囲は 1～255 です。デフォルトは 50 です。

説明

accounting-on enable コマンドは accounting-on 機能を有効にします。

undo accounting-on enable コマンドは accounting-on 機能を無効にします。

accounting-on 機能は装置を再起動したのち、RADIUS サーバに accounting-on パケットを自動で送信します。accounting-on パケットを受信すると RADIUS サーバは装置に対してログインできるようにすべてのオンラインユーザをログアウトします。

次回の装置の再起動時に **accounting-on enable** コマンドを適用させるため、**save** コマンドを実行してください。**save** コマンドの詳細はコマンドマニュアルのセクション 1 *はじめに “コンフィグレーションファイル管理”* を参照してください。

accounting-on enable コマンドのパラメータはコマンドを設定したのち、すぐに適用されます。

例

RADIUS スキーム radius1 で accounting-on 機能を有効にします。accounting-on パケットを再送する間隔を 5 秒に設定し、accounting-on パケットを送信する試行回数を 15 回に設定します。

<AC> system-view

[AC] radius scheme radius1

[AC-radius-radius1] accounting-on enable interval 5 send 15

関連コマンド

display radius scheme

1.3.2 data-flow-format (RADIUS scheme view)

Syntax

data-flow-format { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } } *

undo data-flow-format { **data** | **packet** }

デフォルト

データフローの単位は **byte**、データパケットの単位は **one-packet** です。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

data: データフローの単位を指定します。

byte: データフローの単位をバイトで指定します。

giga-byte: データフローの単位をギガバイトで指定します。

kilo-byte: データフローの単位をキロバイトで指定します。

mega-byte: データフローの単位をメガバイトで指定します。

packet: データパケットの単位をバイトで指定します。

giga-packet: データパケットの単位をギガバイトで指定します。

kilo-packet: データパケットの単位をキロバイトで指定します。

mega-packet: データパケットの単位をメガバイトで指定します。

one-packet: データパケットの単位を 1 パケットで指定します。

説明

data-flow-format コマンドはトラフィックの統計情報を送信する際に使用するデータフロー、またはパケットの単位を指定します。

undo data-flow-format コマンドはデフォルトに戻します。

トラフィックの統計情報を送信する際に使用するデータフロー、またはパケットの単位は RADIUS アカウンティングサーバの設定と同一にしてください。そうでなければアカウンティングは正しく実行できません。

例

RADIUS スキーム radius1 でデータフローの単位をキロバイト、パケットの単位をキロパケットに設定します。

<AC> system-view

[AC] radius scheme radius1

[AC-radius-radius1] data-flow-format data kilo-byte packet kilo-packet

関連コマンド

display radius scheme

1.3.3 display radius scheme

Syntax

display radius scheme [*radius-scheme-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

radius-scheme-name: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。RADIUS スキーム名を指定しない場合、すべての RADIUS スキームの設定が表示されます。

説明

display radius scheme コマンドは RADIUS スキームの設定を表示します。

例

すべての RADIUS スキームの設定を表示します。

<AC> display radius scheme

```
Total 1 RADIUS schemes

------------------------------------------------------------------
RADIUS scheme name  : radius1
  Index : 0
  Primary authentication server:
    IP   : 2.2.2.2                              Port: 1812
    State: Active
    Test profile: 132
      Probe username: test
      Probe interval: 60 minutes
```

```
  Primary accounting server:
    IP : 1.1.1.1                              Port: 1813
    State: Active
  Second authentication server:
    IP : 3.3.3.3                              Port: 1812
    State: Block
    Test profile: Not configured
  Second accounting server:
    IP : 3.3.3.3                              Port: 1813
    State: Block (Mandatory)
  Accounting-On function                  : Enabled
    retransmission times                  : 5
    retransmission interval(seconds)        : 2
  Timeout Interval(seconds)               : 3
  Retransmission Times                    : 3
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes)             : 5
  Realtime Accounting Interval(minutes)     : 22
  NAS IP Address                          : 1.1.1.1
  User Name Format                        : with-domain
  Data flow unit                          : Megabyte
  Packet unit                             : One
  Attribute 15 check-mode                   : Strict
  Attribute 25                            : CAR
  Attribute Remanent-Volume unit            : Mega
  Attribute 31 MAC format                   : hh:hh:hh:hh:hh:hh
------------------------------------------------------------------
```

表 1-4 コマンド出力

フィールド	説明
Index	RADIUSスキームのインデックス番号です。
Primary authentication server	プライマリ認証サーバの情報です。
Primary accounting server	プライマリアカウンティングサーバの情報です。
Second authentication server	セカンダリ認証サーバの情報です。
Second accounting server	セカンダリアカウンティングサーバの情報です。
IP	サーバのIPアドレスです。 サーバが設定されていない場合、**Not configured**と表示されます。

フィールド	説明
Port	サーバのサービスポート番号です。ポート番号が指定されていない場合、デフォルトのポート番号を表示します。
State	サーバの状態です。 ● **Active**–サーバはアクティブ状態です。 ● **Block**–サーバは自動でブロック状態に変更されました。 ● **Block (Mandatory)**–サーバを手動でブロック状態に設定しました。
Test profile	RADIUSサーバのステータス検出で使用されるテストプロファイルです。
Probe username	RADIUSサーバのステータス検出で使用されるユーザ名です。
Probe interval	サーバのステータス検出間隔です。単位は分です。
Accounting-On function	accounting-on機能が有効にされているかどうかを示します。
retransmission times	accounting-onパケット転送の試行回数です。
retransmission interval(seconds)	accounting-onパケットの再送間隔です。単位は秒です。
Timeout Interval(seconds)	RADIUSサーバ応答タイムアウト間隔です。単位は秒です。
Retransmission times	単一RADIUSサーバにRADIUSパケットを転送する最大試行回数です。
Retransmission Times for Accounting Update	アカウンティングの最大試行回数です。
Server Quiet Period(minutes)	サーバの停止間隔です。単位は分です。
Realtime Accounting Interval(minutes)	リアルタイムアカウンティングアップデートの間隔です。単位は分です。
NAS IP Address	送信するRADIUSパケットの送信元IPアドレスです。
User Name Format	RADIUSサーバに送信されたユーザ名の形式です。以下の値が含まれます。 ● **with-domain**–ドメイン名を含みます。 ● **without-domain**–ドメイン名が除外されています。 ● **keep-original**–受信されたユーザ名をそのままユーザ名として転送します。
Data flow unit	データフローの単位です。
Packet unit	データパケットの単位です。

フィールド	説明
Attribute 15 check-mode	RADIUSがSSH、FTP、端末ユーザのログインサービス属性をチェックする方式です。 ● **Strict**–SSH、FTP、端末サービスのログインサービスの属性の値がそれぞれ50、51、52に一致するかどうかを確認します。 ● **Loose**–SSH、FTP、端末サービスの標準ログインサービスの属性が0に一致するか確認します。
Attribute 25	RADIUS属性25の中断状態です。 ● **Standard**–CARパラメータとして中断しません。 ● **CAR**–CARパラメータとして中断します。
Attribute Remanent-Volume unit	RADIUS Remanent_Volume属性のデータ単位です。
Attribute 31 MAC format	RADIUS属性31のMACアドレス形式です。

1.3.4 display radius statistics

Syntax

display radius statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display radius statistics コマンドは RADIUS パケットの統計情報を表示します。

例

RADIUS パケットの統計情報を表示します。

<AC> display radius statistics

```
                        Auth.        Acct.      SessCtrl.
      Request Packet:       0            0            0
        Retry Packet:       0            0            -
      Timeout Packet:       0            0            -
    Access Challenge:       0            -            -
```

```
          Account Start:          -           0           -
         Account Update:          -           0           -
           Account Stop:          -           0           -
      Terminate Request:          -           -           0
            Set Policy:           -           -           0
    Packet With Response:         0           0           0
 Packet Without Response:         0           0           -
         Access Rejects:          0           -           -
         Dropped Packet:          0           0           0
         Check Failures:          0           0           0
```

表 1-5 コマンド出力

フィールド	説明
Auth.	認証パケットです。
Acct.	アカウンティングパケットです。
SessCtrl.	セッションコントロールパケットです。
Request Packet	パケット要求数です。
Retry Packet	パケット要求が再送された数です。
Timeout Packet	パケット要求がタイムアウトした数です。
Access Challenge	アクセスチャレンジを行ったパケット数です。
Account Start	スタートアカウンティング要求のパケット数です。
Account Update	アップデートアカウンティング要求のパケット数です。
Account Stop	ストップアカウンティング要求のパケット数です。
Terminate Request	強制的にユーザをログオフするためのパケット数です。
Set Policy	ユーザ許可情報をアップデートするパケット数です。
Packet With Response	応答が受信されたパケット数です。
Packet Without Response	応答が受信されていないパケット数です。
Access Rejects	アクセス拒否のパケット数です。
Dropped Packet	廃棄されたパケット数です。
Check Failures	チェックサムエラーのパケット数です。

関連コマンド

reset radius statistics

1.3.5 key (RADIUS scheme view)

Syntax

key { **accounting** | **authentication** } { **cipher** | **simple** } *string*

undo key { **accounting** | **authentication** }

デフォルト

設定なし

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

accounting: セキュアな RADIUS アカウンティングの通信を行うために共有キーを設定します。

authentication: セキュアな RADIUS 認証の通信を行うために共有キーを設定します。

cipher: 暗号テキストの共有キーを設定します。

simple: プレーンテキストの共有キーを設定します。セキュリティのため、プレーンテキストで設定された共有キーを含めたすべての共有キーは、暗号化されて保存されます。

string: 共有キーを指定します。大文字、小文字を区別します。

- 暗号テキストの設定範囲は 1～117 文字です。
- プレーンテキストのパスワードは 1～64 文字です。

説明

key コマンドはセキュリティの高いセキュアな RADIUS 認証、アカウンティング通信を行うために共有キーを設定します。

undo key コマンドはセキュリティの高い RADIUS 認証、アカウンティング通信を行うための共有キーを削除します。

デフォルトに戻します。

このコマンドを使用して設定された共有キーはスキームのすべてのサーバに適用されます。

例

RADIUS スキーム radius1 の共有キーok をプレーンテキストで設定します。

<AC> system-view

[AC] radius scheme radius1

[AC-radius-radius1] key accounting simple ok

関連コマンド

display radius scheme

1.3.6 nas-ip (RADIUS scheme view)

🕮 **メモ：**

ap-ip のパラメータは、ソフトウェアバージョン 7.2.93a を含む以降のソフトウェアからサポートしています。

Syntax

nas-ip { *ipv4-address* | **ap-ip** }

undo nas-ip

デフォルト

サーバへ送信されるパケットの送信元 IP アドレスは、system view の **radius nas-ip** コマンドを使用して指定されます。

radius nas-ip コマンドが設定されていない場合、送信元インタフェースのプライマリ IP アドレスがパケットの送信元 IP アドレスとなります。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: 装置の IPv4 アドレスを指定します。0.0.0.0、255.255.255.255、クラス D アドレス、クラス E アドレス、ループバックアドレスを指定することはできません。

ap-ip: RADIUS パケット内の NAS-IP アドレスとして、アクセス AP の IPv4 アドレスを使用します。このパラメータは、ワイヤレス 802.1X、ワイヤレス MAC、およびワイヤレスポータル認証ユーザーにのみ適用されます。

説明

nas-ip コマンドはサーバへ送信される RADIUS パケットの送信元アドレスを設定します。

undo nas-ip コマンドはサーバへ送信される RADIUS パケットの指定されたタイプの送信元アドレスを削除します。

NAS が送信した RADIUS パケットの送信元 IP アドレスは、RADIUS サーバに設定されている NAS の IP アドレスと一致する必要があります。RADIUS サーバは IP アドレスで NAS を識別します。RADIUS パケットを受信すると、RADIUS サーバは、パケットの送信元 IP アドレスが任意の管理 NAS の IP アドレスであるかどうかチェックします。

- パケットの送信元 IP アドレスが管理 NAS の IP アドレスと一致する場合、サーバはパケットを処理します。
- パケットの送信元 IP アドレスが管理 NAS の IP アドレスと一致しない場合、サーバはパケットを廃棄します。

送信される RADIUS パケットに送信元 IP アドレスが指定されていない場合、サーバから戻ってくるパケットは物理ポートのエラーにより装置に到達できません。サーバへ送信される RADIUS パケットの送信元アドレスとしてループバックインタフェースの IP アドレスを設定することを推奨します。

nas-ip コマンドと **radius nas-ip** コマンドの両方を使用する場合、以下のガイドラインに従います。

- RADIUS scheme view の **nas-ip** コマンドは、現在の RADIUS スキームにのみ適用されます。
- system view の **radius nas-ip** コマンドは、すべての RADIUS スキームに適用されます。
- RADIUS scheme view の **nas-ip** コマンドで設定されたコマンドは system view の **radius nas-ip** コマンドで設定されたコマンドよりも優先されます。

RADIUS スキームは発信 RADIUS パケットに対して発信元 IPv4 アドレスを 1 つだけ持つことができます。

例

RADIUS スキーム radius1 でサーバへ送信される RADIUS パケットの送信元アドレス 10.1.1.1 を設定します。

<AC> system-view

[AC] radius scheme radius1

[AC-radius-radius1] nas-ip 10.1.1.1

関連コマンド

- **display radius scheme**
- **radius nas-ip**

1.3.7 primary accounting (RADIUS scheme view)

Syntax

primary accounting *ipv4-address* [*port-number* | **key** { **cipher** | **simple** } *string*] *

undo primary accounting

デフォルト

設定なし

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: プライマリ RADIUS アカウンティングサーバの IPv4 アドレスを指定します。

port-number: プライマリ RADIUS アカウンティングサーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。デフォルトは 1813 です。

key: セキュアなプライマリ RADIUS アカウンティングサーバの通信を行うために共有キーを設定します。

cipher: 暗号テキストを指定します。

simple: プレーンテキストを指定します。セキュリティのため、プレーンテキストで設定された共有キーを含めたすべての共有キーは、暗号化されて保存されます。

string: 共有キーを指定します。大文字、小文字を区別します。暗号テキストの設定範囲は 1～117 文字です。プレーンテキストの設定範囲は 1～64 文字です。

説明

primary accounting コマンドはプライマリ RADIUS アカウンティングサーバを指定します。

undo primary accounting コマンドはプライマリ RADIUS アカウンティングサーバの設定を削除します。

プライマリ RADIUS アカウンティングサーバのポート番号と共有キーの設定は、サーバで設定された値と同一にしてください。

スキームのプライマリとセカンダリの 2 つのアカウンティングサーバでホスト名、IP アドレス、ポート番号を同一にすることはできません。

primary accounting コマンドで設定された共有キーは **key accounting** コマンドで設定された共有キーよりも優先されます。

primary accounting コマンドを使用してスタートアカウンティング要求を送信するプライマリアカウンティングサーバを修正あるいは削除する場合、プライマリサーバとの通信はタイムアウトします。

装置はアカウンティングを行うため、もっとも高い優先度のアクティブなサーバと通信をしようとします。

例

RADIUS スキーム **radius1** に IP アドレス 10.110.1.2、UDP ポート番号 1813、プレーンテキスト共有キー**123456TESTacct&!**のプライマリアカウンティングサーバを指定します。

<AC> system-view

[AC] radius scheme radius1

[AC-radius-radius1] primary accounting 10.110.1.2 1813 key simple 123456TESTacct&!

関連コマンド

- **display radius scheme**
- **key (RADIUS scheme view)**
- **secondary accounting (RADIUS scheme view)**

1.3.8 primary authentication (RADIUS scheme view)

メモ：

test-profile のパラメータは、ソフトウェアバージョン 7.2.21 を含む以降のソフトウェアからサポートしています。

Syntax

primary authentication *ipv4-address* [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name*] *

undo primary authentication

デフォルト

設定なし

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: プライマリ RADIUS 認証サーバの IPv4 アドレスを指定します。

port-number: プライマリ RADIUS 認証サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。デフォルトは 1812 です。

key: セキュアなプライマリ RADIUS サーバとのセキュア通信のための共有キーを設定します。

cipher: 暗号テキストを指定します。

simple: プレーンテキストを指定します。セキュリティのため、プレーンテキストで設定された共有キーを含めたすべての共有キーは、暗号化されて保存されます。

string: 共有キーを指定します。大文字、小文字を区別します。暗号テキストの設定範囲は 1～117 文字です。プレーンテキストの設定範囲は 1～64 文字です。

test-profile *profile-name*：RADIUS サーバの状態を検出するためのテストプロファイルを指定します。大文字と小文字を区別する 1 から 31 文字の文字列です。

説明

primary authentication コマンドはプライマリ RADIUS 認証サーバを指定します。

undo primary authentication コマンドはプライマリ RADIUS 認証サーバの設定を削除します。

プライマリ RADIUS 認証サーバのポート番号と共有キーの設定は、サーバで設定された値と同一にしてください。

スキームのプライマリとセカンダリの 2 つの認証サーバでホスト名、IP アドレス、ポート番号を同一にすることはできません。

primary authentication コマンドで設定された共有キーは **key authentication** コマンドで設定された共有キーよりも優先されます。

テストプロファイルが指定されている場合、装置は RADIUS サーバが利用可能か検出を行います。

primary authentication コマンドを使用して認証の処理中にプライマリ認証サーバを修正あるいは削除する場合、プライマリサーバとの通信はタイムアウトします。

装置は認証を行うため、もっとも高い優先度のアクティブなサーバと通信をしようとします。

例

RADIUS スキーム **radius1** に IP アドレス 10.110.1.1、UDP ポート番号 1812、プレーンテキスト共有キー**123456TESTauth&!**のプライマリ認証サーバを指定します。

<AC> system-view

[AC] radius scheme radius1

[AC-radius-radius1] primary authentication 10.110.1.1 1812 key simple 123456TESTauth&!

関連コマンド

- **display radius scheme**
- **key (RADIUS scheme view)**
- **radius-server test-profile**
- **secondary authentication (RADIUS scheme view)**

1.3.9 radius dscp

Syntax

radius dscp *dscp-value*

undo radius dscp

デフォルト

0

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: RADIUS パケットの DSCP 値を指定します。設定範囲は 0～63 です。値が大きいほど、優先度は高くなります。

説明

radius dscp コマンドは RADIUS パケットの DSCP 値を設定します。

undo radius dscp コマンドはデフォルトに戻します。

RADIUS パケットの優先度を変更するため、ToS フィールドの DSCP 値を設定します。

例

IPv4 RADIUS パケットの DSCP 値を 10 に設定します。

<AC> system-view

[AC] radius dscp 10

1.3.10 radius nas-ip

Syntax

radius nas-ip *ipv4-address*

undo radius nas-ip *ipv4-address*

デフォルト

サーバへ送信されるパケットの送信元 IP アドレスは、送信元インタフェースの IP アドレスがパケットの送信元 IP アドレスとなります。

View

System view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: 装置の IPv4 アドレスを指定します。0.0.0.0、255.255.255.255、クラス D アドレス、クラス E アドレス、ループバックアドレスを指定することはできません。

説明

radius nas-ip コマンドはサーバへ送信される RADIUS パケットの送信元アドレスを設定します。

undo radius nas-ip コマンドはサーバへ送信される RADIUS パケットの送信元アドレスを削除します。

NAS が送信した RADIUS パケットの送信元 IP アドレスは RADIUS サーバに設定されている NAS の IP アドレスと一致する必要があります。RADIUS サーバは IP アドレスで NAS を識別します。RADIUS パケットを受信すると、RADIUS サーバは、パケットの送信元 IP アドレスが任意の管理 NAS の IP アドレスであるかどうかチェックします。

- パケットの送信元 IP アドレスが管理 NAS の IP アドレスと一致する場合、サーバはパケットを処理します。
- パケットの送信元 IP アドレスが管理 NAS の IP アドレスと一致しない場合、サーバはパケットを廃棄します。

サーバへ送信される RADIUS パケットの送信元アドレスが指定されていない場合、サーバから戻ったパケットは物理ポートエラーとして装置に到着することができません。

nas-ip コマンドと **radius nas-ip** コマンドの両方を使用する場合、以下のガイドラインに従います。

- RADIUS scheme view の **nas-ip** コマンドは、現在の RADIUS スキームにのみ適用されます。
- system view の **radius nas-ip** コマンドは、すべての RADIUS スキームに適用されます。
- RADIUS scheme view の **nas-ip** コマンドで設定されたコマンドは system view の **radius nas-ip** コマンドで設定されたコマンドよりも優先されます。

新しい送信元 IPv4 アドレスを指定する場合､最後に指定されたコマンドが適用されます。

例

サーバへ送信される RADIUS パケットの送信元アドレス 129.10.10.1 を設定します。

<AC> system-view

[AC] radius nas-ip 129.10.10.1

関連コマンド

nas-ip (RADIUS scheme view)

1.3.11 radius scheme

Syntax

radius scheme *radius-scheme-name*

undo radius scheme *radius-scheme-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

radius-scheme-name: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

radius scheme コマンドは RADIUS スキームを作成し、RADIUS scheme view に移行します。

undo radius scheme コマンドは RADIUS スキームを削除します。

RADIUS スキームは、同時に 2 つ以上の ISP ドメインで使用されることがあります。

装置は最大 16 までの RADIUS スキームをサポートしています。

例

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

<AC> system-view

[AC] radius scheme radius1

[AC-radius-radius1]

関連コマンド

display radius scheme

1.3.12 reset radius statistics

Syntax

reset radius statistics

View

User view

定義済みユーザロール

network-admin

説明

reset radius statistics コマンドは、RADIUS 統計情報を削除します。

例

RADIUS 統計情報を削除します。

<AC> reset radius statistics

関連コマンド

display radius statistics

1.3.13 retry

Syntax

retry *retries*

undo retry

デフォルト

3

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

retries: RADIUS パケットの再送信の最大試行回数を設定します。設定範囲は 1～20 です。

説明

retry コマンドは 1 つの RADIUS サーバに再送 RADIUS パケットを送信する最大試行回数を設定します。

undo retry コマンドはデフォルトに戻します。

RADIUS はデータ送信に UDP パケットを使用しているため、通信に信頼性がありません。

装置が応答タイムアウト時間以内に RADIUS サーバから要求に対する応答を受信しない場合、装置は RADIUS 要求を再送します。タイムアウト時間を設定する場合、**timer response-timeout** コマンドを使用します。

再送の試行回数が上限に達しても、RADIUS サーバから応答がない場合、装置は要求が失敗したとみなします。

クライアントが認証プロセスの間にタイムアウトした場合、ユーザはすぐにログオフします。ユーザのログオフを防ぐため、以下によって乗算した値は、アクセスモジュールによって定義したクライアントのタイムアウト時間よりも大きくすることができません。

- RADIUS パケットの最大試行回数
- RADIUS サーバ応答タイムアウト時間
- RADIUS スキームの RADIUS 認証サーバ数

装置が新しい RADIUS サーバに RADIUS 要求を送信するとき、RADIUS パケットを転送する総時間を確認してください。総時間が 300 秒を超過した場合、次の RADIUS サーバへの RADIUS 要求の送信を停止します。

パケットの再送試行回数と RADIUS サーバの応答タイムアウト時間を設定する際に、RADIUS サーバの数を考慮してください。

例

RADIUS スキーム radius1 の再送 RADIUS パケットの最大試行回数を 5 に設定します。

<AC> system-view

[AC] radius scheme radius1

[AC-radius-radius1] retry 5

関連コマンド

- **radius scheme**
- **timer response-timeout (RADIUS scheme view)**

1.3.14 retry realtime-accounting

Syntax

retry realtime-accounting *retries*

undo retry realtime-accounting

デフォルト

5

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

retries: アカウンティング要求の再送信の最大試行回数を設定します。設定範囲は 1～255 です。

説明

retry realtime-accounting コマンドはアカウンティング要求を再送信する最大試行回数を設定します。

undo retry realtime-accounting コマンドはデフォルトに戻します。

通常、RADIUS アカウンティングサーバはタイムアウトタイマを使用して、ユーザがオンラインかどうかを確認します。タイムアウト時間内にサーバがリアルタイムアカウンティング要求を受信しない場合、回線または装置に不具合があるとみなします。サーバはユーザのアカウンティングを停止します。

この状況は、予期しない不具合が生じた場合に起こります。この場合、NAS は、アカウンティング要求の再送の最大試行回数に応じて、ユーザを適宜に切断するよう要求されます。最大回数に達しても応答がない場合、NAS は、ユーザを切断します。

たとえば、以下の条件があると仮定します。

- RADIUS サーバの応答タイムアウト時間が 3 秒とします。(**timer response-timeout** コマンドで設定します)
- RADIUS パケットの再送試行回数が 3 回とします。(**retry** コマンドで設定します)
- リアルタイムアカウンティング間隔が 12 分とします。(**timer realtime-accounting** コマンドで設定します。)
- アカウンティング要求を送信する最大試行回数が 5 回(**retry realtime-accounting** コマンドで設定します。)とします。

装置は 12 分ごとにアカウンティング要求を生成し、3 秒以内に応答がなければ、要求を再送します。3 回要求を送信する間に応答がなければアカウンティングは失敗とみなし、

別のアカウンティングを試行します。5 回連続してアカウンティングの送信が失敗した場合、装置はユーザ接続を切断します。

例

RADIUS スキーム radius1 のアカウンティング要求を送信する最大試行回数を 10 に設定します。

<AC> system-view

[AC] radius scheme radius1

[AC-radius-radius1] retry realtime-accounting 10

関連コマンド

- **retry**
- **timer realtime-accounting (RADIUS scheme view)**
- **timer response-timeout (RADIUS scheme view)**

1.3.15 secondary accounting (RADIUS scheme view)

Syntax

secondary accounting *ipv4-address* [*port-number* | **key** { **cipher** | **simple** } *string*] *

undo secondary accounting [*ipv4-address* [*port-number*] *]

デフォルト

設定なし

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: セカンダリ RADIUS アカウンティングサーバの IPv4 アドレスを指定します。

port-number: セカンダリ RADIUS アカウンティングサーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。デフォルトは 1813 です。

key: セキュアなセカンダリ RADIUS アカウンティングサーバの通信を行うために共有キーを設定します。

cipher: 暗号テキストを指定します。

simple: プレーンテキストを指定します。セキュリティのため、プレーンテキストで設定された共有キーを含めたすべての共有キーは、暗号化されて保存されます。

string: 共有キーを指定します。大文字、小文字を区別します。暗号テキストの設定範囲は 1～117 文字です。プレーンテキストの設定範囲は 1～64 文字です。

説明

secondary accounting コマンドはセカンダリ RADIUS アカウンティングサーバを指定します。

undo secondary accounting コマンドはセカンダリ RADIUS アカウンティングサーバを削除します。

セカンダリ RADIUS アカウンティングサーバのポート番号と共有キーの設定は、サーバで設定された値と同一にしてください。

RADIUS スキームに最大 16 のセカンダリ RADIUS アカウンティングサーバを設定することができます。プライマリサーバが故障したとき、装置はアクティブ状態のセカンダリサーバと通信しようとします。装置は設定された順番でセカンダリサーバと接続します。

スキームのプライマリとセカンダリの 2 つのアカウンティングサーバでホスト名、IP アドレス、ポート番号を同一にすることはできません。

secondary accounting コマンドで設定された共有キーは **key accounting** コマンドで設定された共有キーよりも優先されます。

secondary accounting コマンドを使用してスタートアカウンティング要求を送信するセカンダリアカウンティングサーバを修正あるいは削除する場合、セカンダリサーバとの通信はタイムアウトします。

装置はアカウンティングを行うため、もっとも高い優先度のアクティブなサーバと通信をしようとします。

もしアクティブな使用されているアカウンティングサーバを削除する場合、装置はユーザのリアルタイムアカウンティング要求とストップアカウンティング要求を送信しません。ストップアカウンティング要求を保持することはできません。

例

RADIUS スキーム radius1 に IP アドレス 10.110.1.1、UDP ポート番号 1813 のセカンダリアカウンティングサーバを指定します。

<AC> system-view

[AC] radius scheme radius1

[AC-radius-radius1] secondary accounting 10.110.1.1 1813

RADIUS スキーム radius2 の 2 つのセカンダリアカウンティングサーバの IP アドレスを 10.110.1.1 と 10.110.1.2、UDP ポートを 1813 に指定します。

<AC> system-view

[AC] radius scheme radius2

[AC-radius-radius2] secondary accounting 10.110.1.1 1813

[AC-radius-radius2] secondary accounting 10.110.1.2 1813

関連コマンド

- **display radius scheme**
- **key (RADIUS scheme view)**
- **primary accounting (RADIUS scheme view)**

1.3.16 secondary authentication (RADIUS scheme view)

メモ：

test-profile のパラメータは、ソフトウェアバージョン 7.2.21 を含む以降のソフトウェアからサポートしています。

Syntax

secondary authentication *ipv4-address* [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name*] *

undo secondary authentication [**ipv4-address** [*port-number*] *]

デフォルト

設定なし

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: セカンダリ RADIUS 認証サーバの IPv4 アドレスを指定します。

port-number: セカンダリ RADIUS 認証サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。デフォルトは 1812 です。

key: セキュアなセカンダリ RADIUS サーバとのセキュア通信のための共有キーを設定します。

cipher: 暗号テキストを指定します。

simple: プレーンテキストを指定します。セキュリティのため、プレーンテキストで設定された共有キーを含めたすべての共有キーは、暗号化されて保存されます。

string: 共有キーを指定します。大文字、小文字を区別します。暗号テキストの設定範囲は 1～117 文字です。プレーンテキストの設定範囲は 1～64 文字です。

test-profile *profile-name*：RADIUS サーバの状態を検出するためのテストプロファイルを指定します。大文字と小文字を区別する 1 から 31 文字の文字列です。

説明

secondary authentication コマンドはセカンダリ RADIUS 認証サーバを指定します。

undo secondary authentication コマンドはセカンダリ RADIUS 認証サーバの設定を削除します。

セカンダリ RADIUS 認証サーバのポート番号と共有キーの設定は、サーバで設定された値と同一にしてください。

RADIUS スキームに最大 16 のセカンダリ RADIUS 認証サーバを設定することができます。プライマリサーバが故障したとき、装置はアクティブ状態のセカンダリサーバと通信しようとします。装置は設定された順番でセカンダリサーバと接続します。

スキームのプライマリとセカンダリの 2 つの認証サーバでホスト名、IP アドレス、ポート番号を同一にすることはできません。

secondary authentication コマンドで設定された共有キーは **key authentication** コマンドで設定された共有キーよりも優先されます。

テストプロファイルが指定されている場合、装置は RADIUS サーバが利用可能か検出を行います。

secondary authentication コマンドを使用して認証の処理中にセカンダリ認証サーバを修正あるいは削除する場合、セカンダリサーバとの通信はタイムアウトします。

装置は認証を行うため、もっとも高い優先度のアクティブなサーバと通信をしようとします。

例

RADIUS スキーム radius1 に IP アドレス 10.110.1.2、UDP ポート番号 1812 のセカンダリ認証サーバを指定します。

<AC> system-view

[AC] radius scheme radius1

[AC-radius-radius1] secondary authentication 10.110.1.2 1812

RADIUS スキーム radius2 の 2 つのセカンダリ認証サーバの IP アドレスを 10.110.1.1 と 10.110.1.2、UDP ポートを 1812 に指定します。

<AC> system-view

[AC] radius scheme radius2

[AC-radius-radius2] secondary authentication 10.110.1.1 1812

[AC-radius-radius2] secondary authentication 10.110.1.2 1812

関連コマンド

- **display radius scheme**
- **key (RADIUS scheme view)**
- **radius-server test-profile**
- **primary authentication (RADIUS scheme view)**

1.3.17 snmp-agent trap enable radius

Syntax

snmp-agent trap enable radius [**accounting-server-down** | **accounting-server-up** | **authentication-error-threshold** | **authentication-server-down** | **authentication-server-up**] *

undo snmp-agent trap enable radius [**accounting-server-down** | **accounting-server-up** | **authentication-error-threshold** | **authentication-server-down** | **authentication-server-up**] *

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

accounting-server-down: RADIUS アカウンティングサーバに到達不能になったとき、notification を送信します。

accounting-server-up: RADIUS アカウンティングサーバに到達可能になったとき、notification を送信します。

authentication-error-threshold: 認証の失敗がしきい値を超過したとき、notification を送信します。しきい値は認証を試行する総数に対する認証失敗の割合を示します。設定範囲は 1～100%です。デフォルトは 30%です。しきい値は MIB を通してのみ設定できます。

authentication-server-down: RADIUS 認証サーバに到達不能になったとき、notification を送信します。

authentication-server-up: RADIUS 認証サーバに到達可能になったとき、notification を送信します。

説明

snmp-agent trap enable radius コマンドは RADIUS の SNMP notification（inform あるいはトラップ）の通知を有効にします。

undo snmp-agent trap enable radius コマンドは RADIUS の SNMP notification（inform あるいはトラップ）の通知を無効にします。

パラメータを指定しない場合、RADIUS のすべてのタイプの notification を指定します。

RADIUS の SNMP notification が有効であるとき、SNMP エージェントは RADIUS によって作成された以下の notification をサポートします。

- **RADIUS server unreachable notification**－RADIUS サーバに通信できません。指定した RADIUS 要求の再送信の最大試行回数以内にアカウンティング要求あるいは認証要求に対する応答を受信できない場合、RADIUS は notification を作成します。
- **RADIUS server reachable notification**－RADIUS サーバと通信できます。RADIUS サーバが停止タイマの満了後、以前にブロックされた RADIUS サーバに対して notification を作成します。
- **Excessive authentication failures notification**－認証を行った際、失敗した総数が指定したしきい値を超過しています。

例

装置が RADIUS アカウンティングサーバに到達不能になったとき、notification を送信します。

<AC> system-view

[AC] snmp-agent trap enable radius accounting-server-down

1.3.18 state primary

Syntax

state primary { **accounting** | **authentication** } { **active** | **block** }

デフォルト

active

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

accounting: プライマリ RADIUS アカウンティングサーバの状態を設定します。

authentication: プライマリ RADIUS 認証サーバの状態を設定します。

active: RADIUS サーバの状態を **active** に設定します。

block: RADIUS サーバの状態を **block** に設定します。

説明

state primary コマンドはプライマリ RADIUS サーバの状態を設定します。

プライマリサーバがアクティブ状態であるとき、装置は最初にプライマリサーバと通信しようとします。プライマリサーバが使用できない場合、以下の処理を行います。

- プライマリサーバの状態をブロックに変更します。
- サーバの停止タイマを開始します。
- アクティブ状態のセカンダリサーバと通信します。

プライマリサーバの停止タイマがタイムアウトすると、サーバの状態が自動的にアクティブに変化します。停止タイマがタイムアウトする前にサーバの状態をブロックに設定した場合、手動でアクティブ状態に設定しない限り、サーバが自動的にアクティブ状態に戻ることはありません。

プライマリサーバとすべてのセカンダリサーバがブロック状態であるとき、装置はプライマリサーバと通信しようとします。

例

RADIUS スキーム radius1 のプライマリ認証サーバの状態を block に設定します。

<AC> system-view

[AC] radius scheme radius1

[AC-radius-radius1] state primary authentication block

関連コマンド

- **display radius scheme**
- **state secondary**

1.3.19 state secondary

Syntax

state secondary { **accounting** | **authentication** } [*ipv4-address* [*port-number*] *] { **active** | **block** }

デフォルト

active

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

accounting: セカンダリ RADIUS アカウンティングサーバを設定します。

authentication: セカンダリ RADIUS 認証サーバを設定します。

ipv4-address: セカンダリ RADIUS サーバの IPv4 アドレスを指定します。

port-number: セカンダリ RADIUS サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。セカンダリ RADIUS 認証サーバのデフォルトは 1812 です。セカンダリ RADIUS アカウンティングサーバのデフォルトは 1813 です。

active: RADIUS サーバの状態を **active** に設定します。

block: RADIUS サーバの状態を **block** に設定します。

説明

state secondary コマンドはセカンダリ RADIUS サーバの状態を設定します。

IP アドレスが設定されていない場合、このコマンドはすべてのセカンダリサーバの状態を変更します。

装置がアクティブ状態のセカンダリサーバと通信できないことを知った場合、以下の処理を行います。

- 装置はセカンダリサーバの状態をブロックに変更します。
- サーバの停止タイマを開始します。
- 別のアクティブ状態のセカンダリサーバと通信しようとします。

サーバの停止タイマがタイムアウトとなった場合、サーバの状態は自動的にアクティブに変化します。タイマがタイムアウトする前にサーバをブロックの状態にした場合、そのサーバの状態は、手動で切り替えない限り自動的にはアクティブに戻ることはありません。すべてのセカンダリサーバが到達不能である場合、装置は認証あるいはアカウンティングに失敗します。

例

RADIUS スキーム radius1 のすべてのセカンダリ認証サーバの状態を block に設定します。

<AC> system-view

[AC] radius scheme radius1

[AC-radius-radius1] state secondary authentication block

関連コマンド

- **display radius scheme**
- **state primary**

1.3.20 timer quiet (RADIUS scheme view)

Syntax

timer quiet *minutes*

undo timer quiet

デフォルト

5 分

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

minutes: サーバの停止タイマを指定します。設定範囲は 1～255 です。

説明

timer quiet コマンドは RADIUS スキームの指定されたサーバの停止タイマを設定します。

undo timer quiet コマンドはデフォルトに戻します。

サーバの停止タイマが正しく設定されていることを確認してください。

タイマが短すぎる場合、装置がアクティブ状態の通信不能サーバと繰り返し通信しようとするため、頻繁に認証またはアカウンティングの失敗が発生します。

タイマが長すぎる場合、サーバの停止タイマが終了するまでサーバはブロック状態のままとなるため、故障から回復した到達可能なサーバを一時的にブロック状態にします。

例

RADIUS スキーム radius1 でサーバの停止タイマを 10 分に設定します。

<AC> system-view

[AC] radius scheme radius1

[AC-radius-radius1] timer quiet 10

関連コマンド

display radius scheme

1.3.21 timer realtime-accounting (RADIUS scheme view)

Syntax

timer realtime-accounting *interval*

undo timer realtime-accounting

デフォルト

12 分

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

interval: リアルタイムのアカウンティング間隔を指定します。設定範囲は 0～71582 分です。

説明

timer realtime-accounting コマンドはリアルタイムのアカウンティング間隔を設定します。

undo timer realtime-accounting コマンドはデフォルトに戻します。

装置のリアルタイムのアカウンティング間隔が 0 でないとき、装置は設定された間隔で RADIUS アカウンティングサーバにオンラインユーザのアカウンティング情報を送信します。

装置のリアルタイムのアカウンティング間隔が 0 であるとき、装置はサーバに設定されたリアルタイムのアカウンティング間隔で RADIUS アカウンティングサーバにオンラインユーザのアカウンティング情報を送信します。サーバでリアルタイムのアカウンティング間隔が設定されていない場合、装置はオンラインユーザのアカウンティング情報を送信しません。

リアルタイムのアカウンティング間隔が短いと、アカウンティング情報の精度が上がりますが、多くのシステムリソースが必要となります。

表 1-6 リアルタイムのアカウンティング間隔の推奨値

ユーザ数	リアルタイムのアカウンティング間隔
1～99	3分
100～499	6分
500～999	12分
1000以上	15分以上

例

RADIUS スキーム radius1 のリアルタイムのアカウンティング間隔を 51 分に設定します。

<AC> system-view

[AC] radius scheme radius1

[AC-radius-radius1] timer realtime-accounting 51

関連コマンド

retry realtime-accounting

1.3.22 timer response-timeout (RADIUS scheme view)

Syntax

timer response-timeout *seconds*

undo timer response-timeout

デフォルト

3 秒

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

seconds: RADIUS サーバの応答タイムアウト時間を指定します。設定範囲は 1～10 秒です。

説明

timer response-timeout コマンドは RADIUS サーバの応答タイムアウトタイマを設定します。

undo timer response-timeout コマンドはデフォルトに戻します。

RADIUS 要求を送信した後、一定時間内に RADIUS サーバから応答がない場合、NAS はユーザが多くの RADIUS サービスを受ける機会を持てるように、RADIUS リクエストを再送します。NAS は、RADIUS サーバの応答タイムアウトタイマを使用して、この送信間隔を制御します。

クライアントが認証プロセスの間にタイムアウトした場合、ユーザはすぐにログオフします。ユーザのログオフを防ぐため、以下によって乗算した値は、アクセスモジュールによって定義したクライアントのタイムアウト時間よりも大きくすることができません。

- RADIUS パケットの最大試行回数
- RADIUS サーバ応答タイムアウト時間
- RADIUS スキームの RADIUS 認証サーバ数

装置が新しい RADIUS サーバに RADIUS 要求を送信するとき、RADIUS パケットを転送する総時間を確認してください。総時間が 300 秒を超過した場合、次の RADIUS サーバへの RADIUS 要求の送信を停止します。

パケットの再送試行回数と RADIUS サーバの応答タイムアウト時間を設定する際に、RADIUS サーバの数を考慮してください。

例

RADIUS スキーム radius1 の RADIUS サーバの応答タイムアウトタイマを 5 秒に設定します。

<AC> system-view

[AC] radius scheme radius1

[AC-radius-radius1] timer response-timeout 5

関連コマンド

- **display radius scheme**
- **retry**

1.3.23 user-name-format (RADIUS scheme view)

Syntax

user-name-format { **keep-original** | **with-domain** | **without-domain** }

undo user-name-format

デフォルト

with-domain

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

keep-original: RADIUS サーバに入力するユーザ名を送信します。

with-domain: RADIUS サーバに送信されるユーザ名に、ISP ドメイン名を含めます。

without-domain: RADIUS サーバに送信されるユーザ名から ISP ドメイン名を除外します。

説明

user-name-format コマンドは RADIUS スキームの RADIUS サーバに送信されるユーザ名の形式を設定します。

undo user-name-format コマンドはデフォルトに戻します。

通常、ユーザ名の形式は *userid@isp-name* です。*isp-name* はユーザが所属する ISP ドメインを判断するために装置によって使用されます。しかし、旧型の RADIUS サーバの中には、ISP ドメイン名を含むユーザ名を認識できないものがあります。このような RADIUS サーバにドメイン名を含むユーザ名を送信する前に、装置はドメイン名を削除する必要があります。**user-name-format** コマンドを使用することで、RADIUS サーバに送信されるユーザ名にドメイン名を含めるかどうかを指定することができます。

RADIUS スキームが ISP ドメイン名を含まずにユーザ名を送信するよう定義している場合、この RADIUS スキームを複数の ISP ドメインに適用しないでください。これは、異なる 2 つの ISP ドメインに属する 2 つのユーザが、ユーザ ID が同じため、RADIUS サーバには 1 ユーザとみなされる、という混乱を避けるためです。

802.1X ユーザが EAP 認証を使用する場合、RADIUS スキームで設定された **user-name-format** コマンドは適用されません。RADIUS サーバに転送する際、装置はクライアントからユーザ名を変更できません。

RADIUS スキームが無線ユーザのローミングに使用される場合、**keep-original** パラメータを指定してください。指定しない場合、無線ユーザに認証に失敗する可能性があります。

例

RADIUS スキーム radius1 で、RADIUS サーバに送信されるユーザ名に、装置がドメイン名を削除するように指定します。

<AC> system-view

[AC] radius scheme radius1

[AC-radius-radius1] user-name-format without-domain

関連コマンド

display radius scheme

目次

このセクションのページは **9-x-x** です。

2 章 802.1X 2-1
2.1 802.1X 設定コマンド 2-1
2.1.1 display dot1x 2-1
2.1.2 display dot1x connection 2-5
2.1.3 dot1x 2-7
2.1.4 dot1x authentication-method 2-8
2.1.5 dot1x guest-vlan 2-10
2.1.6 dot1x handshake 2-11
2.1.7 dot1x handshake reply enable 2-12
2.1.8 dot1x mandatory-domain 2-12
2.1.9 dot1x max-user 2-13
2.1.10 dot1x multicast-trigger 2-14
2.1.11 dot1x port-control 2-15
2.1.12 dot1x port-method 2-16
2.1.13 dot1x quiet-period 2-17
2.1.14 dot1x re-authenticate 2-18
2.1.15 dot1x retry 2-19
2.1.16 dot1x timer 2-20
2.1.17 dot1x unicast-trigger 2-22
2.1.18 reset dot1x guest-vlan 2-23
2.1.19 reset dot1x statistics 2-24

2章 802.1X

2.1 802.1X設定コマンド

2.1.1 display dot1x

Syntax

display dot1x [**sessions** | **statistics**] [**ap** *ap-name* [**radio** *radio-id*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

sessions: 802.1X のセッション接続情報を表示します。

statistics: 802.1X の統計情報を表示します。

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

radio *radio-id*: ID で無線を指定します。*radio-id* 引数の値の範囲は、装置モデルによって異なります。無線を指定しない場合、このコマンドは指定された AP 上のすべての無線に関する 802.1X 情報を表示します。

説明

display dot1x コマンドは 802.1X についての情報を表示します。

sessions パラメータあるいは **statistics** パラメータのいずれのパラメータを指定しない場合、セッション情報、統計情報、設定情報を含む 802.1X のすべての情報を表示します。

ap *ap-name* [**radio** *radio-id*] パラメータを指定しない場合、すべての 802.1X の情報を表示します。このコマンドは、無線 802.1X 情報の前に有線 802.1X 情報を表示します。

例

802.1X のすべての情報を表示します。

<AC> display dot1x

```
Global 802.1X parameters:
  802.1X authentication  : Enabled
  CHAP authentication    : Enabled
  Max-tx period         : 30 s
  Handshake period      : 15 s
  Quiet timer           : Disabled
     Quiet period       : 60 s
  Supp timeout          : 30 s
  Server timeout        : 100 s
  Reauth period         : 3600 s
  Max auth requests     : 2
  Domain delimiter      : @
 Online 802.1X wired users    : 1
 Online 802.1X wireless users : 1

  EAPOL packets: Tx 3, Rx 3
  Sent EAP Request/Identity packets : 1
      EAP Request/Challenge packets: 1
      EAP Success packets: 1
      EAP Failure packets: 0
  Received EAPOL Start packets : 1
         EAPOL LogOff packets: 1
         EAP Response/Identity packets : 1
         EAP Response/Challenge packets: 1
         Error packets: 0
  Online 802.1X users: 1
       MAC address       Auth state
       0001-0000-0000     Authenticated
AP name: AP1  Radio ID: 1  SSID: wlan_dot1x_ssid
  BSSID                  : 1111-1111-1111
  802.1X authentication     : Enabled
  Handshake               : Enabled
  Handshake security       : Disabled
  Periodic reauth          : Disabled
  Mandatory auth domain     : Not configured
  Max online users         : 4096

  EAPOL packets: Tx 3, Rx 3
  Sent EAP Request/Identity packets : 1
```

```
    EAP Request/Challenge packets: 1
    EAP Success packets: 1
    EAP Failure packets: 0
Received EAPOL Start packets : 1
    EAPOL LogOff packets: 1
    EAP Response/Identity packets : 1
    EAP Response/Challenge packets: 1
    Error packets: 0
Online 802.1X users: 1
      MAC address       Auth state
      0001-0000-0002     Authenticated
```

表 2-1 コマンド出力

フィールド	説明
Global 802.1X parameters	グローバル802.1Xの設定です。
802.1X authentication	802.1Xがグローバルで有効かどうかを示します。
CHAP authentication	RADIUSサーバと通信する際にEAPを終端しCHAPを実行しています。 EAPまたはPAPが有効な場合、このフィールドは使用できません。
EAP authentication	RADIUSサーバと通信する際にEAPパケットの中継とEAP認証のいずれかを実行しています。 EAPまたはPAPが有効な場合、このフィールドは使用できません。
PAP authentication	RADIUSサーバと通信する際にEAPを終端しPAPを実行しています。 EAPまたはPAPが有効な場合、このフィールドは使用できません。
Max-tx period	ユーザ名の要求タイムアウトタイマです。単位は秒です。
Handshake period	ハンドシェイクタイマです。単位は秒です。
Quiet timer	停止タイマの状態をenabledあるいはdisabledで示します。
Quiet period	停止タイマです。単位は秒です。
Supp timeout	クライアントタイムアウトタイマです。単位は秒です。
Server timeout	サーバタイムアウトタイマです。単位は秒です。
Reauth period	定期再認証タイマです。単位は秒です。

フィールド	説明
Max auth requests	認証要求をクライアントに送信する最大試行回数です。
Online 802.1X wired users	有線接続されたオンライン802.1Xユーザの数です。 802.1X認証にパスしたユーザ、802.1X認証を行っているユーザ数を表示します。
Online 802.1X wireless users	無線接続されたオンライン802.1Xユーザの数です。 802.1X認証にパスしたユーザ、802.1X認証を行っているユーザ数を表示します。
EAPOL packets	EAPOLパケットの送信数（Tx）および受信数（Rx）です。
Sent EAP Request/Identity packets	EAP-Request/Identityパケットの送信数です。
EAP Request/Challenge packets	EAP-Request/MD5 Challengeパケットの送信数です。
EAP Success packets	EAP-Successパケットの送信数です。
EAP Failure packets	EAP-Failureパケットの送信数です。
Received EAPOL Start packets	EAPOL-Startパケットの受信数です。
EAPOL LogOff packets	EAPOL-LogOffパケットの受信数です。
EAP Response/Identity packets	EAP-Response/Identityパケットの受信数です。
EAP Response/Challenge packets	EAP-Response/MD5 Challengeパケットの受信数です。
Error packets	エラーパケットの受信数です。
Online 802.1X users	ポートのオンライン802.1Xユーザ数です。
MAC address	オンライン802.1XユーザのMACアドレスです。
Auth state	オンライン802.1Xユーザの認証状態です。
AP name	ユーザが関連付けられているAPの名前です。
Radio ID	ユーザが関連付けられている無線のIDです。
SSID	ユーザが関連付けられているSSIDです。
BSSID	ユーザが関連付けられているSBBのIDです。

2.1.2 display dot1x connection

Syntax

display dot1x connection [**ap** *ap-name* [**radio** *radio-id*] | **user-mac** *mac-addr* | **user-name** *name-string*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

radio *radio-id*: ID で無線を指定します。*radio-id* 引数の値の範囲は、装置モデルによって異なります。無線を指定しない場合、このコマンドは、指定した AP 上のすべての無線に接続されているオンライン 802.1X ユーザに関する情報を表示します。

user-mac *mac-addr*: 802.1X ユーザの MAC アドレスを指定します。形式は H-H-H です。

user-name *name-string*: 802.1X ユーザの名前を指定します。設定範囲は 1～253 文字です。大文字、小文字を区別します。

説明

display dot1x connection コマンドはオンライン 802.1X ユーザの情報を表示します。

パラメータを指定しない場合、このコマンドはすべてのポートのオンライン 802.1X ユーザ情報を表示します。

例

すべてのオンライン 802.1X ユーザの情報を表示します。

<AC> display dot1x connection

```
Total connections: 1


Slot ID: 1
User MAC address             : 0015-e9a6-7cfe
AP name                      : ap1
```

```
Radio ID                    : 1
SSID                        : wlan_dot1x_ssid
BSSID                       : 0015-e9a6-7cf0
User name                   : ias
Authentication domain       : 1
IPv4 address                : 192.168.1.1
IPv6 address                : 2000:0:0:0:1:2345:6789:abcd
Authentication method       : CHAP
Initial VLAN                : 1
Authorization VLAN          : N/A
Authorization ACL number    : 3001
Authorization user profile  : N/A
Termination action          : Default
Session timeout period      : 2 sec
Online from                 : 2013/03/02 13:14:15
Online duration             : 0 h 2 m 15 s
```

表 2-2 コマンド出力

フィールド	説明
Slot ID	装置のメンバIDです。メンバIDは1で固定です。
User MAC address	ユーザのMACアドレスです。
AP name	ユーザが関連付けられているAPの名前です。
Radio ID	ユーザが関連付けられている無線のIDです。
SSID	ユーザが関連付けられているSSIDです。
BSSID	ユーザが関連付けられているBSSのIDです。
Authentication domain	802.1X認証で使用されるISPドメインです。
IPv4 address	ユーザのIPv4アドレスです。 装置がユーザのIPv4アドレスを取得できない場合、このフィールドは無効です。
IPv6 address	ユーザのIPv6アドレスです。 装置がユーザのIPv6アドレスを取得できない場合、このフィールドは無効です。

フィールド	説明
Authentication method	EAPメッセージ操作方式です。 • **CHAP**—RADIUSサーバと通信するEAPを終端しCHAPを実行しています。 • **EAP**— RADIUSサーバと通信する際にEAPパケットの中継とEAP認証のいずれかを実行しています。 • **PAP**—RADIUSサーバと通信する際にEAPを終端しPAPを実行しています。
Initial VLAN	802.1X認証を行う前にユーザが所属するVLANです。
Authorization VLAN	ユーザに許可されたVLANです。
Authorization ACL number	ユーザに許可されたACLです。
Authorization user profile	ユーザに許可されたユーザプロファイルです。
Termination action	セッションタイムアウトタイマが終了したときにサーバに割り当てられたアクションです。 • **Default**—認証されたオンライン802.1Xユーザをログオフします。定期オンラインユーザの再認証が有効で、セッションタイムアウトタイマより定期再認証タイマが短い場合は、適用されません。 • **Radius-request**—セッションタイムアウトタイマが終了したとき、定期オンラインユーザの再認証の設定に関わらず、オンラインユーザを再認証します。 装置がローカル認証を実行するとき、このフィールドは**N/A**と表示されます。
Session timeout period	サーバによって割り当てられたセッションタイムアウトタイマです。 装置がローカル認証を実行するとき、このフィールドは**N/A**と表示されます。
Online from	802.1Xユーザがオンラインになったとき時間です。
Online duration	802.1Xユーザがオンラインになってからの経過時間です。

2.1.3 dot1x

Syntax

dot1x

undo dot1x

デフォルト

802.1X はグローバルおよびポートで無効です。

View

System view

Ethernet interface view

定義済みユーザロール

network-admin

説明

dot1x コマンドは 802.1X をグローバルあるいはポートで有効にします。

undo dot1x コマンドは 802.1X をグローバルあるいはポートで無効にします。

802.1X はグローバルとポートの両方で有効にする必要があります。そうでない場合、動作しません。

例

802.1X をグローバルで有効にします。

<AC> system-view

[AC] dot1x

GigabitEthernet 1/0/1 で 802.1X を有効にします。

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] dot1x

[AC-GigabitEthernet1/0/1] quit

関連コマンド

display dot1x

2.1.4 dot1x authentication-method

Syntax

dot1x authentication-method { **chap** | **eap** | **pap** }

undo dot1x authentication-method

デフォルト

chap

View

System view

定義済みユーザロール

network-admin

パラメータ

chap: RADIUS サーバと通信するために EAP（Extensible Authentication Protocol）を終端し、CHAP（Challenge Handshake Authentication Protocol）認証を使用します。

eap: RADIUS サーバと通信するために、EAP パケットを中継し、EAP 認証をサポートします。

pap: RADIUS サーバと通信するために、EAP を終端し、PAP（Password Authentication Protocol）認証をサポートします。

説明

dot1x authentication-method コマンドは EAP メッセージ操作方法を指定することで 802.1X ユーザの認証方法を設定します。

undo dot1x authentication-method コマンドはデフォルトに戻します。

装置は EAP パケットを終端する、あるいは中継します。

- **EAP 終端モード**—アクセス装置は標準の RADIUS パケットの認証データを再カプセル化し、クライアントから RADIUS サーバに送信します。装置は RADIUS サーバの CHAP あるいは PAP 認証のどちらかを実行します。このモードでは RADIUS サーバは MD5-チャレンジ EAP 認証のみをサポートします。
  - PAP はプレーンテキストでユーザ名とパスワードを転送します。この認証方法は高いセキュリティを必要としないシナリオに適用します。
  - CHAP はネットワークを越えてプレーンテキストのユーザ名と暗号化されたパスワードを転送します。CHAP は PAP よりもセキュリティが高いです。
- EAP 中継モードーアクセス装置はクライアントと RADIUS サーバ間の EAP メッセージを中継します。EAP 中継モードは MD5-チャレンジ、EAP-TLS、PEAP のような複数の EAP 認証方式をサポートします。このモードを使用するため、RADIUS サーバは以下の要件に適用する必要があります。
  - EAP メッセージとメッセージ-認証属性をサポートします。
  - クライアントとして同じ EAP 認証方式を使用します。

  このモードが使用されると、RADIUS scheme view で **user-name-format** コマンドは適用されません。**user-name-format** コマンドについての詳細は、コマンドマニュアルのセクション 9 *セキュリティ “AAA”* を参照してください。

RADIUS 認証が使用されると、RADIUS サーバとして同じ認証方式（PAP、CHAP、EAP）を使用するようにアクセス装置を設定する必要があります。

例

EAP パケットを終端するアクセス装置を有効にし、RADIUS サーバで PAP 認証を実行します。

<AC> system-view

[AC] dot1x authentication-method pap

関連コマンド

display dot1x

2.1.5 dot1x guest-vlan

Syntax

dot1x guest-vlan *guest-vlan-id*

undo dot1x guest-vlan

デフォルト

設定なし

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

guest-vlan-id: 802.1X ゲスト VLAN の ID を指定します。設定範囲は 1～4094 です。VLAN が作成されている必要があります。

説明

dot1x guest-vlan コマンドはポートで 802.1X ゲスト VLAN を設定します。

undo dot1x guest-vlan コマンドは デフォルトに戻します。

802.1X ゲスト VLAN は 802.1X 認証を実行していないユーザに適用されます。ユーザは 802.1X ゲスト VLAN で、アンチウィルスソフトウェアをダウンロードするため、ソフトウェアサーバなどの制限されたネットワークリソースを使用します。

802.1X ゲスト VLAN として設定された VLAN を削除する場合、最初に **undo dot1x guest-vlan** コマンドを使用します。

802.1X ゲスト VLAN の詳細については、オペレーションマニュアルのセクション 9 *セキュリティ “802.1X”* を参照してください。

例

GigabitEthernet 1/0/1 で 802.1X ゲスト VLAN100 を設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] dot1x guest-vlan 100

関連コマンド

display dot1x

2.1.6 dot1x handshake

Syntax

dot1x handshake

undo dot1x handshake

デフォルト

有効

View

Ethernet interface view

定義済みユーザロール

network-admin

説明

dot1x handshake コマンドはオンラインユーザハンドシェイク機能を有効にします。

undo dot1x handshake コマンドは機能を無効にします。

オンラインユーザハンドシェイク機能は、オンライン 802.1X ユーザの接続状態を確認するため、装置が定期的にハンドシェイクメッセージをクライアントに送信することを有効にします。もし装置がハンドシェイクタイマの時間に、ハンドシェイクの最大試行回数を実行してもオンラインユーザからの応答を受信しない場合、ユーザをオフライン状態に設定します。ハンドシェイクタイマを設定する場合、**dot1x timer handshake-period** コマンドを使用します。ハンドシェイクの最大試行回数を設定する場合、**dot1x retry** コマンドを使用します。

例

GigabitEthernet 1/0/1 でオンラインユーザハンドシェイク機能を有効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] dot1x handshake

関連コマンド

- **display dot1x**
- **dot1x timer handshake-period**
- **dot1x retry**

2.1.7 dot1x handshake reply enable

Syntax

dot1x handshake reply enable

undo dot1x handshake reply enable

デフォルト

無効

View

Ethernet interface view

定義済みユーザロール

network-admin

説明

dot1x handshake reply enable コマンドはハンドシェイクリプライ機能を有効にします。

undo dot1x handshake reply enable コマンドはハンドシェイクリプライ機能を無効にします。

dot1x handshake reply enable コマンドは、オンラインハンドシェイク処理中に、802.1X クライアントの EAP-Response/Identity パケットに応答するため、EAP-Success パケットを使用することを有効にします。

802.1X クライアントが装置から EAP-Success パケットを受信しないでオフラインになった場合のみ使用します。

例

GigabitEthernet 1/0/1 でハンドシェイクリプライ機能を設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] dot1x handshake reply enable

関連コマンド

dot1x handshake

2.1.8 dot1x mandatory-domain

Syntax

dot1x mandatory-domain *domain-name*

undo dot1x mandatory-domain

デフォルト

設定なし

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

domain-name: ドメイン名を指定します。設定範囲は 1～255 です。大文字、小文字を区別しません。

説明

dot1x mandatory-domain コマンドはポートで強制 802.1X 認証ドメインを指定します。

undo dot1x mandatory-domain コマンドは強制 802.1X 認証ドメインを削除します。

システムがポートにアクセスを行う 802.1X ユーザの認証を行うとき、以下の順番で認証ドメインを選択します。

1) 強制ドメイン
2) ユーザ名で指定された ISP ドメイン
3) デフォルト ISP ドメイン

例

GigabitEthernet 1/0/1 で 802.1X ユーザに強制 802.1X 認証ドメインを設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] dot1x mandatory-domain my-domain

関連コマンド

display dot1x

2.1.9 dot1x max-user

Syntax

dot1x max-user *user-number*

undo dot1x max-user

デフォルト

4294967295

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

user-number: ポートで 802.1X ユーザが同時に接続する最大数を指定します。設定範囲は 1～4294967295 です。

説明

dot1x max-user コマンドはポートで 802.1X ユーザが同時に接続する最大数を指定します。

undo dot1x max-user コマンドは デフォルトに戻します。

システムリソースが乱用されることを防止するため、ポートで 802.1X ユーザが同時に接続する最大数を設定します。最大数に到達したとき、ポートで後続の 802.1X ユーザは拒否されます。

例

GigabitEthernet 1/0/1 で 802.1X ユーザが同時に接続する最大数を 32 に指定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] dot1x max-user 32

関連コマンド

display dot1x

2.1.10 dot1x multicast-trigger

Syntax

dot1x multicast-trigger

undo dot1x multicast-trigger

デフォルト

無効

View

Ethernet interface view

定義済みユーザロール

network-admin

説明

dot1x multicast-trigger コマンドは 802.1X マルチキャストトリガ機能を有効にします。

undo dot1x multicast-trigger コマンドは機能を無効にします。

802.1X マルチキャストトリガ機能は装置がイニシエータとして動作することを有効にします。装置は 802.1X クライアントを検出し、認証を開始するため、定期的に EAP-Request/Identity パケットをマルチキャストします。マルチキャスト EAP-Request/Identity パケットを送信する間隔を設定するため、**dot1x timer tx-period** コマンドを使用します。

無線 LAN ではマルチキャストトリガを無効にします。無線クライアントとアクセス装置の無線モジュールは、それぞれ 802.1X 認証を開始することができます。

例

GigabitEthernet 1/0/1 で 802.1X マルチキャストトリガ機能を有効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] dot1x multicast-trigger

関連コマンド

- **display dot1x**
- **dot1x timer tx-period**
- **dot1x unicast-trigger**

2.1.11 dot1x port-control

Syntax

dot1x port-control { **authorized-force** | **auto** | **unauthorized-force** }

undo dot1x port-control

デフォルト

auto

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

authorized-force: ポートを許可された状態に設定します。認証を行わずネットワークにアクセスできるようにポートのユーザを有効にします。

auto: 指定されたポートあるいはすべてのポートを最初は EAPOL フレームだけは通す許可されていない状態に設定し、認証に成功した後は、ネットワークへのアクセスを許可する許可状態に変更します。これが最も一般的な使用方法です。

unauthorized-force: ポートを許可されていない状態に設定します。ポートのユーザからのアクセス要求を拒否します。

説明

dot1x port-control コマンドはポートの許可状態を設定します。

undo dot1x port-control コマンドは デフォルトに戻します。

このコマンドを使用することで、クライアントのネットワークへのアクセスを許可されるかどうかを決定するため、ポートに許可状態を設定することができます。

例

GigabitEthernet 1/0/1 の許可状態を unauthorized-force に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] dot1x port-control unauthorized-force

関連コマンド

display dot1x

2.1.12 dot1x port-method

Syntax

dot1x port-method { **macbased** | **portbased** }

undo dot1x port-method

デフォルト

macbased

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

macbased: MAC ベースアクセス制御方式を使用します。この方式はポートのそれぞれのユーザを個別に認証します。認証されたユーザがログオフしたとき、この方式を使用しても、他のオンラインユーザには影響しません。

portbased: ポートでポートベースアクセス制御方式を使用します。この方式はポートで最初のユーザが認証に成功すると他のすべてのユーザが認証なしでネットワークへアクセスすることができます。最初のユーザがログオフになったとき、同時に他のすべてのユーザもログオフになります。

説明

dot1x port-method コマンドはポートのアクセス制御方式を指定します。

undo dot1x port-method コマンドは デフォルトに戻します。

ポート上で 802.1X 認証とポータル認証のそれぞれを使用するには、MAC ベースのアクセス制御を指定する必要があります。

例

GigabitEthernet 1/0/1 をポートベースアクセス制御方式に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] dot1x port-method portbased

関連コマンド

display dot1x

2.1.13 dot1x quiet-period

Syntax

dot1x quiet-period

undo dot1x quiet-period

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

dot1x quiet-period コマンドは停止タイマを有効にします。

undo dot1x quiet-period コマンドは停止タイマを無効にします。

クライアントが 802.1X 認証に失敗したとき、装置は、クライアントから認証要求を処理する前に、一定期間を待つ必要があります。停止タイマの時間を設定する場合、**dot1x timer quiet-period** コマンドを使用します。

例

停止タイマを有効にし、停止時間を 100 秒に設定します。

<AC> system-view

[AC] dot1x quiet-period

[AC] dot1x timer quiet-period 100

関連コマンド

- **display dot1x**
- **dot1x timer**

2.1.14 dot1x re-authenticate

Syntax

dot1x re-authenticate

undo dot1x re-authenticate

デフォルト

無効

View

Ethernet interface view

定義済みユーザロール

network-admin

説明

dot1x re-authenticate コマンドは定期的なオンラインユーザの再認証機能を有効にします。

undo dot1x re-authenticate コマンドは機能を無効にします。

定期再認証機能を有効にすると、アクセス装置は、ポートのオンライン 802.1X ユーザを定期的に認証します。この機能はオンラインユーザの接続状態を確認し、ACL や VLAN、ユーザプロファイルなどの、サーバに割り当てられた許可属性をアップデートします。

再認証を行う期間を設定する場合、**dot1x timer reauth-period** コマンドを使用します。

例

GigabitEthernet 1/0/1 で 802.1X オンラインユーザの再認証機能を有効にし、再認証を行う期間を 1800 秒に設定します。

<AC> system-view

[AC] dot1x timer reauth-period 1800

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] dot1x re-authenticate

関連コマンド

- **display dot1x**
- **dot1x timer**

2.1.15 dot1x retry

Syntax

dot1x retry *max-retry-value*

undo dot1x retry

デフォルト

2

View

System view

定義済みユーザロール

network-admin

パラメータ

retries: クライアントに認証要求を送信する最大試行回数を指定します。設定範囲は 1～10 です。

説明

dot1x retry コマンドはクライアントに認証要求を送信する最大試行回数を設定します。

undo dot1x retry コマンドは デフォルトに戻します。

以下のいずれかの状況により、アクセス装置はクライアントに認証要求を再送します。

- 装置はユーザ名の要求タイマ内にクライアントから応答を受信しません。EAP-Request/Identity パケットのタイマは **dot1x timer tx-period** *tx-period-value* コマンドで設定することができます。
- 装置はクライアントタイムアウトタイマ内にクライアントから応答を受信しません。EAP-Request/MD5-Challenge パケットのタイマは **dot1x timer supp-timeout** *supp-timeout-value* コマンドで設定することができます。

認証要求を送信する試行回数が最大に到達しても応答を受信しない場合、アクセス装置は要求の再送を停止します。

例

クライアントに認証要求を送信する最大試行回数を 9 に設定します。

<AC> system-view

[AC] dot1x retry 9

関連コマンド

- **display dot1x**
- **dot1x timer**

2.1.16 dot1x timer

Syntax

dot1x timer { **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **reauth-period** *reauth-period-value* | **server-timeout** *server-timeout-value* | **supp-timeout** *supp-timeout-value* | **tx-period** *tx-period-value* }

undo dot1x timer { **handshake-period** | **quiet-period** | **reauth-period** | **server-timeout** | **supp-timeout** | **tx-period** }

デフォルト

- ハンドシェイクタイマ：15 秒
- 停止タイマ：60 秒
- 定期再認証タイマ：3600 秒
- サーバタイムアウトタイマ：100 秒
- クライアントタイムアウトタイマ：30 秒
- ユーザ名要求タイムアウトタイマ：30 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

handshake-period *handshake-period-value*: ハンドシェイクタイマを設定します。設定範囲は 5～1024 秒です。

quiet-period *quiet-period-value*: 停止タイマを設定します。設定範囲は 10～120 秒です。

reauth-period *reauth-period-value*: 定期再認証タイマを設定します。設定範囲は 60～7200 秒です。

server-timeout *server-timeout-value*: サーバタイムアウトタイマを設定します。設定範囲は 100～300 秒です。

supp-timeout *supp-timeout-value*: クライアントタイムアウトタイマを設定します。設定範囲は 1～120 秒です。

tx-period *tx-period-value*: ユーザ名要求タイムアウトタイマを設定します。設定範囲は 10～120 秒です。

説明

dot1x timer コマンドは 802.1X タイマを設定します。

undo dot1x timer コマンドはデフォルトに戻します。

ほとんどの状況ではデフォルトの設定で十分です。ネットワークの状況に依存してタイマを設定することができます。

- 低速ネットワークでは、クライアントタイムアウトタイマを増加します。
- 脆弱なネットワークでは、停止タイマの値を大きい値に設定します。
- 認証の応答が早急な高性能ネットワークでは、停止タイマを小さい値に設定します。
- 異なる性能の認証サーバがあるネットワークではサーバタイムアウトタイマを適切に設定します。

サーバがセッションタイムアウトタイマを装置に割り当てた場合、定期再認証タイマは有効になりません。

ネットワーク装置は以下の 802.1X タイマを使用します。

- **ハンドシェイクタイマ（handshake-period）**－装置が認証ユーザのオンライン状況の確認のためハンドシェイク要求を定期的に送信する間隔を設定します。ハンドシェイク要求に応答がない場合には、認証ユーザがログオフしたと判断します。
- **停止タイマ（quiet-period）**—クライアントが認証に失敗したとき開始します。アクセス装置はクライアントから認証処理を開始する前に、タイマの時間を待つ必要があります。
- **定期再認証タイマ（reauth-period）**—ポート上の定期再認証を有効にすると、装置は、タイマで設定された間隔でポート上のオンラインユーザを再認証します。この設定は **dot1x re-authenticate** コマンドで設定します。まだオンラインにユーザが存在しているときに再認証間隔を変更すると、装置は、変更前の間隔での再認証を継続します。オンラインユーザの再認証を終了した後、装置は新しく設定された再認証間隔を使います。
- **サーバタイムアウトタイマ（server-timeout）**—アクセス装置が認証サーバに RADIUS Access-Request パケットを送信するときに開始します。このタイマが時間

切れになるまでに応答がなかった場合、アクセス装置は、サーバに要求を再送します。

- **クライアントタイムアウトタイマ（supp-timeout）**—アクセス装置がクライアントに EAP-Request/MD5 Challenge パケットを送信するときに開始します。このタイマが時間切れになるまで応答がなかった場合、アクセス装置は、クライアントに要求を再送します。
- **ユーザ名要求タイムアウトタイマ（tx-period）**—装置が EAP-Request/Identity パケットをクライアントに認証要求の応答として送信するときに開始します。タイマが終了する前に装置が応答を受信しない場合、要求を再送します。認証をアクティブに要求できないクライアントを検出するため、EAP-Request/Identity パケットをネットワーク装置に、設定されたタイマの間隔でマルチキャストします。

定期再認証タイマは古い再認証タイマが終了した後、新しく設定された再認証の間隔が適用されます。他のタイマは設定を変更するとすぐに適用されます。

例

サーバタイムアウトタイマを 150 秒に設定します。

<AC> system-view

[AC] dot1x timer server-timeout 150

関連コマンド

display dot1x

2.1.17 dot1x unicast-trigger

Syntax

dot1x unicast-trigger

undo dot1x unicast-trigger

デフォルト

無効

View

Ethernet interface view

定義済みユーザロール

network-admin

説明

dot1x unicast-trigger コマンドは 802.1X ユニキャストトリガ機能を有効にします。

undo dot1x unicast-trigger コマンドは 802.1X ユニキャストトリガ機能を無効にします。

802.1X ユニキャストトリガ機能は、未知の送信元 MAC アドレスからデータフレームを受信したときに 802.1X 認証を開始する機能です。装置は、ユニキャスト EAP-Request/Identity パケットを未知の送信元の MAC アドレスに送信しますが、一定時間内（**dot1x timer tx-period** コマンドで指定されます）に反応がない場合、パケットを再送します。このプロセスはで設定された最大試行回数（**dot1x retry** コマンドで指定されます）、実施します。

例

GigabitEthernet 1/0/1 のユニキャストトリガ機能を有効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] dot1x unicast-trigger

関連コマンド

- **display dot1x**
- **dot1x multicast-trigger**
- **dot1x retry**
- **dot1x timer**

2.1.18 reset dot1x guest-vlan

Syntax

reset dot1x guest-vlan interface *interface-type interface-number* [**mac-address** *mac-address*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

mac-address *mac-address*: ゲスト VLAN の 802.1X ユーザの MAC アドレスを指定します。指定しない場合、ポートのすべての 802.1X ユーザを削除します。

説明

reset dot1x guest-vlan コマンドはポートの 802.1X ゲスト VLAN からユーザを削除します。

例

GigabitEthernet 1/0/1 の 802.1X ゲスト VLAN から MAC アドレスが 1-1-1 のユーザを削除します。

<AC> reset dot1x guest-vlan interface gigabitethernet 1/0/1 mac-address 1-1-1

関連コマンド

dot1x guest-vlan

2.1.19 reset dot1x statistics

Syntax

reset dot1x statistics [**ap** *ap-name* [**radio** *radio-id*]]

View

User view

定義済みユーザロール

network-admin

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

radio *radio-id*: ID で無線を指定します。*radio-id* 引数の値の範囲は、装置モデルによって異なります。無線を指定しない場合、このコマンドは指定された AP 上のすべての無線に関する 802.1X 統計情報を削除します。

説明

reset dot1x statistics コマンドはポートの 802.1X の統計情報を削除します。

パラメータを指定しない場合、このコマンドはすべての 802.1X 統計情報を削除します。

例

802.1X の統計情報を削除します。

<AC> reset dot1x statistics

関連コマンド

display dot1x

目次

このセクションのページは **9-x-x** です。

3 章 MAC アドレス認証 3-1
3.1 MAC アドレス認証設定コマンド.....3-1
3.1.1 display mac-authentication.....3-1
3.1.2 display mac-authentication connection.....3-4
3.1.3 mac-authentication 3-6
3.1.4 mac-authentication authentication-method.....3-7
3.1.5 mac-authentication domain 3-8
3.1.6 mac-authentication max-user.....3-9
3.1.7 mac-authentication timer server-timeout.....3-10
3.1.8 mac-authentication user-name-format.....3-11
3.1.9 reset mac-authentication statistics 3-13

3章 MAC アドレス認証

3.1 MACアドレス認証設定コマンド

3.1.1 display mac-authentication

Syntax

display mac-authentication [**ap** *ap-name* [**radio** *radio-id*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

radio *radio-id*: 無線の ID を指定します。設定範囲は AP のモデルにより異なります。無線を指定しない場合、このコマンドは指定した AP のすべての無線の MAC アドレス認証設定と統計情報を表示します。

説明

display mac-authentication コマンドは MAC アドレス認証の設定と統計情報を表示します。設定情報、MAC アドレス認証の統計情報、オンラインユーザの統計情報を表示します。

すべてのパラメータを指定しない場合、すべての MAC アドレス認証の設定と統計情報を表示します。

例

すべての MAC アドレス認証の設定と統計情報を表示します。

<AC> display mac-authentication

```
Global MAC authentication parameters:
```

```
  MAC authentication     : Enabled
  User name format       : MAC address in lowercase(xxxxxxxxxxxx)
         Username        : mac
         Password        : Not configured
  Offline detect period  : 300 s
  Quiet period           : 60 s
  Server timeout         : 100 s
  Authentication domain  : Not configured, use default domain
Online MAC-auth wired users    : 0
Online MAC-auth wireless users : 1

Silent MAC users:
        MAC address      VLAN ID  From port            Port index

AP name: AP1  Radio ID: 1  SSID: wlan_maca_ssid
  BSSID                   : 487a-daa0-74f0
  MAC authentication      : Enabled
  Authentication domain   : Not configured
  Max online users        : 4096
  Authentication attempts : successful 1, failed 0
  Current online users    : 1
        MAC address      Auth state
        2477-032b-db8c   Authenticated
```

表 3-1 コマンド出力

フィールド	説明
MAC authentication	MACアドレス認証がグローバルで有効かどうかを示します。
User name format	ユーザアカウントタイプです。MACベースあるいは共有があります。 ● MACベースアカウントが使用される場合、ユーザ名のフォーマットで表示されます。たとえば、ハイフンなし、16進数表示、小文字でMACアドレスが**MAC address in lowercase(xxxxxxxxxxxx)**と表示されます。 ● 共有アカウントが使用される場合、**Fixed account**と表示されます。

フィールド	説明
Username	MACアドレス認証のユーザ名です。 ● MACベースアカウントが使用される場合、**mac**と表示されます。装置はMACアドレス認証のユーザ名とパスワードとして各ユーザのMACアドレスを使用します。 ● 共有アカウントが使用される場合、MACアドレス認証ユーザの共有アカウントのユーザ名が表示されます。デフォルトのユーザ名は**mac**です。
Password	MACアドレス認証のパスワードです。 ● MACベースアカウントが使用されている場合、あるいは共有アカウントでパスワードが設定されていない場合、**Not configured**と表示されます。 ● 共有アカウントでパスワードが設定されている場合、とアスタリスク（******）の文字列が表示されます。
Offline detect period	オフライン検出タイマです。
Quiet period	Quietタイマです。
Server timeout	サーバタイムアウトタイマです。
Authentication domain	system viewで指定されたMACアドレス認証のドメインです。system viewでMACアドレス認証のドメインが指定されていない場合、**Not configured, use default domain**と表示されます。
Online MAC-auth wired users	MAC認証を通過したユーザやMAC認証を実行しているユーザを含む、有線オンラインMAC認証ユーザの数です。
Online MAC-auth wireless users	MAC認証を通過したユーザやMAC認証を実行しているユーザを含む、無線オンラインMAC認証ユーザの数です。
Silent MAC users	サイレントMACアドレスについての情報です。
MAC address	サイレントMACアドレスです。
VLAN ID	サイレントMACアドレスが所属するVLANのIDです。
From port	サイレントMACアドレスとしてMACアドレスを記載するポート名です。
Port index	サイレントMACアドレスとしてMACアドレスを記載するポートのインデックスです。
AP name	ユーザが紐付けられたAPの名前です。
Radio ID	ユーザが紐付けられた無線のIDです。
SSID	ユーザが紐付けられたSSIDです。

フィールド	説明
BSSID	ユーザが紐付けられたBSSのIDです。

3.1.2 display mac-authentication connection

Syntax

display mac-authentication connection [**ap** *ap-name* [**radio** *radio-id*] | **user-mac** *mac-address* | **user-name** *user-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

radio *radio-id*: 無線の ID を指定します。設定範囲は AP のモデルにより異なります。無線を指定しない場合、このコマンドは指定した AP に接続されたすべてのオンライン MAC アドレス認証ユーザに関する情報を表示します。

user-mac *mac-address*: オンライン MAC アドレス認証ユーザの MAC アドレスを指定します。*mac-address* はユーザの MAC アドレスを示します。形式は H-H-H です。

user-name *user-name*: オンライン MAC アドレス認証ユーザのユーザ名を指定します。設定範囲は 1～55 文字です。大文字、小文字を区別します。ドメイン名を含むことができます。

説明

display mac-authentication connection コマンドはオンライン MAC アドレス認証ユーザの情報を表示します。

すべてのパラメータを指定しない場合、すべてのポートのオンライン MAC アドレス認証ユーザの情報を表示します。

例

すべてのオンライン MAC アドレス認証ユーザの情報を表示します。

<AC> display mac-authentication connection

```
Total connections: 1

Slot ID: 1
User MAC address            : 0015-e9a6-7cfe
AP name                    : ap1
Radio ID                   : 1
SSID                       : wlan_dot1x_ssid
BSSID                      : 0015-e9a6-7cf0
User name                  : ias
Authentication domain       : 1
Initial VLAN               : 1
Authorization VLAN          : 100
Authorization ACL number     : 3001
Authorization user profile   : N/A
Authorization URL           : N/A
Termination action          : Radius-request
Session timeout period       : 2 sec
Online from                : 2016/06/02 13:14:15
Online duration             : 0h 2m 15s
```

表 3-2 コマンド出力

フィールド	説明
Total connections	オンラインMACアドレス認証ユーザの総数です。
Slot ID	デバイスのメンバーIDで、1で固定されています。
User MAC address	ユーザのMACアドレスです。
AP name	ユーザが紐付けられたAPの名前です。
Radio ID	ユーザが紐付けられた無線のIDです。
SSID	ユーザが紐付けられたSSIDです。
BSSID	ユーザが紐付けられたBSSのIDです。
Authentication domain	ユーザが所属するMACアドレス認証のドメインです。
Initial VLAN	MACアドレス認証を行う前にユーザを保持するVLANです。

フィールド	説明
Authorization VLAN	ユーザに許可されたVLANです。
Authorization ACL number	このフィールドは現在のソフトウェアバージョンではサポートされていません。 ユーザに許可されたACLです。
Authorization user profile	このフィールドは現在のソフトウェアバージョンではサポートされていません。 ユーザに許可されたユーザプロファイルです。
Authorization URL	このフィールドは現在のソフトウェアバージョンではサポートされていません。 ユーザに承認されたURLをリダイレクトします。
Termination action	セッションタイムアウトタイマが終了したとき、サーバに割り当てられたアクションの属性です。 • **Default**—セッションタイムアウトタイマが終了したとき、オンライン認証ユーザをログオフします。 • **Radius-request**—セッションタイムアウトタイマが終了したとき、オンラインユーザを再認証します。 ローカル認証が実行されている場合、**N/A**と表示されます。
Session timeout period	サーバによって割り当てられたセッションタイムアウトタイマです。 ローカル認証が実行されている場合、**N/A**と表示されます。
Online from	MACアドレス認証ユーザがオンラインになった時間です。
Online duration	MACアドレス認証ユーザがオンラインになってからの経過時間です。

3.1.3 mac-authentication

Syntax

mac-authentication

undo mac-authentication

デフォルト

無効

View

System view

Ethernet interface view

定義済みユーザロール

network-admin

説明

mac-authentication コマンドはグローバルあるいはポートで MAC アドレス認証を有効にします。

undo mac-authentication コマンドはグローバルあるいはポートで MAC アドレス認証を無効にします。

ポートで MAC アドレス認証を使用する場合、グローバルとポートの両方で MAC アドレス認証を有効にする必要があります。

例

グローバルで MAC アドレス認証を有効にします。

<AC> system-view

[AC] mac-authentication

GigabitEthernet 1/0/1 で MAC アドレス認証を有効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] mac-authentication

関連コマンド

display mac-authentication

3.1.4 mac-authentication authentication-method

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.55 を含む以降のソフトウェアからサポートしています。

Syntax

mac-authentication authentication-method { chap | pap }

undo mac-authentication authentication-method

デフォルト

RADIUS サーバとの通信に PAP を使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

chap: RADIUS サーバとの通信に Challenge Handshake Authentication Protocol (CHAP) を使用します。

pap: RADIUS サーバとの通信に Password Authentication Protocol (PAP) を使用します。

説明

mac-authentication authentication-method コマンドは MAC アドレス認証の認証方式を設定します。

undo mac-authentication authentication-method コマンドはデフォルトに戻します。

RADIUS ベースの MAC 認証では、次の認証方式がサポートされています。

- PAP:ユーザ名とパスワードをプレーンテキストで転送します。認証方法は、高度なセキュリティを必要としないシナリオに適用されます。
- CHAP:ユーザ名をプレーンテキストで、パスワードを暗号化してネットワーク経由で転送します。CHAP は PAP よりも安全です。

例

MAC 認証に CHAP を使用するようにデバイスを設定します。

<AP> system-view

[AP] mac-authentication authentication-method chap

関連コマンド

display mac-authentication

3.1.5 mac-authentication domain

Syntax

mac-authentication domain *domain-name*

undo mac-authentication domain

デフォルト

MAC アドレス認証ユーザの認証ドメインは指定されていません。システムはデフォルトの認証ドメインを使用します。デフォルト認証ドメインの詳細は、オペレーションマニュ

アルのセクション 9 *セキュリティ “AAA”* の **domain default enable** コマンドを参照してください。

View

System view

Service template view

定義済みユーザロール

network-admin

パラメータ

domain-name: ISP ドメインの名前を指定します。設定範囲は 1～255 文字です。大文字、小文字を区別しません。

説明

mac-authentication domain コマンドはグローバルあるいはサービステンプレート固有の認証ドメインを指定します。

undo mac-authentication domain コマンドはデフォルトに戻します。

サービステンプレートは、以下の順番で MAC アドレス認証ユーザの認証ドメインを選択します。

1) サービステンプレートで指定された認証ドメインを指定します。
2) system view で指定されたグローバルの認証ドメインを指定します。
3) デフォルトの認証ドメインを指定します。

例

グローバルの MAC アドレス認証ドメインとしてドメイン domain1 を指定します。

<AC> system-view

[AC] mac-authentication domain domain1

関連コマンド

- **display mac-authentication**
- **domain default enable**

3.1.6 mac-authentication max-user

Syntax

mac-authentication max-user *max-number*

undo mac-authentication max-user

デフォルト

4294967295

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

max-number: ポートの MAC アドレス認証のユーザが同時に接続可能な最大数を設定します。設定範囲は 1～4294967295 です。

説明

mac-authentication max-user コマンドはポートの MAC アドレス認証のユーザが同時に接続可能な最大数を設定します。

undo mac-authentication max-user コマンドはデフォルトに戻します。

システムリソースが乱用されることを防止するため、ポートで MAC アドレス認証ユーザが同時に接続する最大数を設定します。最大数に到達したとき、ポートで後続の MAC アドレス認証ユーザは拒否されます。

例

GigabitEthernet 1/0/1 の MAC アドレス認証のユーザが同時に接続可能な最大数を 32 に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] mac-authentication max-user 32

関連コマンド

display mac-authentication

3.1.7 mac-authentication timer server-timeout

Syntax

mac-authentication timer server-timeout *server-timeout-value*

undo mac-authentication timer server-timeout

デフォルト

100 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

server-timeout *server-timeout-value*: server timeout timer を設定します。設定範囲は 100～300 秒です。

説明

mac-authentication timer server-timeout コマンドは MAC アドレス認証のサーバタイムアウトタイマを設定します。

undo mac-authentication timer server-timeout コマンドはデフォルトに戻します。

server timeout timer は RADIUS サーバが使用不能であることを検出するために、装置が RADIUS サーバからの応答を待つ時間をタイマに設定します。MAC アドレス認証中にタイムアウトした場合、ユーザはネットワークにアクセスすることはできません。

例

server timeout timer を 150 秒に設定します。

<AC> system-view

[AC] mac-authentication timer server-timeout 150

関連コマンド

display mac-authentication

3.1.8 mac-authentication user-name-format

Syntax

mac-authentication user-name-format { **fixed** [**account** *name*] [**password** { **cipher** | **simple** } *string*] | **mac-address** [{ **with-hyphen** [**six-section** | **three-section**] | **without-hyphen** } [**lowercase** | **uppercase**]] }

undo mac-authentication user-name-format

デフォルト

MAC アドレス認証のユーザ名とパスワードとして各ユーザの MAC アドレスが使用されます。MAC アドレスは 6 セクション形式で、文字は小文字です。

View

System view

定義済みユーザロール

network-admin

パラメータ

fixed: すべての MAC アドレス認証ユーザの共有アカウントを使用します。

account *name*: 共有アカウントのユーザ名を指定します。設定範囲は 1～55 文字です。大文字、小文字を区別します。アットマーク（@）は指定できません。指定しない場合、デフォルトのユーザ名 **mac** が適用されます。

password: 共有ユーザアカウントのパスワードを指定します。

cipher: 暗号化された形式でパスワードを指定します。

simple: 平文形式でパスワードを指定します。セキュリティ上の理由から、平文形式で指定されたパスワードは暗号化された形式で保存されます。

string: パスワードを指定します。暗号化された形式は、大文字と小文字を区別する 1～117 文字の文字列です。平文形式は、大文字と小文字を区別する 1～63 文字の文字列です。

mac-address: MAC アドレス認証ユーザの MAC ベースユーザアカウントを使用します。以下のパラメータを使用してユーザ名とパスワードの形式を指定することができます。

- **with-hyphen**: MAC アドレスにハイフンを含みます。以下の形式で指定します。
  - six-section: xx-xx-xx-xx-xx-xx または XX-XX-XX-XX-XX-XX
  - three-section: xxxx-xxxx-xxxx または XXXX-XXXX-XXXX

  キーワードを指定しない場合、MAC アドレスは six-section 形式です。
- **without-hyphen**: MAC アドレスにハイフンを含みません。xxxxxxxxxxxx または XXXXXXXXXXXX で指定します。
- **lowercase**: 小文字を指定します。
- **uppercase**: 大文字を指定します。

説明

mac-authentication user-name-format コマンドは MAC アドレス認証ユーザのユーザアカウントのタイプを設定します。

undo mac-authentication user-name-format コマンドはデフォルトに戻します。

MAC ベースのユーザアカウントを指定する場合、装置は、ユーザの MAC アドレス認証のユーザ名とパスワードとしてユーザの MAC アドレスを使用します。ユーザアカウントタイプは認証のセキュリティを高めます。しかし、認証サーバは、ユーザ名とパスワードとしてユーザの MAC アドレスを使用し、各ユーザのユーザアカウントを作成する必要があります。

共有ユーザアカウントを使用する場合、装置は、すべてのユーザの MAC アドレス認証を行うため指定されたユーザ名とパスワードを使用します。すべての MAC アドレスユーザは、認証用に 1 つのアカウントを使用するため、認証サーバで 1 つのアカウントのみを作成します。このユーザアカウントタイプは信頼されたネットワーク用に適しています。

例

MAC アドレス認証ユーザの共有アカウントを設定し、ユーザ名を abc、パスワードをプレーンテキストで xyz に設定します。

<AC> system-view

[AC] mac-authentication user-name-format fixed account abc password simple xyz

MAC アドレス認証ユーザの MAC ベースユーザアカウントを設定します。各 MAC アドレスはハイフンつき、大文字の 16 進数で設定します。

<AC> system-view

[AC] mac-authentication user-name-format mac-address with-hyphen uppercase

関連コマンド

display mac-authentication

3.1.9 reset mac-authentication statistics

Syntax

reset mac-authentication statistics [**ap** *ap-name* [**radio** *radio-id*]]

View

User view

定義済みユーザロール

network-admin

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

radio *radio-id*: 無線の ID を指定します。設定範囲は AP のモデルにより異なります。無線を指定しない場合、このコマンドは指定した AP のすべての無線の MAC アドレス認証の統計情報を削除します。

説明

reset mac-authentication statistics コマンドは MAC アドレス認証の統計情報を削除します。

すべてのパラメータを指定しない場合、すべての MAC アドレス認証の統計情報を削除します。

例

すべての MAC アドレス認証の統計情報を削除します。

<AC> reset mac-authentication statistics

関連コマンド

display mac-authentication

目次

このセクションのページは **9-x-x** です。

4 章 パスワード管理.....4-1
4.1 パスワード管理設定コマンド.....4-1
4.1.1 display password-control.....4-1
4.1.2 display password-control blacklist.....4-3
4.1.3 password-control { aging | composition | history | length } enable.....4-4
4.1.4 password-control aging.....4-6
4.1.5 password-control alert-before-expire.....4-7
4.1.6 password-control change-password first-login enable.....4-8
4.1.7 password-control complexity.....4-9
4.1.8 password-control composition.....4-10
4.1.9 password-control enable.....4-12
4.1.10 password-control expired-user-login.....4-13
4.1.11 password-control history.....4-14
4.1.12 password-control length.....4-15
4.1.13 password-control login idle-time.....4-17
4.1.14 password-control login-attempt.....4-18
4.1.15 password-control super aging.....4-21
4.1.16 password-control super composition.....4-22
4.1.17 password-control super length.....4-23
4.1.18 password-control update-interval.....4-23
4.1.19 reset password-control blacklist.....4-24
4.1.20 reset password-control history-record.....4-25

4章 パスワード管理

🕮 メモ：

パスワード管理はソフトウェアバージョン 7.2.46 を含む以降のソフトウェアからサポートしています。

4.1 パスワード管理設定コマンド

4.1.1 display password-control

Syntax

display password-control [**super**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

super: super パスワードのパスワード管理の情報を表示します。指定しない場合、グローバルのパスワード管理の設定を表示します。

説明

display password-control コマンドはパスワード管理の設定を表示します。

Enabled と表示されているコマンドでも、**password-control enable** コマンドの有効化が必要な機能は、**Enabled** と表示されている状態でも動作しません。

例

グローバルのパスワード管理の設定を表示します。

<AC> display password-control

```
Global password control configurations:
 Password control:                  Enabled (device management users)
                                  Enabled (network access users)
 Password aging:                    Enabled (90 days)
 Password length:                   Enabled (10 characters)
 Password composition:               Enabled (1 types, 1 characters per type)
```

```
Password history:                  Enabled (max history records:4)
Early notice on password expiration:  7 days
User authentication timeout:         600 seconds
Maximum login attempts:             3
Action for exceeding login attempts:  Lock user for 1 minutes
Minimum interval between two updates: 24 hours
User account idle time:              90 days
Logins with aged password:           3 times in 30 days
Password complexity:                 Disabled (username checking)
                                   Disabled (repeated characters checking)
Password change:                     Enabled (first login)
```

super パスワードのパスワード管理の設定を表示します。

<AC> display password-control super

```
Super password control configurations:
Password aging:                    Enabled (90 days)
Password length:                   Enabled (10 characters)
Password composition:               Enabled (1 types, 1 characters per type)
```

表 4-1 コマンド出力

フィールド	説明
Password control	パスワード管理機能が有効かどうかを示します。
Password aging	パスワードの有効期限の設定が有効かどうかを示します。有効である場合、有効期限が表示されます。
Password length	最小パスワード長の設定が有効かどうかを示します。有効である場合、設定を表示します。
Password composition	パスワード構成ポリシー機能が有効かどうかを示します。有効である場合、設定を表示します。
Password history	パスワード履歴機能が有効かどうかを示します。有効である場合、設定を表示します。
Early notice on password expiration	ユーザのパスワードの有効期限が終了する前に、ユーザに通知するまでの日数です。
Maximum login attempts	FTPユーザとVTYユーザがログインできる最大試行回数です。
Action for exceeding login attempts	ユーザが試行回数後にログインに失敗したときのアクションです。
Minimum interval between two updates	パスワードアップデートの最小間隔です。
Login with aged password	パスワードの有効期限後、ユーザがログインできる最大日時と最大回数です。

フィールド	説明
Password complexity	パスワード複雑性の確認が有効かどうかを示します。 • **username checking**—パスワードはユーザ名あるいはユーザ名の逆の順番を含むかどうかを確認します。 • **repeated characters checking**—文字あるいは数字が3回以上連続して続くかどうかを確認します。
Password change	初回ログイン時のパスワード変更機能の状態を示します。 • Enabled (first login)— 初回ログイン時のパスワード変更機能が有効です。 • Disabled (first login)— 初回ログイン時のパスワード変更機能が無効です。

4.1.2 display password-control blacklist

Syntax

display password-control blacklist [**user-name** *user-name* | **ip** *ipv4-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

user-name *user-name*: ユーザ名を指定します。設定範囲は 1～55 文字です。大文字、小文字を区別します。

ip *ipv4-address*: ユーザの IPv4 アドレスを指定します。

説明

display password-control blacklist コマンドはパスワード管理ブラックリストの情報を表示します。

パラメータを指定しない場合、パスワード管理ブラックリストのすべてのユーザの情報を表示します。

コンソールポートを経由してアクセスしたユーザが認証に失敗すると、そのユーザアカウントがパスワード制御ブラックリストに追加されます。FTP や VTY ユーザが認証に失敗すると、その IP アドレスおよびユーザアカウントがパスワード制御ブラックリストに追加されます。**display password-control blacklist** コマンドを使用して、ブラックリストに掲載されたユーザに関する情報を表示できます。

例

パスワード管理ブラックリストのユーザの情報を表示します。

<AC> display password-control blacklist

```
Blacklist items matched: 2.
 Username                  IP address          Login failures   Lock flag
 abcd                      169::168:34:1       4                lock
 admin                     192.168.34.1        1                unlock
```

表 4-2 コマンド出力

フィールド	説明
Blacklist items matched	ブラックリストのユーザ数です。
IP address	ユーザのIPアドレスです。
Login failures	ログイン失敗回数です。
Lock flag	ユーザログインの禁止が行われているかどうかを示します。IPアドレスを持つユーザの場合、ユーザアカウントとIPアドレスの両方がロックされます。 IPアドレスを持たないユーザの場合は、ユーザアカウントだけがロックされます。ユーザは、このユーザアカウントを使用してコンソール回線経由でログインすることはできません。 • **unlock**—禁止されていません。 • **lock**— **password-control login-attempt**コマンドによって一時的あるいは永久に禁止されています。

4.1.3 password-control { aging | composition | history | length } enable

Syntax

password-control { **aging** | **composition** | **history** | **length** } **enable**

undo password-control { **aging** | **composition** | **history** | **length** } **enable**

デフォルト

パスワード管理機能はすべて（**aging**、**composition**、**history**、**length**）有効です。

View

System view

定義済みユーザロール

network-admin

パラメータ

aging: パスワードの有効期限の設定を有効にします。

composition: パスワード構成ポリシー機能を有効にします。

history: パスワード履歴機能を有効にします。

length: 最小パスワード長の設定を有効にします。

説明

password-control { **aging | composition | history | length** } **enable** コマンドはパスワード管理機能（有効期限、パスワード構成ポリシー、パスワード履歴、最小パスワード長の機能）を有効にします。

undo password-control { **aging | composition | history | length** } **enable** コマンドはパスワード管理機能を無効にします。

グローバルパスワード制御機能（**password-control enable** コマンド）が有効であるかどうかに関係なく、パスワード構成の制限および最小パスワード長制限がデフォルトで有効になります。デフォルトでは、パスワード構成ポリシーと最小パスワード長は次のとおりです。

- パスワードには、2 つ以上の文字タイプと、各タイプにつき 1 つ以上の文字を含める必要があります。
- パスワードは 10 文字以上にする必要があります。

装置管理ユーザのパスワードがハッシュ形式の場合、次の要件を満たしていても、パスワードに対する制限設定は有効になりません。

- グローバルパスワード制御が有効
- パスワード制限機能が有効

undo password-control history enable コマンドを実行した後、システムは新しいパスワードと履歴パスワードを比較しませんが、履歴パスワードの記録は停止しません。ユーザの履歴パスワードレコードの数が **password-control history** コマンドで設定された最大数に達すると、最新の履歴レコードによって最も古い履歴レコードが上書きされます。

例

グローバルパスワード管理機能を有効にします。

<AC> system-view

[AC] password-control enable

パスワード構成ポリシー機能を有効にします。

[AC] password-control composition enable

パスワードの有効期限の機能を有効にします。

[AC] password-control aging enable

最小パスワード長の設定を有効にします。

[AC] password-control length enable

パスワード履歴の機能を有効にします。

[AC] password-control history enable

関連コマンド

- **display password-control**
- **password-control enable**

4.1.4 password-control aging

Syntax

password-control aging *aging-time*

undo password-control aging

デフォルト

パスワードの有効期限は 90 日です。ユーザグループのパスワードの有効期限はグローバルの設定と同一です。ローカルユーザのパスワードの有効期限はローカルユーザが所属しているユーザグループのパスワードの有効期限と同一です。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

aging-time: パスワードの有効期限を指定します。設定範囲は 1～365 日です。

説明

password-control aging コマンドはパスワードの有効期限を設定します。

undo password-control aging コマンドはデフォルトに戻します。

パスワードの有効期限は各 view に依存します。

- system view のパスワードの有効期限はグローバルであり、すべてのユーザグループに適用します。
- user group view のパスワードの有効期限はユーザグループのすべてのローカルユーザに適用します。

- local user view のパスワードの有効期限はローカルユーザのみに適用します。

パスワードの有効期限は小さい範囲でのパスワードの設定が高い優先度を持ちます。システムはローカルユーザに local user view のパスワードの有効期限を使用します。

- ローカルユーザにパスワードの有効期限が設定されていない場合、システムはローカルユーザが所属しているユーザグループのパスワードの有効期限を使用します。
- ユーザグループにパスワードの有効期限が設定されていない場合、システムはグローバルのパスワードの有効期限を使用します。

例

グローバルのパスワードの有効期限を 80 日に設定します。

<AC> system-view

[AC] password-control aging 80

ユーザグループ **test** のパスワードの有効期限を 90 日に設定します。

[AC] user-group test

[AC-ugroup-test] password-control aging 90

[AC-ugroup-test] quit

装置管理ユーザ **abc** のパスワードの有効期限を 100 日に設定します。

[AC] local-user abc class manage

[AC-luser-manage-abc] password-control aging 100

関連コマンド

- **display local-user**
- **display password-control**
- **display user-group**
- **password-control aging enable**

4.1.5 password-control alert-before-expire

Syntax

password-control alert-before-expire *alert-time*

undo password-control alert-before-expire

デフォルト

7 日

View

System view

定義済みユーザロール

network-admin

パラメータ

alert-time: ユーザのパスワードの有効期限が終了する前にユーザに通知するまでの日数を指定します。設定範囲は 1～30 日です。

説明

password-control alert-before-expire コマンドはユーザのパスワードの有効期限が終了する前に、ユーザに通知するまでの日数を設定します。

undo password-control alert-before-expire コマンドはデフォルトに戻します。

このコマンドは FTP ユーザ以外のユーザに適用されます。FTP ユーザは、管理者によってのみパスワードを変更することができます。

例

ユーザのパスワードの有効期限が終了する前に、ユーザに通知するまでの日数を 10 日に設定します。

<AC> system-view

[AC] password-control alert-before-expire 10

関連コマンド

display password-control

4.1.6 password-control change-password first-login enable

Syntax

password-control change-password first-login enable

undo password-control change-password first-login enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

password-control change-password first-login enable コマンドは、初回ログイン時のパスワード変更機能を有効にします。

undo password-control change-password first-login enable コマンドは、初回ログイン時のパスワード変更機能を無効にします。

初回ログイン時のパスワード変更機能を有効にするには、**password-control enable** コマンドと **password-control change-password first-login enable** コマンドの両方を設定する必要があります。

例

初回ログイン時のパスワード変更機能を有効に設定します。

<AC> system-view

[AC] password-control change-password first-login enable

関連コマンド

- **display password-control**
- **password-control enable**

4.1.7 password-control complexity

Syntax

password-control complexity { **same-character** | **user-name** } **check**

undo password-control complexity { **same-character** | **user-name** } **check**

デフォルト

ユーザグループのパスワードの複雑性のポリシーはグローバルの設定と同一です。ローカルユーザのパスワードの複雑性のポリシーはローカルユーザが所属しているユーザグループのパスワードの複雑性のポリシーと同一です。

グローバルのパスワードの複雑性のポリシーは、**user-name check** は有効、**same-character check** は無効です。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

same-character: パスワードに文字あるいは数字が 3 回以上連続して続くことを禁止します。たとえば、パスワード **aaabc** はポリシーに適合しません。

user-name: パスワードにユーザ名あるいはユーザ名の逆の順番を含むことを禁止します。たとえば、ユーザ名が **123** であるとき、**abc123** あるいは **321df** のパスワードはポ

リシーに適合しません。**password-control enable** コマンドを設定していなくても、本コマンドが有効な場合には有効になります。

説明

password-control complexity コマンドはパスワードの複雑性のポリシーを設定します。

undo password-control complexity コマンドはパスワードの複雑性のポリシーを削除します。

パスワードの複雑性のポリシーは各 view に依存します。

- system view のパスワードの複雑性のポリシーはグローバルであり、すべてのユーザグループに適用します。
- user group view のパスワードの複雑性のポリシーはユーザグループのすべてのローカルユーザに適用します。
- local user view のパスワードの複雑性のポリシーはローカルユーザのみに適用します。

パスワードの複雑性のポリシーは小さい範囲でのパスワードの設定が高い優先度を持ちます。システムはローカルユーザに local user view のパスワードの複雑性のポリシーを使用します。

- ローカルユーザにパスワードの複雑性のポリシーが設定されていない場合、システムはローカルユーザが所属しているユーザグループのパスワードの複雑性のポリシーを使用します。
- ユーザグループにパスワードの複雑性のポリシーが設定されていない場合、システムはグローバルのパスワードの複雑性のポリシーを使用します。

パスワード内のユーザ名の有無の確認と、パスワードの文字の反復回数の確認の両方を有効にすることができます。

例

パスワード内のユーザ名の有無の確認、あるいはパスワードの文字の反復回数の確認を禁止するパスワードの複雑性のポリシーを設定します。

<AC> system-view

[AC] password-control complexity user-name check

関連コマンド

- **display local-user**
- **display password-control**
- **display user-group**

4.1.8 password-control composition

Syntax

password-control composition type-number *type-number* [**type-length** *type-length*]

undo password-control composition

デフォルト

グローバルのパスワード構成ポリシーは、少なくとも 2 種類の文字タイプと、各タイプに 1 文字以上を含む必要があります。

ユーザグループのパスワード構成ポリシーはグローバルの設定と同一です。ローカルユーザのパスワード構成ポリシーはローカルユーザが所属しているユーザグループのパスワード構成ポリシーと同一です。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

type-number *type-number*: パスワードに含まれる文字タイプの最小数を指定します。設定範囲は 1~4 です。

type-length *type-length*: パスワードの各タイプの最小文字数を指定します。設定範囲は 1～63 です。

説明

password-control composition コマンドはパスワード構成ポリシーを設定します。

undo password-control composition コマンドはデフォルトに戻します。

password-control enable コマンドを設定していなくても、本コマンドの設定が有効になります。

パスワード構成ポリシーは各 view に依存します。

- system view のパスワード構成ポリシーはグローバルであり、すべてのユーザグループに適用します。
- user group view のパスワード構成ポリシーはユーザグループのすべてのローカルユーザに適用します。
- local user view のパスワード構成ポリシーはローカルユーザのみに適用します。

パスワード構成ポリシーは小さい範囲でのパスワードの設定が高い優先度を持ちます。システムはローカルユーザに local user view のパスワード構成ポリシーを使用します。

- ローカルユーザにパスワード構成ポリシーが設定されていない場合、システムはローカルユーザが所属しているユーザグループのパスワード構成ポリシーを使用します。

- ユーザグループにパスワード構成ポリシーが設定されていない場合、システムはグローバルのパスワード構成ポリシーを使用します。

文字タイプの最小数と各タイプの最小文字数はパスワードの最大長より小さくする必要があります。

例

すべてのパスワードに少なくとも 4 種類の文字と各タイプに 5 文字以上を含むように指定します。

<AC> system-view

[AC] password-control composition type-number 4 type-length 5

ユーザグループ **test** のパスワードに少なくとも 4 種類の文字と各タイプに 5 文字以上を含むように指定します。

[AC] user-group test

[AC-ugroup-test] password-control composition type-number 4 type-length 5

[AC-ugroup-test] quit

装置管理ユーザ **abc** のパスワードに少なくとも 4 種類の文字と各タイプに 5 文字以上を含むように指定します。

[AC] local-user abc class manage

[AC-luser-manage-abc] password-control composition type-number 4 type-length 5

関連コマンド

- **display local-user**
- **display password-control**
- **display user-group**
- **password-control composition enable**

4.1.9 password-control enable

Syntax

password-control enable

undo password-control enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

password-control enable コマンドはグローバルでパスワード管理機能を有効にします。

undo password-control enable コマンドはグローバルでパスワード管理機能を無効にします。

グローバルでパスワード管理機能を有効にしたのち、指定したパスワード管理機能が適用されます。

グローバルでパスワード管理機能を有効にしたのち、対応する **display** コマンドを使用して装置管理ユーザのパスワード設定と super パスワードの設定を表示することはできません。ネットワークアクセスユーザのパスワード設定が表示されます。装置管理ユーザの設定された初期パスワードは少なくとも 4 種類の文字を含む必要があります。

例

グローバルでパスワード管理機能を有効にします。

<AC> system-view

[AC] password-control enable

関連コマンド

- **display password-control**
- **password-control** { **aging** |**composition** | **history** | **length** } **enable**

4.1.10 password-control expired-user-login

Syntax

password-control expired-user-login delay *delay* **times** *times*

undo password-control expired-user-login

デフォルト

ユーザはパスワードの有効期限が終了したのち、30 日以内に 3 回ログインすることができます。すべてのログイン試行に失敗するか、30 日後にユーザがログイン試行を行うと、ユーザに新しいパスワードを設定するようプロンプトが表示されます。

View

System view

定義済みユーザロール

network-admin

パラメータ

delay *delay*: パスワードの有効期限が終了した後、ユーザがログインできる最大日時を設定します。設定範囲は 1～90 日です。

times *times*: パスワードの有効期限が終了した後、ユーザがログインできる最大回数を設定します。設定範囲は 0～10 です。パスワードの有効期限が終了した後、ユーザがシステムプロンプトで新しいパスワードを設定するには、値を 0 に設定します。

説明

password-control expired-user-login コマンドはパスワードの有効期限が終了した後、ユーザがログインできる最大日時と最大回数を設定します。

undo password-control expired-user-login コマンドはデフォルトに戻します。

このコマンドは、FTP 以外のログインユーザにのみ有効です。

FTP ユーザはパスワードの有効期限が終了した後、ログインすることができません。

例

パスワードの有効期限が終了した後、ユーザがログインできる最大日時を 60 日、最大回数を 5 回に設定します。

<AC> system-view

[AC] password-control expired-user-login delay 60 times 5

関連コマンド

display password-control

4.1.11 password-control history

Syntax

password-control history *max-record-number*

undo password-control history

デフォルト

4

View

System view

定義済みユーザロール

network-admin

パラメータ

max-record-number: 各ユーザのパスワード履歴の最大数を指定します。設定範囲は 2～15 です。

説明

password-control history コマンドは各ユーザのパスワード履歴の最大数を設定します。

undo password-control history コマンドはデフォルトに戻します。

パスワード履歴が最大数になったとき、後続のパスワード履歴はもっとも古いパスワードに上書きします。

システムは **undo password-control history enable** コマンドを実行した後、パスワードの記録を停止しますが、すでに記録されたパスワードを削除しません。

既存のパスワード履歴を削除する場合、以下のいずれかの方法を使用します。

- グローバルでパスワード管理機能を無効にするため、**undo password-control enable** コマンドを使用します。
- 手動でパスワードを削除するため、**reset password-control history-record** コマンドを使用します。

例

各ユーザのパスワード履歴の最大数を 10 に設定します。

<AC> system-view

[AC] password-control history 10

関連コマンド

- **display password-control**
- **password-control history enable**
- **reset password-control blacklist**

4.1.12 password-control length

Syntax

password-control length *length*

undo password-control length

デフォルト

グローバルの最小パスワード長は 10 文字です。

ユーザグループの最小パスワード長はグローバルの設定と同一です。ローカルユーザの最小パスワード長はローカルユーザが所属しているユーザグループの最小パスワード長と同一です。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

length: 最小パスワード長を指定します。設定範囲は 4～32 文字です。

説明

password-control length コマンドは最小パスワード長を設定します。

undo password-control length コマンドはデフォルトに戻します。

password-control enable コマンドを設定していなくても、本コマンドの設定が有効になります。

最小パスワード長の設定は各 view に依存します。

- system view の最小パスワード長の設定はグローバルであり、すべてのユーザグループに適用します。
- user group view の最小パスワード長の設定はユーザグループのすべてのローカルユーザに適用します。
- local user view の最小パスワード長の設定はローカルユーザのみに適用します。

最小パスワード長の設定は小さい範囲でのパスワードの設定が高い優先度を持ちます。システムはローカルユーザに local user view の最小パスワード長の設定を使用します。

- ローカルユーザに最小パスワード長が設定されていない場合、システムはローカルユーザが所属しているユーザグループの最小パスワード長の設定を使用します。
- ユーザグループに最小パスワード長が設定されていない場合、システムはグローバルの最小パスワード長の設定を使用します。

例

グローバルの最小パスワード長を 16 文字に設定します。

<AC> system-view

[AC] password-control length 16

ユーザグループ **test** の最小パスワード長を 16 文字に設定します。

[AC] user-group test

[AC-ugroup-test] password-control length 16

[AC-ugroup-test] quit

装置管理ユーザ **abc** の最小パスワード長を 16 文字に設定します。

[AC] local-user abc class manage

[AC-luser-manage-abc] password-control length 16

関連コマンド

- **display local-user**
- **display password-control**
- **display user-group**
- **password-control length enable**

4.1.13 password-control login idle-time

Syntax

password-control login idle-time *idle-time*

undo password-control login idle-time

デフォルト

90 日

View

System view

定義済みユーザロール

network-admin

パラメータ

idle-time: アカウントアイドルタイムの最大日数を指定します。設定範囲は 0～365 日です。0 はアカウントアイドルタイムの制限を行いません。

説明

password-control login idle-time コマンドはアカウントアイドルタイムの最大日数を設定します。

undo password-control login idle-time コマンドはデフォルトに戻します。

ユーザが最後にログインしてから指定した期間内にログインしない場合、ユーザアカウントは無効になります。

例

アカウントアイドルタイムの最大日数を 30 日に設定します。

<AC> system-view

[AC] password-control login idle-time 30

関連コマンド

display password-control

4.1.14 password-control login-attempt

Syntax

password-control login-attempt *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]

undo password-control login-attempt

デフォルト

グローバルのログイン試行の設定は以下です。

- 連続してログインに失敗できる最大数は 3 です。
- 3 回ログインに失敗した後、ログインの試行を無効にする時間は 1 分です。

ユーザグループのログイン試行の設定はグローバルの設定と同一です。ローカルユーザのログイン試行の設定はローカルユーザが所属しているユーザグループのログイン試行の設定と同一です。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

login-times: 連続してログインに失敗できる最大数を指定します。設定範囲は 2～10 です。

exceed: ユーザが試行回数後にログインに失敗した後のアクションを指定します。

- **lock**: FTP または VTY ユーザの場合、ユーザアカウントとユーザの IP アドレスは両方ともロックされます。このロックされた IP アドレスからは、このユーザアカウントを使用してログインできません。 コンソールユーザの場合、ユーザアカウントがロックされます。ユーザは、このユーザアカウントを使用してコンソール回線経由でログインできません。
- **lock-time** *time*: 設定範囲は 1～360 分です。
  ロックタイマが期限切れになると、FTP または VTY ユーザはこのユーザアカウントを使用して、IP アドレスから再度ログインできます。ロックタイマが期限切れになると、コンソールユーザはこのユーザアカウントを使用して再度ログインできます。

- **unlock**: ユーザが試行回数後にログインに失敗した後もユーザアカウントを使用することができます。

説明

password-control login-attempt コマンドはログイン試行の制限を設定します。ログイン最大試行回数と、ユーザが試行回数後にログインに失敗したときのアクションを設定できます。

undo password-control login-attempt コマンドはデフォルトに戻します。

ログイン試行の制限の設定は各 view に依存します。

- system view のログイン試行の制限の設定はグローバルであり、すべてのユーザグループに適用します。
- user group view のログイン試行の制限の設定はユーザグループのすべてのローカルユーザに適用します。
- local user view のログイン試行の制限の設定はローカルユーザのみに適用します。

ログイン試行の制限の設定は小さい範囲でのパスワードの設定が高い優先度を持ちます。システムはローカルユーザに local user view のログイン試行の制限の設定を使用します。

- ローカルユーザにログイン試行の制限が設定されていない場合、システムはローカルユーザが所属しているユーザグループのログイン試行の制限の設定を使用します。
- ユーザグループにログイン試行の制限が設定されていない場合、システムはグローバルのログイン試行の制限の設定を使用します。

FTP あるいは VTY ユーザが最大ログイン試行後にログインに失敗した場合、システムはユーザアカウントとユーザの IP アドレスをパスワード管理ブラックリストに追加します。

コンソールユーザも同様の操作でパスワード管理ブラックリストに追加します

アカウントは、ブラックリストに追加されたユーザのみロックされます。他のユーザはアカウントを使用することができます。ブラックリストに記載されているユーザは他のユーザアカウントを使用することができます。ロックされた IP アドレスのユーザに対してのみロックされます。ロック解除された IP アドレスのユーザはこのアカウントを使用でき、ロックされた IP アドレスのユーザは他のロック解除されたユーザアカウントを使用できます。

- ユーザのユーザアカウントが永久にロックされた場合、パスワード管理ブラックリストからアカウントを削除しない限り、ユーザはこのアカウントを使用することができません。ユーザアカウントを削除する場合、**reset password-control blacklist** コマンドを使用します。
- 一時的にロックされたユーザアカウントを使用する場合、以下のいずれかの処理を行うことができます。
  - □　ロックしているタイマが終了するまで待ちます。
  - □　パスワード管理ブラックリストからアカウントを削除します。
- ユーザアカウントとユーザがブラックリストに登録されているが、ロックされていない場合、ユーザは、このアカウントを使用してログインを行うことができます。ユーザがユーザアカウントを使用して装置に正常にログインしたとき、パスワード管理ブラックリストからアカウントとユーザの IP アドレスが削除されます。

password-control login-attempt コマンドは、コマンドが設定されたのち、すぐに適用されます。パスワード管理ブラックリストにすでに存在するユーザも適用されます。

例

ユーザアカウントのログイン最大試行回数を 4 に設定し、ユーザが試行回数後にログインに失敗した後、ユーザアカウントを無効にします。

<AC> system-view

[AC] password-control login-attempt 4 exceed lock

装置にログインするユーザアカウント **test** を使用し、4 回間違ったパスワードを入力します。

パスワード管理ブラックリストを表示します。出力は、ブラックリストのユーザアカウントに存在し、アクションが **lock** であることを示します。

[AC] display password-control blacklist

```
Username: test
   IP: 192.168.44.1       Login failures: 4     Lock flag: lock

Blacklist items matched: 1.
```

192.168.44.1 のユーザが、このユーザアカウントを使用してログインできないことを確認します。

ユーザアカウントのログイン試行回数を 2 に設定し、ユーザが試行回数後にログインに失敗した後、3 分間、ユーザアカウントを無効にします。

<AC> system-view

[AC] password-control login-attempt 2 exceed lock-time 3

装置にログインするユーザアカウント **test** を使用し、2 回間違ったパスワードを入力します。

パスワード管理ブラックリストを表示します。出力は、ブラックリストのユーザアカウントに存在し、アクションが **lock** であることを示します。

[AC] display password-control blacklist

```
Username: test
   IP: 192.168.44.1       Login failures: 2     Lock flag: lock

Blacklist items matched: 1.
```

3 分後、ユーザアカウントがパスワード管理ブラックリストから削除され、192.168.44.1 のユーザが、このユーザアカウントを使用してログインできることを確認します。

関連コマンド

- **display local-user**

- **display password-control**
- **display password-control blacklist**
- **display user-group**
- **reset password-control blacklist**

4.1.15 password-control super aging

Syntax

password-control super aging *aging-time*

undo password-control super aging

デフォルト

90 日

View

System view

定義済みユーザロール

network-admin

パラメータ

aging-time: super パスワードの有効期限を指定します。設定範囲は 1～365 日です。

説明

password-control super aging コマンドは super パスワードの有効期限を設定します。

undo password-control super aging コマンドはデフォルトに戻します。

例

super パスワードの有効期限を 10 日に設定します。

<AC> system-view

[AC] password-control super aging 10

関連コマンド

- **display password-control**
- **password-control aging**

4.1.16 password-control super composition

Syntax

password-control super composition type-number *type-number* [**type-length** *type-length*]

undo password-control super composition

デフォルト

super パスワード構成ポリシーは少なくとも 2 種類の文字と各タイプに 1 文字以上を含む必要があります。

View

System view

定義済みユーザロール

network-admin

パラメータ

type-number *type-number*: super パスワードに含まれる文字タイプの最小数を指定します。設定範囲は 1～4 文字です。

type-length *type-length*: パスワードの各タイプの最小数を指定します。設定範囲は 1～63 です。

説明

password-control super composition コマンドは super パスワードの複雑性のポリシーを設定します。

undo password-control super composition コマンドはデフォルトに戻します。

password-control enable コマンドを設定していなくても、本コマンドの設定が有効になります。

文字タイプの最小数と各タイプの最小文字数は super パスワードの最大長より小さくする必要があります。

例

super パスワードに少なくとも 4 種類の文字と各タイプに 5 文字以上を含むように指定します。

<AC> system-view

[AC] password-control super composition type-number 4 type-length 5

関連コマンド

- **display password-control**
- **password-control composition**

4.1.17 password-control super length

Syntax

password-control super length *length*

undo password-control super length

デフォルト

10 文字

View

System view

定義済みユーザロール

network-admin

パラメータ

length: super パスワードの最小パスワード長を指定します。設定範囲は 4～63 です。

説明

password-control super length コマンドは super パスワードの最小パスワード長を設定します。

undo password-control super length コマンドはデフォルトに戻します。

password-control enable コマンドを設定していなくても、本コマンドの設定が有効になります。

例

super パスワードの最小パスワード長を 16 文字に設定します。

<AC> system-view

[AC] password-control super length 16

関連コマンド

- **display password-control**
- **password-control length**

4.1.18 password-control update-interval

Syntax

password-control update-interval *interval*

undo password-control update-interval

デフォルト

24 時間

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: パスワードアップデートの最小間隔を指定します。設定範囲は 0～168 時間です。0 はパスワードのアップデートを行わないことを示します。

説明

password-control update-interval コマンドはパスワードアップデートの最小間隔を設定します。パスワードアップデートの最小間隔はユーザがパスワードを変更できる最小間隔です。

undo password-control update-interval コマンドはデフォルトに戻します。

設定された最小間隔は、最初のログイン時またはパスワードの有効期限が切れた後にパスワードの変更を求められる装置管理ユーザでは有効ではありません。

例

パスワードアップデートの最小間隔を 36 時間に設定します。

<AC> system-view

[AC] password-control update-interval 36

関連コマンド

display password-control

4.1.19 reset password-control blacklist

Syntax

reset password-control blacklist [**user-name** *user-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

user-name *user-name*: パスワード管理ブラックリストから削除するユーザを指定します。設定範囲は 1～55 文字です。大文字、小文字を区別します。

説明

reset password-control blacklist コマンドはパスワード管理ブラックリストからユーザを削除します。

ログイン試行を超過したためにブラックリストに記録されたユーザが再度ログインできるようにするため、このコマンドを使用して、パスワード管理ブラックリストからユーザを削除します。

例

パスワード管理ブラックリストからユーザ **test** を削除します。

<AC> reset password-control blacklist user-name test

```
Are you sure to delete the specified user in blacklist? [Y/N]:
```

関連コマンド

display password-control blacklist

4.1.20 reset password-control history-record

Syntax

reset password-control history-record [**super** [**role** *role-name*] | **user-name** *user-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

super: 指定された、あるいはすべての super パスワードの履歴の記録を削除します。

role *role name*: ユーザロールを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。このオプションを指定しないと、すべての super パスワードの履歴の記録が削除されます。

user-name *user-name*: パスワード履歴を削除するユーザのユーザ名を指定します。設定範囲は 1～55 文字です。大文字、小文字を区別します。

説明

reset password-control history-record コマンドはパスワード履歴の記録を削除します。

パラメータを指定しない場合、すべてのローカルユーザのパスワード履歴の記録を削除します。

例

すべてのローカルユーザのパスワード履歴の記録を削除します。

<AC> reset password-control history-record

```
Are you sure to delete all local user's history records? [Y/N]:y
```

関連コマンド

password-control history

目次

このセクションのページは **9-x-x** です。

5 章 公開鍵 5-1
5.1 公開鍵設定コマンド 5-1
5.1.1 display public-key local public 5-1
5.1.2 display public-key peer 5-4
5.1.3 peer-public-key end 5-6
5.1.4 public-key local create 5-7
5.1.5 public-key local destroy 5-10
5.1.6 public-key local export dsa 5-12
5.1.7 public-key local export rsa 5-15
5.1.8 public-key peer 5-17
5.1.9 public-key peer import sshkey 5-18

5章 公開鍵

5.1 公開鍵設定コマンド

5.1.1 display public-key local public

Syntax

display public-key local { **dsa | rsa** } **public** [**name** *key-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dsa: DSA 鍵ペアタイプを指定します。

rsa: RSA 鍵ペアタイプを指定します。

name *key-name*: ローカル非対称鍵ペアの名前を指定します。設定範囲は 1～64 文字です。英字、数字、ハイフン（-）を含みます。名前を指定しない場合、指定されたタイプのすべてのローカル非対称鍵ペアの公開鍵を表示します。

説明

display public-key local public コマンドはローカル鍵ペアを表示します。

例

すべてのローカル RSA 鍵ペアの公開鍵を表示します。

<AC> display public-key local rsa public

```
=============================================
Key name: hostkey (default)
Key type: RSA
Time when key pair created: 15:40:48 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
   667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
   C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
   FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
```

```
   2DA4C04EF5AE0835090203010001
=============================================
Key name: serverkey (default)
Key type: RSA
Time when key pair created: 15:40:48 2011/05/12
Key code:
   307C300D06092A864886F70D0101010500036B003068026100CAB4CACCA16442AD5F453442
   762F03897E0D494FEDE69224F5C051A441D290976733A278C9F0C0F5A198E66143EAB54A64
   DB608269CAE844B1E7CC64AD7E808972E7CF887F3B657F056E7930FC84FBF1AD83A01CC47E
   9D85C13413996ECD093B0203010001
=============================================
Key name: rsa1
Key type: RSA
Time when key pair created: 15:42:26 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DEBC46F217DDF11D
   426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
   1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
   9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
   92D8C6D940890BF4290203010001
```

すべてのローカル DSA 鍵ペアの公開鍵を表示します。

<AC> display public-key local dsa public

```
=============================================
Key name: dsakey (default)
Key type: DSA
Time when key pair created: 15:41:37 2011/05/12
Key code:
   308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF038184000218041912CE34D12BCD2157E7AB1C2F03B3EF395
   100F3DB4A9E2FDFE860C1BD663D676438F7DA40A9406D61CA9079AF13E330489F1C76785DE
   52DA649AC8BC04B6D39CD7C52CD0A14F75F7491A91D31D6AC22340B5981B27A915CDEC4F09
   887E541EC1E5302D500F68E7AC29A084463C60F9EE266985A502FC92193E1CF4D265C4BA
=============================================
Key name: dsa1
```

```
Key type: DSA
Time when key pair created: 15:35:42 2011/05/12
Key code:
  308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
  96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
  DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
  DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
  7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
  4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
  35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
  91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
  585DA7F42519718CC9B09EEF038185000281810 0A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
  3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
  0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
  15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

ローカル RSA 鍵ペア rsa1 の公開鍵を表示します。

<AC> display public-key local rsa public name rsa1

```
=============================================
Key name: rsa1
Key type: RSA
Time when key pair created: 15:42:26 2011/05/12
Key code:
  30819F300D06092A864886F70D010101050003818D0030818902818100DEBC46F217DDF11D
  426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
  1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
  9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
  92D8C6D940890BF4290203010001
```

ローカル DSA 鍵ペア dsa1 の公開鍵を表示します。

<AC> display public-key local dsa public name dsa1

```
=============================================
Key name: dsa1
Key type: DSA
Time when key pair created: 15:35:42 2011/05/12
Key code:
  308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
  96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
  DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
  DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
  7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
  4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
```

```
35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
585DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

表 5-1 コマンド出力

フィールド	説明
Key name	ローカル鍵ペアの名前です。 鍵ペアを作成したとき、名前を指定しない場合、以下の鍵ペア名の後ろに（default）が追加されます。 以下に各鍵アルゴリズムのデフォルト鍵ペアを示します。 • **hostkey**—デフォルトRSAホスト鍵ペア名です。 • **serverkey**—デフォルトRSAサーバ鍵ペア名です。 • **dsakey**—デフォルトDSAホスト鍵ペア名です。
Key type	オプションです。 • **RSA** • **DSA**
Time when key pair created	ローカル鍵ペアが作成された日時です。
Key code	公開鍵の文字列です。

関連コマンド

public-key local create

5.1.2 display public-key peer

Syntax

display public-key peer [**brief** | **name** *publickey-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

brief: すべてのピアのホスト公開鍵の概要を表示します。鍵タイプ、鍵モジュール、鍵名のみ表示します。

name *publickey-name*: ピアのホスト公開鍵の詳細情報を表示します。鍵コードが含まれます。*publickey-name* はピアのホスト公開鍵の名前を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別します。

説明

display public-key peer コマンドはピアのホスト公開鍵の情報を表示します。

パラメータを指定しない場合、ローカル装置で設定したすべてのピアのホスト公開鍵の詳細情報を表示します。

ローカル装置のピアのホスト公開鍵を設定する場合、**public-key peer** コマンドあるいは **public-key peer import sshkey** コマンドを使用します。

例

ピアのホスト公開鍵 idrsa の詳細情報を表示します。

<AC> display public-key peer name idrsa

```
=========================================
Key name: idrsa
Key type: RSA
Key modulus: 1024
Key code:
  30819F300D06092A864886F70D010101050003818D0030818902818100C5971581A78B5388
  B3C9063EC6B53D395A6704D9752B6F9B7B1F734EEB5DD509F0B050662C46FFB8D27F797E37
  918F6270C5793F1FC63638970A0E4D51A3CEF7CFF6E92BFAFD73F530E0BDE27056E81F2525
  6D0883836FD8E68031B2C272FE2EA75C87734A7B8F85B8EBEB3BD51CC26916AF3B3FDC32C3
  42C142D41BB4884FEB0203010001
```

表 5-2 コマンド出力

フィールド	説明
Key name	ピアのホスト公開鍵の名前です。
Key type	鍵タイプです。RSA、DSAがあります。
Key modulus	鍵モジュール長です。単位はビットです。
Key code	公開鍵の文字列です。

すべてのピアのホスト公開鍵の概要情報を表示します。

<AC> display public-key peer brief

```
Type  Modulus  Name
---------------------------
RSA   1024    idrsa
DSA   1024    10.1.1.1
```

表 5-3 コマンド出力

フィールド	説明
Type	鍵タイプです。RSA、DSAがあります。
Modulus	鍵モジュール長です。単位はビットです。
Name	ピアの公開鍵の名前です。

関連コマンド

- **public-key peer**
- **public-key peer import sshkey**

5.1.3 peer-public-key end

Syntax

peer-public-key end

View

Public key view

定義済みユーザロール

network-admin

説明

peer-public-key end コマンドは public key view から system view に戻り、設定されたピアのホスト公開鍵を保存します。

ローカル装置でピアのホスト公開鍵を入力した後、このコマンドを使用し、public key view から system view に戻り、ホスト公開鍵を保存します。

システムは公開鍵を保存する前に確認します。鍵が正しい形式でない場合、システムは鍵を廃棄し、エラーメッセージを表示します。鍵が正常である場合、鍵を保存します。鍵はたとえば、**display public-key local public** コマンドで表示することができます。

例

public key view から system view に戻り、設定されたピアのホスト公開鍵を保存します。

<AC> system-view

[AC] public-key peer key1

```
Enter public key view. Return to system view with "peer-public-key end" command.
```

[AC-pkey-public-key-key1]30819F300D06092A864886F70D010101050003818D0030818902818100C0EC8014F82515F6335A0A

[AC-pkey-public-key-key1]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E719D1643135877E13B1C531B4

[AC-pkey-public-key-key1]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B952ADF6B80EB5F52698FCF3D6

[AC-pkey-public-key-key1]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050BD4A9B1DDE675AC30CB020301

[AC-pkey-public-key-key1]0001

[AC-pkey-public-key-key1] peer-public-key end

[AC]

関連コマンド

- **display public-key local public**
- **display public-key peer**
- **public-key peer**

5.1.4 public-key local create

Syntax

public-key local create { **dsa** | **rsa** } [**name** *key-name*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

dsa: DSA 鍵ペアを作成します。

rsa: RSA 鍵ペアを作成します。

name *key-name*: ローカル非対称鍵ペアの名前を割り当てます。設定範囲は 1～64 文字です。英字、数字、ハイフン（-）を含みます。名前を割り当てない場合、デフォルト名を適用します。

表 5-4 デフォルトのローカル鍵ペア名

タイプ	デフォルト名
RSA	• **ホスト鍵ペア**：hostkey • **サーバ鍵ペア**：serverkey
DSA	dsakey

説明

public-key local create コマンドはローカル非対称鍵ペアを作成します。

鍵アルゴリズムはセキュリティアプリケーションで要求されたアルゴリズムと同一にする必要があります。

RSA または DSA 鍵ペアを作成するときは、プロンプトに適切な鍵モジュールの長さを入力します。鍵モジュールの長さが長いほど、セキュリティが高くなりますが鍵生成時間も長くなります。

鍵モジュールの長さと鍵の長さの詳細については、表 5-5 を参照してください。

鍵ペアの名前を割り当てない場合、デフォルトの名前を割り当て、鍵ペアを default としてマーキングします。デフォルトの名前を別の鍵ペアに割り当てることができますが、鍵ペアを default としてマーキングしません。鍵ペアの名前は、同じ鍵アルゴリズムを使用する鍵ペア間で一意にする必要がありますが、異なる鍵アルゴリズムを使用する鍵ペアでは同じ名前を使用することができます。もし名前が重複している場合、存在する鍵ペアに上書きしていいか確認メッセージが表示されます。

鍵ペアは自動で保存され、装置の再起動が行われても削除されません。

表 5-5 非対称鍵アルゴリズムの異なるタイプの比較

タイプ	鍵ペア数	モジュール / 鍵長
RSA	• 鍵ペアの名前を指定する場合、ホスト鍵ペアを作成します。 • 鍵ペアの名前を指定しない場合、1つのサーバ鍵ペアと1つのホスト鍵ペアを作成し、デフォルト名を使用します。	設定範囲は512～2048ビットです。 デフォルトは1024ビットです。
DSA	1つのホスト鍵ペアを作成します。	設定範囲は512～2048ビットです。 デフォルトは1024ビットです。

例

デフォルト名のローカル RSA 鍵ペアを作成します。

<AC> system-view

[AC] public-key local create rsa

```
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...++++++
.++++++
..++++++++
....++++++++
Create the key pair successfully.
```

デフォルト名のローカル DSA 鍵ペアを作成します。

<AC> system-view

[AC] public-key local create dsa

```
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+..+.................
.......+..........+.............+..........+...+.....+...............+..+...
...+.................+..........+...+.+.......+.....+............+.........+.
.........................+........+.......+.............+.....+...+..........
```

```
..............+.........+..........+........+........+....+..................
.....++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*
Create the key pair successfully.
```

名前が rsa1 のローカル RSA 鍵ペアを作成します。

<AC> system-view

[AC] public-key local create rsa name rsa1

```
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...++++++
.............................++++++
Create the key pair successfully.
```

名前が dsa1 のローカル DSA 鍵ペアを作成します。

<AC> system-view

[AC] public-key local create dsa name dsa1

```
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.................................+..+.................
.......+..........+............+.........+...+.....+.............+..+...
...+.................+.........+...+.+.......+.....+...........+.........+.
.........................+........+.......+............+.....+...+..........
..............+.........+..........+........+........+....+..................
.....++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*
Create the key pair successfully.
```

関連コマンド

- **display public-key local public**
- **public-key local destroy**

5.1.5 public-key local destroy

Syntax

public-key local destroy { **dsa** | **rsa** } [**name** *key-name*]

View

System view

定義済みユーザロール

network-admin

パラメータ

dsa: DSA 鍵ペアタイプを指定します。

rsa: RSA 鍵ペアタイプを指定します。

name *key-name*: ローカル非対称鍵ペアの名前を指定します。設定範囲は 1～64 文字です。英字、数字、ハイフン（-）を含みます。大文字と小文字を区別しません。名前を指定しない場合、デフォルト名のローカル鍵ペアの指定されたタイプを削除します。

説明

public-key local destroy コマンドはローカル鍵ペアを削除します。

以下の状況が発生した場合、鍵を正常に保つため、ローカル非対称鍵ペアを削除し、新しいペアを生成する必要があります。

- 不正侵入が発生した場合。
- 装置の記憶媒体を交換した場合。
- ローカル証明書が期限切れとなった場合。ローカル証明書の詳細はオペレーションマニュアルのセクション 9 *セキュリティ* を参照してください。

例

デフォルト名のローカル RSA 鍵ペアを削除します。

<AC> system-view

[AC] public-key local destroy rsa

```
Confirm to destroy the key pair? [Y/N]:y
```

デフォルト名のローカル DSA 鍵ペアを削除します。

<AC> system-view

[AC] public-key local destroy dsa

```
Confirm to destroy the key pair? [Y/N] :y
```

名前が rsa1 のローカル RSA 鍵ペアを削除します。

<AC> system-view

[AC] public-key local destroy rsa name rsa1

```
Confirm to destroy the key pair? [Y/N]:y
```

名前が dsa1 のローカル DSA 鍵ペアを削除します。

<AC> system-view

[AC] public-key local destroy dsa name dsa1

```
Confirm to destroy the key pair? [Y/N] :y
```

関連コマンド

public-key local create

5.1.6 public-key local export dsa

Syntax

public-key local export dsa [**name** *key-name*] { **openssh** | **ssh2** } [*filename*]

View

System view

定義済みユーザロール

network-admin

パラメータ

name *key-name*: ローカル DSA 鍵ペアの名前を指定します。設定範囲は 1～64 文字です。英字、数字、ハイフン（-）を含みます。指定しない場合、デフォルト名のローカル DSA 鍵ペアのホスト公開鍵を表示あるいはエクスポートします。

openssh: OpenSSH の形式を使用します。

ssh2: SSH2.0 の形式を使用します。

filename: 保存するローカルホスト公開鍵の名前を指定します。設定範囲は 1～128 文字です。大文字、小文字を区別しません。”./”、”../” を除いて指定します。名前は、ドット（.）、hostkey、serverkey、dsakey、ecdsakey を使用することができません。また先頭をスラッシュにすることができません。*filename* が指定されている場合、ローカル DSA ホスト公開鍵をエクスポートします。指定されていない場合、ローカル DSA ホスト公開鍵を表示します。ファイル名の詳細はオペレーションマニュアルのセクション 1 *はじめに* “*ファイルシステム管理*”を参照してください。

説明

public-key local export dsa コマンドは指定した形式のローカル DSA ホスト公開鍵を表示あるいはファイルにエクスポートします。

ローカル DSA ホスト公開鍵をピアの装置に分配する前に、コマンドを使用して表示あるいはエクスポートすることができます。

1) ローカルホスト公開鍵を以下のいずれかの方法でファイルに保存します。
   - **public-key local export dsa** [**name** *key-name*] { **openssh** | **ssh2** }コマンドを使用し、指定した形式のローカルホスト公開鍵を表示します。内容をコピーし、ファイルにペーストします。

- **public-key local export dsa** [**name** *key-name*] { **openssh** | **ssh2** } *filename* コマンドを使用し、ファイルにローカルホスト公開鍵をエクスポートします。ホスト公開鍵をフォルダ pkey あるいはサブフォルダにエクスポートすることはできません。

2) バイナリモードの FTP あるいは TFTP などを使用してファイルのコピーをピアの装置に転送します。
3) ピアの装置でファイルから **public-key peer import sshkey** コマンドを使用してホスト公開鍵をインポートします。

SSH2.0 と OpenSSH は異なる公開鍵形式です。ホスト公開鍵をインポートする装置でサポートされる形式に従って適切に選択してください。

例

OpenSSH 形式のデフォルト名のローカル DSA 鍵ペアのホスト公開鍵をファイル key.pub にエクスポートします。

<AC> system-view

[AC] public-key local export dsa openssh key.pub

SSH2.0 形式のデフォルト名のローカル DSA 鍵ペアのホスト公開鍵を表示します。

<AC> system-view

[AC] public-key local export dsa ssh2

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-2011/05/12"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5
sJlhUiJ3B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKN
l/BnjXcitTQchQbzWCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIE
AgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UI
LiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9
LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxwvA7PvOVEA89tKni/f6GDBvWY9Z2Q499pAqUBt
YcqQea8T4zBInxx2eF3lLaZJrIvAS205zXxSzQoU9190kakdMdasIjQLWYGyepFc3sTwmIflQeweU
wLVAPaOesKaCERjxg+e4maYWlAvySGT4c9NJlxLo=
---- END SSH2 PUBLIC KEY ----
```

OpenSSH 形式のデフォルト名のローカル DSA 鍵ペアのホスト公開鍵を表示します。

<AC> system-view

[AC] public-key local export dsa openssh

```
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5
sJlhUiJ3B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKN
l/BnjXcitTQchQbzWCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIE
AgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UI
LiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9
LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxwvA7PvOVEA89tKni/f6GDBvWY9Z2Q499pAqUBt
```

```
YcqQea8T4zBInxx2eF3lLaZJrIvAS205zXxSzQoU9190kakdMdasIjQLWYGyepFc3sTwmIflQeweU
wLVAPaOesKaCERjxg+e4maYWlAvySGT4c9NJlxLo= dsa-key
```

OpenSSH 形式のローカル DSA 鍵ペア dsa1 のホスト公開鍵をファイル dsa1.pub にエクスポートします。

<AC> system-view

[AC] public-key local export dsa name dsa1 openssh dsa1.pub

SSH2.0 形式のローカル DSA 鍵ペア dsa1 のホスト公開鍵を表示します。

<AC> system-view

[AC] public-key local export dsa name dsa1 ssh2

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-2011/05/12"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5
sJlhUiJ3B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKN
l/BnjXcitTQchQbzWCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIE
AgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UI
LiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9
LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98qGmtaboNkK0YEAkRdp+QDZxX0aPdmVeEU1GC3
ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEYZullatZRH0km+DdpZ7CrcV+ft7UUv
BF0FV3W4HOx/LOidJ5sX+qBAD4WcpSX0OrZEF4+dq
---- END SSH2 PUBLIC KEY ----
```

OpenSSH 形式のローカル DSA 鍵ペア dsa1 のホスト公開鍵を表示します。

<AC> system-view

[AC] public-key local export dsa name dsa1 openssh

```
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5
sJlhUiJ3B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKN
l/BnjXcitTQchQbzWCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIE
AgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UI
LiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9
LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98qGmtaboNkK0YEAkRdp+QDZxX0aPdmVeEU1GC3
ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEYZullatZRH0km+DdpZ7CrcV+ft7UUv
BF0FV3W4HOx/LOidJ5sX+qBAD4WcpSX0OrZEF4+dq dsa-key
```

関連コマンド

- **public-key local create**
- **public-key peer import sshkey**

5.1.7 public-key local export rsa

Syntax

public-key local export rsa [**name** *key-name*] { **openssh** | **ssh1** | **ssh2** } [*filename*]

View

System view

定義済みユーザロール

network-admin

パラメータ

name *key-name*: ローカル RSA 鍵ペアの名前を指定します。設定範囲は 1～64 文字です。英字、数字、ハイフン（-）を含みます。名前を指定しない場合、デフォルト名のローカル鍵 RSA ペアのホスト公開鍵を表示あるいはエクスポートします。

openssh: OpenSSH の形式を使用します。

ssh1: SSH1.5 の形式を使用します。

ssh2: SSH2.0 の形式を使用します。

filename: 保存するローカルホスト公開鍵の名前を指定します。設定範囲は 1～128 文字です。大文字、小文字を区別しません。”./”、”../”を除いて指定します。名前は、ドット（.）、hostkey、serverkey、dsakey、ecdsakey を使用することができません。また先頭をスラッシュにすることができません。*filename* が指定されている場合、ローカル RSA ホスト公開鍵をエクスポートします。指定されていない場合、ローカル RSA ホスト公開鍵を表示します。ファイル名の詳細はオペレーションマニュアルのセクション 1 *はじめに “ファイルシステム管理”* を参照してください。

説明

public-key local export rsa コマンドは指定した形式のローカル RSA ホスト公開鍵を表示あるいはファイルにエクスポートします。

ローカル DSA ホスト公開鍵をピアの装置に分配する前に、コマンドを使用して表示あるいはエクスポートすることができます。

1) ローカルホスト公開鍵を以下のいずれかの方法でファイルに保存します。
   - **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh2** }コマンドを使用し、指定した形式のローカルホスト公開鍵を表示します。内容をコピーし、ファイルにペーストします。
   - **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh2** } *filename* コマンドを使用し、ファイルにローカルホスト公開鍵をエクスポートします。ホスト公開鍵をフォルダ pkey あるいはサブフォルダにエクスポートすることはできません。
2) バイナリモードの FTP あるいは TFTP などを使用してファイルのコピーをピアの装置に転送します。

3) ピアの装置でファイルから **public-key peer import sshkey** コマンドを使用してホスト公開鍵をインポートします。

SSH1.5、SSH2.0、OpenSSH は異なる公開鍵形式です。ホスト公開鍵をインポートする装置でサポートされる形式に従って適切に選択してください。

例

OpenSSH 形式のデフォルト名のローカル RSA 鍵ペアのホスト公開鍵をファイル key.pub にエクスポートします。

<AC> system-view

[AC] public-key local export rsa openssh key.pub

SSH2.0 形式のデフォルト名のローカル RSA 鍵ペアのホスト公開鍵を表示します。

<AC> system-view

[AC] public-key local export rsa ssh2

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-2011/05/12"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDapKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGM
rSfddq/bYcbgM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+XOvy
vPJilneKJqhPT0xdv4tlas+mLNloY0dImbwS2kwE71rgg1CQ==
---- END SSH2 PUBLIC KEY ----
```

OpenSSH 形式のデフォルト名のローカル RSA 鍵ペアのホスト公開鍵を表示します。

<AC> system-view

[AC] public-key local export rsa openssh

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDapKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGM
rSfddq/bYcbgM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+XOvy
vPJilneKJqhPT0xdv4tlas+mLNloY0dImbwS2kwE71rgg1CQ== rsa-key
```

OpenSSH 形式のローカル RSA 鍵ペア rsa1 のホスト公開鍵をファイル rsa1.pub にエクスポートします。

<AC> system-view

[AC] public-key local export rsa name rsa1 openssh rsa1.pub

SSH2.0 形式のローカル RSA 鍵ペア rsa1 のホスト公開鍵を表示します。

<AC> system-view

[AC] public-key local export rsa name rsa1 ssh2

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-2011/05/12"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDevEbyF93xHUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J0
0fBQ8XY+q2olqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05
t8mCLVaupbfCzP8ba8UkrUmMO4fUvW6zavA5LYxtlAiQv0KQ==
---- END SSH2 PUBLIC KEY ----
```

OpenSSH 形式のローカル RSA 鍵ペア rsa1 のホスト公開鍵を表示します。

<AC> system-view

[AC] public-key local export rsa name rsa1 openssh

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDevEbyF93xHUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J0
0fBQ8XY+q2olqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05
t8mCLVaupbfCzP8ba8UkrUmMO4fUvW6zavA5LYxtlAiQv0KQ== rsa-key
```

関連コマンド

- **public-key local create**
- **public-key peer import sshkey**

5.1.8 public-key peer

Syntax

public-key peer *keyname*

undo public-key peer *keyname*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

keyname: ピアの公開鍵の名前を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別します。

説明

public-key peer コマンドはピアのホスト公開鍵の名前を指定し、その view に移行するか、既存の public key view に移行します。

undo public-key peer コマンドはピアのホスト公開鍵を削除します。

public key view に移行するため、コマンドを実行した後、公開鍵を入力します。半角スペースと改行は入力できますが、保存されません。

ローカル装置でピアの公開鍵を手動で指定するため、最初に 16 進数のピアの公開鍵を取得し、ローカル装置で以下の処理を行ってください。

1)　public key view に移行するため、**public-key peer** コマンドを実行します。

2)　公開鍵を入力します。

3)　**peer-public-key end** コマンドを実行し、公開鍵を保存し、system view に戻ります。

public key view で正しい形式の公開鍵を入力してください。ピアの装置が QX シリーズである場合、公開鍵を記録するため、**display public-key local public** コマンドを使用することを推奨します。

例

ピアの公開鍵 key1 を指定し、public key view に移行します。

<AC> system-view

[AC] public-key peer key1

[AC-pkey-public-key-key1]

関連コマンド

- **display public-key local public**
- **display public-key peer**
- **peer-public-key end**

5.1.9 public-key peer import sshkey

Syntax

public-key peer *keyname* **import sshkey** *filename*

undo public-key peer *keyname*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

keyname: ピアの公開鍵の名前を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別します。

filename: 保存するピアの公開鍵の名前を指定します。設定範囲は 1～128 文字です。大文字、小文字を区別しません。"./"、"../"を除いて指定します。名前は、ドット(.)、hostkey、serverkey、dsakey、ecdsakey を使用することができません。また先頭をスラッシュにすることができません。ファイル名の詳細はオペレーションマニュアルのセクション 1 *はじめに* *"ファイルシステム管理"* を参照してください。

説明

public-key peer import sshkey コマンドは公開鍵ファイルからピアのホスト公開鍵をインポートします。

undo public-key peer コマンドは指定したピアのホスト公開鍵を削除します。

ピアのホスト公開鍵をインポートする前に、バイナリモードで FTP または TFTP を使用してピアの装置から公開鍵のファイルのコピーの取得を行ってください。

このコマンドを設定した後、システムは自動的に PKCS（Public Key Cryptography Standards）形式にホスト公開鍵を変換し、保存します。

装置は SSH1.5、SSH2.0、OpenSSH の形式の公開鍵をインポートすることができます。

例

公開鍵ファイル key.pub からピアのホスト公開鍵 key2 をインポートします。

<AC> system-view

[AC] public-key peer key2 import sshkey key.pub

関連コマンド

- **display public-key peer**
- **public-key local export dsa**
- **public-key local export rsa**

目次

このセクションのページは **9-x-x** です。

6 章 SSH 6-1
6.1 SSH サーバ設定コマンド 6-1
6.1.1 display ssh server 6-1
6.1.2 display ssh user-information 6-3
6.1.3 sftp server enable 6-5
6.1.4 sftp server idle-timeout 6-5
6.1.5 ssh server acl 6-6
6.1.6 ssh server authentication-retries 6-7
6.1.7 ssh server authentication-timeout 6-8
6.1.8 ssh server compatible-ssh1x enable 6-9
6.1.9 ssh server dscp 6-10
6.1.10 ssh server enable 6-11
6.1.11 ssh server port 6-12
6.1.12 ssh server rekey-interval 6-13
6.1.13 ssh user 6-14
6.2 SSH クライアント設定コマンド 6-16
6.2.1 bye 6-16
6.2.2 cd 6-17
6.2.3 cdup 6-18
6.2.4 delete 6-18
6.2.5 dir 6-19
6.2.6 display sftp client source 6-20
6.2.7 display ssh client source 6-21
6.2.8 exit 6-21
6.2.9 get 6-22
6.2.10 help 6-23
6.2.11 ls 6-24
6.2.12 mkdir 6-25
6.2.13 put 6-25
6.2.14 pwd 6-26
6.2.15 quit 6-26
6.2.16 remove 6-27
6.2.17 rename 6-28
6.2.18 rmdir 6-28
6.2.19 sftp 6-29
6.2.20 sftp client source 6-31

6.2.21 ssh client source..... 6-32
6.2.22 ssh2..... 6-33

6章 SSH

6.1 SSHサーバ設定コマンド

6.1.1 display ssh server

Syntax

display ssh server { **session** | **status** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

session: SSH サーバのセッションを表示します。

status: SSH サーバの状態を表示します。

説明

display ssh server コマンドは SSH サーバで SSH サーバのセッションあるいは状態を表示します。

例

SSH サーバの状態を表示します。

<AC> display ssh server status

```
Stelnet server: Disable
SSH version : 2.0
SSH authentication-timeout : 60 second(s)
SSH server key generating interval : 0 hour(s)
SSH authentication retries : 3 time(s)
SFTP server: Disable
SFTP server Idle-Timeout: 10 minute(s)
NETCONF server: Disable
SCP server: Disable
```

表 6-1 コマンド出力

フィールド	説明
Stelnet server	Stelnetサーバ機能が有効かどうかを示します。
SSH version	SSHプロトコルのバージョンです。 SSH1をサポートしている場合、プロトコルバージョンは1.99です。その他の場合、プロトコルバージョンは2です。
SSH authentication-timeout	認証タイムアウトタイマです。
SSH server key generating interval	SSHサーバ鍵ペアのアップデート間隔です。
SSH authentication retries	SSHユーザの認証の最大試行回数です。
SFTP server	SFTPサーバ機能が有効かどうかを示します。
SFTP server Idle-Timeout	SFTP接続アイドルタイムアウトタイマです。
Netconf server	NETCONF over SSHが有効かどうかを示します。 NETCONF over SSHはサポートしていません。
SCP server	SCPサーバ機能が有効かどうかを示します。 SCPサーバ機能はサポートしていません。

SSH サーバのセッションを表示します。

<AC> display ssh server session

```
UserPid   SessID Ver   Encrypt    State        Retries  Serv     Username   Idx
 184       0     2.0   aes128-cbc Established   1       Stelnet  abc@123
```

表 6-2 コマンド出力

フィールド	説明
UserPid	ユーザプロセスIDです。
SessID	セッションIDです。
Ver	SSHサーバのプロトコルバージョンです。
Encrypt	SSHサーバで使用される暗号化アルゴリズムです。

フィールド	説明
State	セッション状態です。 ● **Init**–初期化状態です。 ● **Ver-exchange**–バージョンのネゴシエーション状態です。 ● **Keys-exchange**–鍵交換状態です。 ● **Auth-request**–認証要求状態です。 ● **Serv-request**–セッションサービス要求状態です。 ● **Established**–セッションが確立されています。 ● **Disconnected**–セッションが切断されています。
Retries	認証に失敗した数です。
Serv	サービスタイプです。 ● SCPです。 ● SFTPです。 ● Stelnetです。 ● NETCONFです。
Username	サーバにログインしているユーザ名です。
Idx	クライアントがサーバにログインするために使用するユーザ行の絶対数。ユーザのSSH接続がリダイレクトされない場合、このフィールドの値は空です。

6.1.2 display ssh user-information

Syntax

display ssh user-information [*username*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

username: SSH ユーザ名を指定します。設定範囲は 1～80 文字です。大文字、小文字を区別します。指定しない場合、すべての SSH ユーザの情報を表示します。

説明

display ssh user-information コマンドは SSH サーバの SSH ユーザの情報を表示します。

このコマンドは、SSH サーバ上で **ssh user** コマンドを使用して設定された SSH ユーザのみの情報を表示します。

例

すべての SSH ユーザの情報を表示します。

<AC> display ssh user-information

```
Total ssh users:2
Username          Authentication-type  User-public-key-name  Service-type
yemx              password                                   Stelnet|SFTP
test              publickey          pubkey                  SFTP
```

表 6-3 コマンド出力

フィールド	説明
Total ssh users	SSHユーザの総数です。
Authentication-type	認証方式です。 ● パスワード認証です。 ● 公開鍵認証です。 ● パスワード-公開鍵認証です。 ● 他の認証です。
User-public-key-name	ユーザの公開鍵名です。パスワード認証が使用される場合、表示されません。
Service-type	サービスタイプです。 ● Stelnetです。 ● SFTPです。 ● SCPです。 ● NETCONFです。 SSHユーザで複数のサービスタイプが有効である場合、垂直バー（|）で区切られます。

関連コマンド

ssh user

6.1.3 sftp server enable

Syntax

sftp server enable

undo sftp server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

sftp server enable コマンドは SFTP サーバ機能を有効にします。

undo sftp server enable コマンドは SFTP サーバ機能を無効にします。

例

SFTP サーバ機能を有効にします。

<AC> system-view

[AC] sftp server enable

関連コマンド

display ssh server

6.1.4 sftp server idle-timeout

Syntax

sftp server idle-timeout *time-out-value*

undo sftp server idle-timeout

デフォルト

10 分

View

System view

定義済みユーザロール

network-admin

パラメータ

time-out-value: タイムアウトタイマを指定します。設定範囲は 1～35791 分です。

説明

sftp server idle-timeout コマンドは SFTP サーバの SFTP ユーザ接続のアイドルタイムアウトタイマを設定します。

undo sftp server idle-timeout コマンドはデフォルトに戻します。

アイドルタイムアウトタイマが終了したとき、SFTP 接続がアイドルである場合、システムは自動的に接続を切断します。多くの SFTP 接続が確立されている場合、接続リソースを即座に開放できるように、タイマを小さい値に設定することができます。

例

SFTP ユーザ接続のアイドルタイムアウトタイマを 500 分に設定します。

<AC> system-view

[AC] sftp server idle-timeout 500

関連コマンド

display ssh server

6.1.5 ssh server acl

Syntax

ssh server acl { *basic-acl-number* | *advanced-acl-number* | **mac** *mac-acl-number* }

undo ssh server acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

basic-acl-number: 標準 IPv4 ACL を指定します。設定範囲は 2000～2999 です。

advanced-acl-number: 拡張 IPv4 ACL を指定します。設定範囲は 3000～3999 です。

mac *mac-acl-number:* L2 ACL を指定します。設定範囲は 4000～4999 です。

説明

ssh server acl コマンドは IPv4 SSH サーバへのアクセスを制御します。

undo ssh server acl コマンドはデフォルトに戻します。

ACL を使用して IPv4 SSH クライアントの要求パケットをフィルタするために使用します。

- ACL ルールが設定されている場合、ACL の permit 条件に一致する IPv4 SSH クライアントの要求パケットのみがサーバにアクセスすることができます。
- ACL ルールが存在しない、あるいは ACL に条件がない場合、すべての IPv4 SSH クライアントがサーバにアクセスすることができます。

この設定は、設定した後に SSH 接続を行った要求パケットから有効になります。

このコマンドを複数実行した場合、最後に行われた設定が適用されます。

例

IPv4 SSH クライアント 1.1.1.1 のみサーバにアクセスできるように ACL 2001 を設定します。

<AC> system-view

[AC] acl basic 2001

[AC-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0

[AC-acl-ipv4-basic-2001] quit

[AC] ssh server acl 2001

関連コマンド

display ssh server

6.1.6 ssh server authentication-retries

Syntax

ssh server authentication-retries *times*

undo ssh server authentication-retries

デフォルト

3

View

System view

定義済みユーザロール

network-admin

パラメータ

times: SSH ユーザの認証を試行する最大数を指定します。設定範囲は 1～5 です。

説明

ssh server authentication-retries コマンドは SSH ユーザの認証を試行する最大数を指定します。

undo ssh server authentication-retries コマンドはデフォルトに戻します。

偽のユーザ名とパスワードの攻撃を防ぐため、最大数を設定することができます。

- 認証方式が any である場合、公開鍵とパスワード認証の合計の試行回数が設定した上限を超えることができません。
- 認証方式がパスワード-公開鍵である場合、SSH ユーザを認証するため、最初にサーバは公開鍵認証を使用し、ユーザパスワード認証を使用します。プロセスは 1 つの認証を行うものとして扱います。

この設定はログインユーザには適用されません。新しい SSH ユーザのみ適用されます。

例

SSH ユーザの認証を試行する最大数を 4 に設定します。

<AC> system-view

[AC] ssh server authentication-retries 4

関連コマンド

display ssh server

6.1.7 ssh server authentication-timeout

Syntax

ssh server authentication-timeout *time-out-value*

undo ssh server authentication-timeout

デフォルト

60 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

time-out-value: 認証タイムアウトタイマを指定します。設定範囲は 1～120 秒です。

説明

ssh server authentication-timeout コマンドは SSH サーバで SSH ユーザ認証のタイムアウトタイマを設定します。

undo ssh server authentication-timeout コマンドはデフォルトに戻します。

タイムアウトタイマが終了したとき、ユーザが認証を終了しない場合、接続は確立することができません。

タイムアウトタイマの値を小さくすることで、認証が中断される間に、偽の TCP 接続による占有を防ぐことができます。

例

SSH ユーザ認証のタイムアウトタイマを 10 秒に設定します。

<AC> system-view

[AC] ssh server authentication-timeout 10

関連コマンド

display ssh server

6.1.8 ssh server compatible-ssh1x enable

Syntax

ssh server compatible-ssh1x enable

undo ssh server compatible-ssh1x

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

network-operator

説明

ssh server compatible-ssh1x enable コマンドは SSH1 クライアントをサポートする SSH サーバを有効にします。

undo ssh server compatible-ssh1x コマンドは SSH サーバで SSH1 クライアントのサポートを無効にします。

この設定はログインユーザには適用されません。次回ログインしたユーザのみ適用します。

例

SSH1 クライアントをサポートする SSH サーバを有効にします。

<AC> system-view

[AC] ssh server compatible-ssh1x enable

関連コマンド

display ssh server

6.1.9 ssh server dscp

Syntax

ssh server dscp *dscp-value*

undo ssh server dscp

デフォルト

48

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: 送信 IPv4 パケットの DHCP を指定します。設定範囲は 0〜63 です。

説明

ssh server dscp コマンドは SSH サーバが SSH クライアントに IPv4 パケットを送信する DHCP を設定します。

undo ssh server dscp コマンドはデフォルトに戻します。

DHCP パケットの DSCP の値はパケットのプライオリティを指定します。パケットを送信するプライオリティに影響します。DSCP の値が大きくなると、プライオリティが高くなります。

例

SSH サーバによって送信される IPv4 パケットの DSCP を 30 に設定します。

<AC> system-view

[AC] ssh server dscp 30

6.1.10 ssh server enable

Syntax

ssh server enable

undo ssh server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ssh server enable コマンドは Stelnet サーバ機能を有効にします。

undo ssh server enable コマンドは Stelnet サーバ機能を無効にします。

例

Stelnet サーバ機能を有効にします。

<AC> system-view

[AC] ssh server enable

関連コマンド

display ssh server

6.1.11 ssh server port

🕮 **メモ**：

このコマンドはソフトウェアバージョン 7.2.73 を含む以降のソフトウェアからサポートしています。

Syntax

ssh server port *port-number*

undo ssh server port

デフォルト

SSH server port：22

View

System view

定義済みユーザロール

network-admin

パラメータ

port-number: ポート番号を 1～65535 の範囲で指定します。

説明

ssh server port を使用して SSH サービスポートを指定します。

undo ssh server port を使用してデフォルトに戻します。

⚠ **注意:**

- SSH サーバが有効な状態で SSH ポート番号を変更すると、変更後は、SSH サービスが再起動し、すべての SSH 接続が切断されます。SSH ユーザがサーバにアクセスする場合は、SSH サーバに再接続してください。
- SSH ポートを well-known ポート番号に設定した場合、well-known ポート番号を使用したサービスが起動できない場合があります。well-known ポート番号として設定できる範囲は 1～1024 です。

例

SSH サービスポートを 1025 に設定します。

<AP> system-view

[AP] ssh server port 1025

6.1.12 ssh server rekey-interval

Syntax

ssh server rekey-interval *hours*

undo ssh server rekey-interval

デフォルト

アップデート間隔の値は 0 時間です。

View

System view

定義済みユーザロール

network-admin

パラメータ

hours: RSA サーバ鍵ペアのアップデート間隔を指定します。設定範囲は 1～24 時間です。

説明

ssh server rekey-interval コマンドは RSA サーバ鍵ペアのアップデート間隔を設定します。

undo ssh server rekey-interval コマンドはデフォルトに戻します。

RSA サーバ鍵ペアを定期的にアップデートすることで、鍵ペアのハッキングを防ぎ、SSH 接続のセキュリティを強化することができます。

システムはSSH1ユーザがサーバにログイン後にアップデート最小間隔を数え始めます。新しい SSH1 ユーザがアップデート最小間隔後にサーバにログインする場合、システムは以下の操作をします。

1) RSA サーバ鍵ペアをアップデートします。
2) 新しいユーザの鍵ペアネゴシエーションにアップデートされた RSA サーバ鍵ペアを使用します。
3) アップデート最小間隔を再び数え始めます。

このコマンドは、SSH1 クライアントソフトウェアを使用する SSH クライアントのみ適用します。

例

RSA サーバ鍵ペアのアップデート間隔を 3 時間に設定します。

<AC> system-view

[AC] ssh server rekey-interval 3

関連コマンド

display ssh server

6.1.13 ssh user

Syntax

ssh user *username* **service-type** { **all** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* } }

undo ssh user *username*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

username: SSH ユーザ名を指定します。設定範囲は 1～80 文字です。大文字、小文字を区別します。ユーザ名に ISP ドメイン名が含まれる場合、*pureusername@domain*、*pureusername/domain* 、または *domain¥pureusername* の形式を使用します。*pureusername* の設定範囲は 1～55 文字です。*domain* の設定範囲は 1～24 文字です。SCP ユーザのユーザ名にハイフン（-）を含めないでください。そうしないと、そのユーザ名を使用する SCP ログインは失敗します。

service-type: SSH ユーザのサービスタイプを指定します。

- **all**: Stelnet、SFTP を指定します。
- **sftp**: SFTP のサービスタイプを指定します。
- **stelnet**: Stelnet のサービスタイプを指定します。

authentication-type: SSH ユーザの認証方法を指定します。

- **password**: パスワード認証を指定します。認証方式は容易で暗号時間が早くなりますが、セキュリティ強度は脆弱です。ユーザ認証、許可、アカウンティングを実行する AAA と同時に使用することができます。
- **any**: パスワード認証あるいは公開鍵認証のどちらかを指定します。
- **password-publickey**: SSH2 クライアントのパスワード認証と公開鍵認証の両方を指定します。SSH2 クライアントでは、**password-publickey** 認証方式は高いセキュリティを提供します。SSH1 クライアントではパスワード認証あるいは公開鍵認証のどちらかを指定します。

- **publickey**: 公開鍵認証を指定します。認証方式は複雑で暗号時間が遅いですが、セキュリティ強度は強くなり、総当たり攻撃（ブルートフォース攻撃）に対して防御することができます。この認証方式は、使用しやすいです。一度設定すると、パスワードを記憶しておくことやパスワードを入力することなく、認証プロセスが自動で完了します。

assign: クライアントを確認するために使用するパラメータを指定します。

- **publickey** *keyname*: SSH クライアントの公開鍵を指定します。*keyname* はサーバで設定される SSH クライアントの公開鍵を示します。設定範囲は 1～64 文字です。大文字、小文字を区別しません。サーバはクライアントの確認を行うため、クライアントの公開鍵を使用します。もしクライアントの公開鍵のファイルが変更されている場合、すぐにサーバのクライアントの公開鍵をアップデートする必要があります。

説明

ssh user コマンドは SSH ユーザを作成し、サービスタイプと認証方式を指定します。

undo ssh user コマンドは SSH ユーザを削除します。

SSH ユーザを設定するため、認証方式に従ってコマンドを使用します。

- 認証方式が公開鍵である場合、SSH ユーザとローカルユーザを作成する必要があります。SSH ユーザが正しい作業ディレクトリとユーザロールを割り当てられるように、ローカルユーザは SSH ユーザのユーザ名と同一にする必要があります。
- 認証方式がパスワードである場合、SSH ユーザは以下の処理のどちらか 1 つを実行する必要があります。
  - ローカル認証用に、**local-user** コマンドを使用してローカルユーザを設定します。
  - リモート認証用に、RADIUS サーバのようなリモート認証サーバの SSH ユーザを設定します。

  ssh user コマンドを使用して SSH ユーザを作成する必要がありません。しかし、集中管理のため、すべての SSH ユーザ（パスワード認証のみの SSH ユーザを含みます）を表示する場合、このコマンドを使用することができます。SSH ユーザが作成された場合、正しいサービスタイプと認証方式であることを確認してください。
- 認証方式が **password-publickey** あるいは **any** である場合、SSH ユーザは以下の処理のどちらか 1 つを実行する必要があります。
  - ローカル認証用に、**local-user** コマンドを使用してローカルユーザを設定します。
  - リモート認証用に、RADIUS サーバのようなリモート認証サーバの SSH ユーザを設定します。

  どちらの場合でも、ローカルユーザあるいはリモート認証サーバで設定される SSH ユーザは SSH ユーザと同じユーザ名を使用する必要があります。

ホスト公開鍵を指定するため、このコマンドを複数回使用した場合、最後に行った設定が適用されます。

ユーザが SSH サーバと通信しているとき、SSH ユーザの認証方式、サービスタイプ、ホスト公開鍵を変更することができますが、設定の変更は次回ログインのクライアントのみ適用されます。

SFTP ユーザでは、作業ディレクトリは認証方式に依存します。

- 認証方式がパスワードである場合、作業ディレクトリはAAAによって許可されます。
- 認証方式が **publickey** あるいは **password-publickey** である場合、作業ディレクトリは、関連した local user view で **authorization-attribute** コマンドを使用して指定されます。

SSH ユーザでは、ユーザロールは認証方式に依存します。

- 認証方式がパスワードである場合、ユーザロールはリモート AAA サーバあるいはローカル装置によって許可されます。
- 認証方式が **publickey** あるいは **password-publickey** である場合、ユーザロールは関連した local user view で **authorization-attribute** コマンドを使用して指定されます。

例

SSH ユーザ user1 を作成します。ユーザにサービスタイプ sftp、認証方式 password-publickey を指定します。ユーザにホスト公開鍵 key1 を割り当てます。

<AC> system-view

[AC] ssh user user1 service-type sftp authentication-type password-publickey assign publickey key1

ローカル装置管理ユーザ user1 を作成します。プレーンテキストでパスワード 123456TESTplat&!を指定し、ユーザのサービスタイプ ssh を指定します。作業ディレクトリ cfa0:を割り当て、ユーザにユーザロール network-admin を割り当てます。

[AC] local-user user1 class manage

[AC-luser-manage-user1] password simple 123456TESTplat&!

[AC-luser-manage-user1] service-type ssh

[AC-luser-manage-user1] authorization-attribute work-directory cfa0: user-role network-admin

関連コマンド

- **authorization-attribute**
- **display ssh user-information**
- **local-user**
- **pki domain**

6.2 SSHクライアント設定コマンド

6.2.1 bye

Syntax

bye

View

SFTP client view

定義済みユーザロール

network-admin

説明

bye コマンドは SFTP サーバとの通信を終了し、user view に戻ります。

このコマンドは **exit** コマンド、**quit** コマンドと同一です。

例

SFTP サーバとの通信を終了し、user view に戻ります。

sftp> bye

<AC>

6.2.2 cd

Syntax

cd [*remote-path*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-path: サーバのパスの名前を指定します。

説明

cd コマンドは SFTP サーバの作業パスを変更します。

上位のディレクトリに戻るため、**cd ..**コマンドを使用できます。

ルートディレクトリに戻るため、**cd /**コマンドを使用できます。

例

作業パスを new1 に変更します。

sftp> cd new1

Current Directory is:/new1

sftp> pwd

```
Remote working directory: /new1
sftp>
```

6.2.3 cdup

Syntax

cdup

View

SFTP client view

定義済みユーザロール

network-admin

説明

cdup コマンドは上位のディレクトリに戻ります。

例

現在の作業ディレクトリ/test1 から上位のディレクトリに戻ります。

sftp> cd test1

```
Current Directory is:/test1
```

sftp> pwd

```
Remote working directory: /test1
```

sftp> cdup

```
Current Directory is:/
```

sftp> pwd

```
Remote working directory: /
sftp>
```

6.2.4 delete

Syntax

delete *remote-file*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-file: サーバから削除するファイルを指定します。

説明

delete コマンドはサーバからファイルを削除します。

このコマンドは **remove** コマンドと同一です。

例

サーバからファイル temp.c を削除します。

sftp> delete temp.c

```
Removing /temp.c
```

6.2.5 dir

Syntax

dir [**-a** | **-l**] [*remote-path*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

-a: リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。ドット（.）で始まる名前のファイルとサブディレクトリも含みます。

-l: リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。ドット（.）で始まる名前のファイルとサブディレクトリは除きます。

remote-path: ディレクトリの名前を指定します。指定しない場合、現在の作業ディレクトリの下にあるファイルとディレクトリの詳細情報を表示します。

説明

dir コマンドはディレクトリの下にあるファイルとサブディレクトリの情報を表示します。

-**a** あるいは-**l** のいずれも指定しない場合、ディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。

このコマンドは **ls** コマンドと同一です。

例

リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。ドット（.）で始まる名前のファイルとサブディレクトリも含みます。

sftp> dir -a

```
drwxrwxrwx    2 1       1             512 Dec 18 14:12 .
drwxrwxrwx    2 1       1             512 Dec 18 14:12 ..
-rwxrwxrwx    1 1       1             301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1       1             301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1       1             301 Dec 18 14:12 012.pub
```

リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。

sftp> dir -l

```
-rwxrwxrwx    1 1       1             301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1       1             301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1       1             301 Dec 18 14:12 012.pub
```

🕮 **メモ**：

出力形式は、SSH サーバ装置モデルによって異なります。

6.2.6 display sftp client source

Syntax

display sftp client source

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display sftp client source コマンドは SFTP クライアントの送信元 IP アドレスを表示します。

例

SFTP クライアントの送信元 IP アドレスを表示します。

<AC> display sftp client source

```
The source IP address of the SFTP client is 192.168.0.1
```

関連コマンド

sftp client source

6.2.7 display ssh client source

Syntax

display ssh client source

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ssh client source コマンドは Stelnet クライアントの送信元 IP アドレスを表示します。

例

Stelnet クライアントの送信元 IP アドレスを表示します。

<AC> display ssh client source

```
The source IP address of the SSH client is 192.168.0.1
```

関連コマンド

ssh client source

6.2.8 exit

Syntax

exit

View

SFTP client view

定義済みユーザロール

network-admin

説明

exit コマンドは SFTP サーバとの通信を終了し、user view に戻ります。

このコマンドは **bye** コマンド、**quit** コマンドと同一です。

例

SFTP サーバとの通信を終了し、user view に戻ります。

sftp> exit

<AC>

6.2.9 get

Syntax

get *remote-file* [*local-file*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-file: SFTP サーバの名前を指定します。

local-file: ローカルファイルの名前を指定します。指定しない場合、ファイルはサーバのファイルと同一の名前で保存されます。

説明

get コマンドは FTP サーバからファイルをダウンロードし、ローカルにファイルを保存します。

例

ファイル temp1.c をダウンロードし、ローカルにファイル temp.c として保存します。

sftp> get temp1.c temp.c

```
Fetching /temp1.c to temp.c
/temp.c                                       100% 1424     1.4KB/s   00:00
```

6.2.10 help

Syntax

help

View

SFTP client view

定義済みユーザロール

network-admin

説明

help コマンドは SFTP クライアントコマンドのヘルプ情報を表示します。

このコマンドはクォーテーションマーク（?）を入力した場合と同一です。

例

SFTP クライアントでヘルプ情報を表示します。

sftp> help

```
Available commands:
  bye                       Quit sftp
  cd [path]                  Change remote directory to 'path'
  cdup                      Change remote directory to the parent directory
  delete path                Delete remote file
  dir [-a|-l][path]           Display remote directory listing
      -a                     List all filenames
      -l                     List filename including the specific
                             information of the file
  exit                      Quit sftp
  get remote-path [local-path] Download file
  help                      Display this help text
  ls [-a|-l][path]            Display remote directory
      -a                      List all filenames
      -l                      List filename including the specific
                              information of the file
  mkdir path                 Create remote directory
  put local-path [remote-path] Upload file
  pwd                       Display remote working directory
  quit                      Quit sftp
  rename oldpath newpath      Rename remote file
  remove path                Delete remote file
  rmdir path                 Delete remote empty directory
  ?                         Synonym for help
```

6.2.11 ls

Syntax

ls [**-a** | **-l**] [*remote-path*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

-a: リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。ドット（.）で始まる名前のファイルとサブディレクトリも含みます。

-l: リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。ドット（.）で始まる名前のファイルとサブディレクトリは除きます。

remote-path: ディレクトリの名前を指定します。指定しない場合、現在の作業ディレクトリの下にあるファイルとディレクトリの詳細情報を表示します。

説明

ls コマンドはディレクトリの下にあるファイルとサブディレクトリの情報を表示します。

-a あるいは**-l** のいずれも指定しない場合、ディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。

このコマンドは **dir** コマンドと同一です。

例

リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。ドット（.）で始まる名前のファイルとサブディレクトリも含みます。

sftp> ls -a

```
drwxrwxrwx    2 1       1             512 Dec 18 14:12 .
drwxrwxrwx    2 1       1             512 Dec 18 14:12 ..
-rwxrwxrwx    1 1       1             301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1       1             301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1       1             301 Dec 18 14:12 012.pub
```

リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。

sftp> ls -l

```
-rwxrwxrwx    1 1       1             301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1       1             301 Dec 18 14:12 011.pub
```

```
-rwxrwxrwx   1 1      1           301 Dec 18 14:12 012.pub
```

🕮 **メモ：**

出力形式は、SSH サーバ装置モデルによって異なります。

6.2.12 mkdir

Syntax

mkdir *remote-path*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-path: SFTP サーバのディレクトリ名を指定します。

説明

mkdir コマンドは SFTP サーバ上にディレクトリを作成します。

例

SFTP サーバ上にディレクトリを作成します。

sftp> mkdir test

6.2.13 put

Syntax

put *local-file* [*remote-file*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

local-file: ローカルファイルの名前を指定します。

remote-file: SFTP サーバの名前を指定します。指定しない場合、ファイルはローカルファイルと同一の名前で保存されます。

説明

put コマンドは SFTP サーバにローカルファイルをアップロードします。

例

SFTP サーバにローカルファイル startup.bak をアップロードし、startup01.bak として保存します。

sftp> put startup.bak startup01.bak

```
Uploading startup.bak to /startup01.bak
startup01.bak                                 100% 1424     1.4KB/s   00:00
```

6.2.14 pwd

Syntax

pwd

View

SFTP client view

定義済みユーザロール

network-admin

説明

pwd コマンドは SFTP サーバの現在の作業ディレクトリを表示します。

例

SFTP サーバの現在の作業ディレクトリを表示します。

sftp> pwd

```
Remote working directory: /
```

出力では、現在の作業ディレクトリはルートディレクトリであることを示します。

6.2.15 quit

Syntax

quit

View

SFTP client view

定義済みユーザロール

network-admin

説明

quit コマンドは SFTP サーバとの通信を終了し、user view に戻ります。

このコマンドは **bye** コマンド、**exit** コマンドと同一です。

例

SFTP サーバとの通信を終了し、user view に戻ります。

sftp> quit

<AC>

6.2.16 remove

Syntax

remove *remote-file*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-file: ファイルを指定します。

説明

remove コマンドは SFTP サーバからファイルを削除します。

このコマンドは **delete** コマンドと同一です。

例

SFTP サーバからファイル temp.c を削除します。

sftp> remove temp.c

```
Removing /temp.c
```

6.2.17 rename

Syntax

rename *old-name new-name*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

old-name: 既存のファイルあるいはディレクトリの名前を指定します。

new-name: 新しいファイルあるいはディレクトリの名前を指定します。

説明

rename コマンドは SFTP サーバのファイルあるいはディレクトリの名前を変更します。

例

SFTP サーバのファイルの名前を temp1.c から temp2.c に変更します。

sftp> dir

```
aa.pub  temp1.c
```

sftp> rename temp1.c temp2.c

sftp> dir

```
aa.pub  temp2.c
```

6.2.18 rmdir

Syntax

rmdir *remote-path*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-path: ディレクトリを指定します。

説明

rmdir コマンドは SFTP サーバからディレクトリを削除します。

例

SFTP サーバの現在のディレクトリの下のサブディレクトリ temp1 を削除します。

sftp> rmdir temp1

6.2.19 sftp

Syntax

sftp *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

View

User view

定義済みユーザロール

network-admin

パラメータ

server: IPv4 アドレスあるいはホスト名でサーバを指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。

port-number: サーバのポート番号を指定します。設定範囲は 1～65535 です。デフォルトは 22 です。

identity-key: クライアントの公開鍵アルゴリズムを指定します。サーバが公開鍵認証を使用する場合、指定する必要があります。クライアントはアルゴリズムに関連したローカル秘密鍵を使用してデジタル署名を作成します。

- **dsa**: 公開鍵アルゴリズム dsa を指定します。
- **rsa**: 公開鍵アルゴリズム rsa を指定します。

prefer-compress: サーバとクライアント間で優先される圧縮アルゴリズムを指定します。

zlib: 圧縮アルゴリズム zlib を指定します。

prefer-ctos-cipher: クライアントからサーバへの優先される暗号化アルゴリズムを指定します。アルゴリズム **des-cbc**、**3des-cbc**、**aes128-cbc** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

優先クライアントからサーバへの暗号化アルゴリズムを指定します。 デフォルトは aes128-cbc です。

次のアルゴリズムは、セキュリティ強度と計算時間の昇順で表示されます。

- **des-cbc**: 暗号化アルゴリズム des-cbc を指定します。
- **3des-cbc**: 暗号化アルゴリズム 3des-cbc を指定します。
- **aes128-cbc**: 暗号化アルゴリズム aes128-cbc を指定します。

prefer-ctos-hmac: クライアントからサーバへの優先される HMAC アルゴリズムを指定します。

- **md5:** HMAC アルゴリズム hmac-md5 を指定します。
- **md5-96:** HMAC アルゴリズム hmac-md5-96 を指定します。
- **sha1:** HMAC アルゴリズム hmac-sha1 を指定します。アルゴリズム sha1 は md5 よりもセキュリティの強度が強くなるが、計算時間が長くなります。
- **sha1-96:** HMAC アルゴリズム hmac-sha1-96 を指定します。

prefer-kex: 優先される鍵交換アルゴリズムを指定します。アルゴリズム **dh-group-exchange-sha1**、**dh-group1-sha1**、**dh-group14-sha1** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

- **dh-group-exchange-sha1**: 鍵交換アルゴリズム diffie-hellman-group-exchange-sha1 を指定します。
- **dh-group1-sha1**: 鍵交換アルゴリズム diffie-hellman-group1-sha1 を指定します。
- **dh-group14-sha1**: 鍵交換アルゴリズム diffie-hellman-group14-sha1 を指定します。アルゴリズム **dh-group14-sha1** は **dh-group1-sha1** よりセキュリティの強度が強くなり、計算時間が長くなります。

prefer-stoc-cipher: サーバからクライアントへの優先される暗号化アルゴリズムを指定します。サポートされているアルゴリズムは、クライアントからサーバへの暗号化アルゴリズムと同じです（**prefer-ctos-cipher** キーワードを参照）。

prefer-stoc-hmac: サーバからクライアントへの優先される HMAC アルゴリズムを指定します。サポートされているアルゴリズムは、クライアントからサーバへの HMAC アルゴリズムと同じです（**prefer-ctos-hmac** キーワードを参照）。

dscp *dscp-value*: SFTP クライアントによって送信される IPv4 SFTP パケットの DSCP を指定します。設定範囲は 0～63 です。デフォルトは 48 です。DSCP の値はパケットを送信するプライオリティに影響します。

public-key *keyname*: サーバを認証するためにクライアントが使用するサーバのホスト公開鍵を指定します。設定範囲は大文字と小文字を区別しない 1～64 文字です。

source: SFTP パケットの送信元 IP アドレスあるいは送信元インタフェースを指定します。デフォルトで SFTP パケットは送信元アドレスとして、ルーティングエントリで指定された送信インタフェースのプライマリ IP アドレスを使用します。SFTP 接続を正しく行うため、送信元インタフェースとしてループバックインタフェースを指定する、あるいは送信元 IPv4 アドレスとしてループバックインタフェースの IPv4 アドレスを指定します。

- **interface** *interface-type interface-number*: 送信元インタフェースのタイプと番号を指定します。インタフェースのプライマリ IPv4 アドレスは SFTP パケットの送信元 IPv4 アドレスです。
- **ip** *ip-address*: 送信元 IPv4 アドレスを指定します。

説明

sftp コマンドは IPv4 SFTP サーバとの接続を確立し、SFTP client view に移行します。

例

IPv4 SFTP サーバ 10.1.1.2 に SFP クライアントを接続し、サーバの公開鍵として svkey を指定します。SFTP クライアントは公開鍵認証を使用します。以下のアルゴリズムを使用します。

- 優先される鍵交換アルゴリズムは dh-group14-sha1 です。
- サーバからクライアントへの優先される暗号化アルゴリズムは aes128-cbc です。
- クライアントからサーバへの優先される HMAC アルゴリズムは sha1 です。
- サーバからクライアントへの優先される HMAC アルゴリズムは sha1-96 です。
- サーバとクライアント間で優先される圧縮アルゴリズムは zlib です。

<AC> sftp 10.1.1.2 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey

6.2.20 sftp client source

Syntax

sftp client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo sftp client source

デフォルト

出力 SFTP パケットの送信元 IPv4 アドレスは設定されていません。SFTP クライアントは、出力 SFTP パケットの送信元 IPv4 アドレスとして、一致するルートの出力インタフェースのプライマリ IPv4 アドレスを使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 送信元インタフェースをタイプと番号で指定します。SFTP クライアントは、出力 SFTP パケットの送信元アドレスとしてインタフェースのプライマリ IPv4 アドレスを使用します。

ip *ip-address*: 送信元 IPv4 アドレスを指定します。

説明

sftp client source コマンドは SFTP クライアントから送信された SFTP パケットの送信元 IPv4 アドレスを指定します。

undo sftp client source コマンドはデフォルトに戻します。

このコマンドはすべての SFTP 接続に適用します。**sftp** コマンドで指定された送信元 IP アドレスは、現在の SFTP 接続のみ適用します。このコマンドと **sftp** コマンドの両方で送信元 IP アドレスが指定された場合、**sftp** コマンドで指定された送信元 IP アドレスが適用されます。

このコマンドを複数実行した場合、最後に行われた設定が適用されます。

例

SFTP パケットの送信元 IP アドレスとして 192.168.0.1 を指定します。

<AC> system-view

[AC] sftp client source ip 192.168.0.1

関連コマンド

display sftp client source

6.2.21 ssh client source

Syntax

ssh client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo ssh client source

デフォルト

出力 SSH パケットの送信元 IPv4 アドレスは設定されていません。Stelnet クライアントは、出力 SSH パケットの送信元 IPv4 アドレスとして、一致するルートの出力インタフェースのプライマリ IPv4 アドレスを使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 送信元インタフェースをタイプと番号で指定します。Stelnet クライアントは、出力 SSH パケットの送信元アドレスとしてインタフェースのプライマリ IPv4 アドレスを使用します。

ip *ip-address*: 送信元 IPv4 アドレスを指定します。

説明

ssh client source コマンドは Stelnet クライアントが送信する SSH パケットの送信元 IPv4 アドレスを指定します。

undo ssh client source コマンドはデフォルトに戻します。

このコマンドはすべての Stelnet 接続に適用します。**ssh2** コマンドで指定された送信元 IP アドレスは、現在の Stelnet 接続のみ適用します。このコマンドと **ssh2** コマンドの両方で送信元 IP アドレスが指定された場合、**ssh2** コマンドで指定された送信元 IP アドレスが適用されます。

このコマンドを複数実行した場合、最後に行われた設定が適用されます。

例

SSH パケットの送信元 IPv4 アドレスとして 192.168.0.1 を指定します。

<AC> system-view

[AC] ssh client source ip 192.168.0.1

関連コマンド

display ssh client source

6.2.22 ssh2

Syntax

ssh2 *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **escape** *character* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

View

User view

定義済みユーザロール

network-admin

パラメータ

server: IPv4 アドレスあるいはホスト名でサーバを指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。

port-number: サーバのポート番号を指定します。設定範囲は 1～65535 です。デフォルトは 22 です。

identity-key: クライアントの公開鍵アルゴリズムを指定します。サーバが公開鍵認証を使用する場合、指定する必要があります。クライアントはアルゴリズムに関連したローカル秘密鍵を使用してデジタル署名を作成します。

- **dsa**: 公開鍵アルゴリズム dsa を指定します。
- **rsa**: 公開鍵アルゴリズム rsa を指定します。

prefer-compress: サーバとクライアント間で優先される圧縮アルゴリズムを指定します。

zlib: 圧縮アルゴリズム zlib を指定します。

prefer-ctos-cipher: クライアントからサーバへの優先される暗号化アルゴリズムを指定します。アルゴリズム **des-cbc**、**3des-cbc**、**aes128-cbc** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

- **des-cbc**: 暗号化アルゴリズム des-cbc を指定します。
- **3des-cbc**: 暗号化アルゴリズム 3des-cbc を指定します。
- **aes128-cbc**: 暗号化アルゴリズム aes128-cbc を指定します。

prefer-ctos-hmac: クライアントからサーバへの優先される HMAC アルゴリズムを指定します。

- **md5:** HMAC アルゴリズム hmac-md5 を指定します。
- **md5-96:** HMAC アルゴリズム hmac-md5-96 を指定します。
- **sha1:** HMAC アルゴリズム hmac-sha1 を指定します。アルゴリズム sha1 は md5 よりもセキュリティの強度が強くなるが、計算時間が長くなります。
- **sha1-96:** HMAC アルゴリズム hmac-sha1-96 を指定します。

prefer-kex: 優先される鍵交換アルゴリズムを指定します。

- **dh-group-exchange-sha1**: 鍵交換アルゴリズム diffie-hellman-group-exchange-sha1 を指定します。
- **dh-group1-sha1**: 鍵交換アルゴリズム diffie-hellman-group1-sha1 を指定します。
- **dh-group14-sha1**: 鍵交換アルゴリズム diffie-hellman-group14-sha1 を指定します。アルゴリズム **dh-group14-sha1** は **dh-group1-sha1** よりセキュリティの強度が強くなり、計算時間が長くなります。

prefer-stoc-cipher: サーバからクライアントへの優先される暗号化アルゴリズムを指定します。サポートされているアルゴリズムは、クライアントからサーバへの暗号化アルゴリズムと同じです（**prefer-ctos-cipher** キーワードを参照）。

prefer-stoc-hmac: サーバからクライアントへの優先される HMAC アルゴリズムを指定します。サポートされているアルゴリズムは、クライアントからサーバへの HMAC アルゴリズムと同じです（**prefer-ctos-hmac** キーワードを参照）。

dscp *dscp-value*: IPv4 SSH パケットの DSCP を指定します。設定範囲は 0～63 です。デフォルトは 48 です。DSCP の値はパケットを送信するプライオリティに影響します。

escape *character*: Stelnet 接続を切断するための文字を指定します。デフォルトはチルダ（~）です。

public-key *keyname*: サーバのホスト公開鍵を指定します。サーバを認証するために使用します。設定範囲は 1～64 です。大文字、小文字を区別しません。

source: SSH パケットの送信元 IP アドレスあるいは送信元インタフェースを指定します。デフォルトで SSH パケットは送信元アドレスとして、ルーティングエントリで指定された送信インタフェースのプライマリ IP アドレスを使用します。Stelnet 接続を正しく行うため、送信元インタフェースとしてループバックインタフェースを指定する、あるいは送信元 IPv4 アドレスとしてループバックインタフェースの IPv4 アドレスを指定します。

- **interface** *interface-type interface-number*: 送信元インタフェースのタイプと番号を指定します。インタフェースのプライマリ IPv4 アドレスは SSH パケットの送信元 IP アドレスです。
- **ip** *ip-address*: 送信元 IPv4 アドレスを指定します。

説明

ssh2 コマンドは IPv4 Stelnet サーバとの接続を確立します。

escape *character* パラメータとドット（.）の組み合わせは、エスケープシーケンスとして働きます。このエスケープシーケンスは、一般に、サーバが再起動や例外的な挙動をするときに SSH 接続を素早く切断します。

エスケープシーケンスを適用するには、ラインのその最初に入力しなければなりません。ラインに他の文字を入力したり、操作を実行した場合、次のラインにエスケープシーケンスを入力してください。

escape *character* パラメータにはデフォルトの（~）を使用することを推奨します。SSH ユーザ名として別の文字を使用しないでください。

例

IPv4 Stelnet サーバ 3.3.3.3 へ接続を確立し、サーバの公開鍵として svkey を指定します。Stelnet クライアントは公開鍵認証を使用します。**escape** *character* として（$）を指定します。以下のアルゴリズムを使用します。

- 優先される鍵交換アルゴリズムは dh-group14-sha1 です。
- サーバからクライアントへの優先される暗号化アルゴリズムは aes128-cbc です。
- クライアントからサーバへの優先される HMAC アルゴリズムは sha1 です。
- サーバからクライアントへの優先される HMAC アルゴリズムは sha1-96 です。
- サーバとクライアント間で優先される圧縮アルゴリズムは zlib です。

<AC> ssh2 3.3.3.3 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey escape $

目次

このセクションのページは **9-x-x** です。

7 章 PKI 7-1
7.1 PKI 設定コマンド 7-1
7.1.1 attribute 7-1
7.1.2 ca identifier 7-2
7.1.3 certificate request entity 7-3
7.1.4 certificate request from 7-4
7.1.5 certificate request mode 7-4
7.1.6 certificate request polling 7-6
7.1.7 certificate request url 7-7
7.1.8 common-name 7-7
7.1.9 country 7-8
7.1.10 crl check enable 7-9
7.1.11 crl url 7-10
7.1.12 display pki certificate access-control-policy 7-11
7.1.13 display pki certificate attribute-group 7-12
7.1.14 display pki certificate domain 7-13
7.1.15 display pki certificate request-status 7-17
7.1.16 display pki crl domain 7-18
7.1.17 fqdn 7-20
7.1.18 ip 7-21
7.1.19 locality 7-22
7.1.20 organization 7-22
7.1.21 organization-unit 7-23
7.1.22 pki abort-certificate-request 7-24
7.1.23 pki certificate access-control-policy 7-25
7.1.24 pki certificate attribute-group 7-26
7.1.25 pki delete-certificate 7-26
7.1.26 pki domain 7-28
7.1.27 pki entity 7-29
7.1.28 pki import 7-29
7.1.29 pki request-certificate 7-32
7.1.30 pki retrieve-certificate 7-33
7.1.31 pki retrieve-crl domain 7-35
7.1.32 pki storage 7-36
7.1.33 pki validate-certificate 7-37
7.1.34 public-key dsa 7-38

7.1.35 public-key ecdsa 7-39
7.1.36 public-key rsa 7-41
7.1.37 root-certificate fingerprint 7-42
7.1.38 state 7-44

7章 PKI

7.1 PKI設定コマンド

7.1.1 attribute

Syntax

attribute *id* { **alt-subject-name** { **fqdn** | **ip** } | { **issuer-name** | **subject-name** } { **dn** | **fqdn** | **ip** } } { **ctn** | **equ** | **nctn** | **nequ** } *attribute-value*

undo attribute *id*

デフォルト

設定なし

View

Certificate attribute group view

定義済みユーザロール

network-admin

パラメータ

id: 1～16 でルール ID を指定します。

alt-subject-name: alternative subject name field(代名のフィールド)を指定します。

fqdn: FQDN 属性を指定します。

ip: IP アドレス属性を指定します。

dn: DN 属性を指定します。

issuer-name: issuer name field(発行人名フィールド)を指定します。

subject-name: subject name field を指定します。

ctn: contain operation を指定します。

equ: equal operation を指定します。

nctn: not-contain operation を指定します。

nequ: not-equal operation を指定します。

attribute-value: 属性値(1～128 文字)を設定します。

説明

attribute コマンドは、certificate issuer name、subject name、alternative subject name の各フィールドの attribute に基づいて証明書をフィルタリングするルールを設定します。

undo attribute コマンドはデフォルトに戻します。

例

#証明書属性グループを作成し、その view に入ります。

<AP> system-view

[AP] pki certificate attribute-group mygroup

#対象 DN で、”abc”含んでいる証明書とマッチする、属性ルールを設定します。

[AP-pki-cert-attribute-group-mygroup] attribute 1 subject-name dn ctn abc

issuer name field に FQDN "abc"を含んでいない証明書とマッチする属性ルールを設定します。

[AP-pki-cert-attribute-group-mygroup] attribute 2 issuer-name fqdn nequ abc

alternative subject name field に IP アドレス"10.0.0.1"を含んでいない証明書とマッチする属性ルールを設定します。

[AP-pki-cert-attribute-group-mygroup] attribute 3 alt-subject-name ip nequ 10.0.0.1

7.1.2 ca identifier

Syntax

ca identifier *name*

undo ca identifier

デフォルト

trusted-CA は PKI ドメインに指定されていません。

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

name： trusted-CA の識別子を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

説明

ca identifier コマンドは、信頼できる CA の識別子を設定します。

undo ca identifier コマンドは、デフォルトに戻します。

証明書要求、取得、取り消しおよびクエリのすべては trusted-CA に依存しています。

例

#信頼できる CA として **new-ca** を指定します。

<AP> system-view

[AP] pki domain 1

[AP-pki-domain-1] ca identifier new-ca

7.1.3 certificate request entity

Syntax

certificate request entity *entity-name*

undo certificate request entity

デフォルト

すべてのエンティティは証明書要求に指定されていません。

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

entity-name：証明書要求のエンティティの名前を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別しません。

説明

certificate request entity コマンドは、証明書要求のエンティティを指定します。

undo certificate request entity コマンドは、デフォルトに戻します。

例

証明書要求のエンティティを entity1 として指定します。

<AP> system-view

[AP] pki domain 1

[AP-pki-domain-1] certificate request entity entity1

関連コマンド

pki entity

7.1.4 certificate request from

Syntax

certificate request from { **ca** | **ra** }

undo certificate request from

デフォルト

証明書要求に指定された権限はありません。

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

ca： エンティティが CA に証明書を要求することを指定します。

ra： エンティティが RA に証明書を要求することを指定します。

説明

certificate request from コマンドは、証明書要求の権限を指定します。

undo certificate request from コマンドはデフォルトに戻します。

例

エンティティが CA に証明書を要求することを指定します。

<AP> system-view

[AP] pki domain 1

[AP-pki-domain-1] certificate request from ca

7.1.5 certificate request mode

Syntax

certificate request mode { **auto** [**password** { **cipher** | **simple** } *string*] | **manual** }

undo certificate request mode

デフォルト

マニュアル要求モード

Views

PKI domain view

定義済みユーザロール

network-admin

パラメータ

auto: オート証明書要求モードを指定します。

password: 証明書取消し用のパスワードを指定します。

cipher: 暗号化された形でパスワードを指定します。

simple: 平文形でパスワードを指定します。セキュリティ向上のために、平文で指定したパスワードは暗号化されます。

string: パスワードを指定します。平文指定では 1～31 文字、暗号化指定では 1～73 文字で設定します。大文字小文字を区別します

manual: マニュアルの証明書要求モードを指定します。

説明

certificate request mode コマンドは、証明書要求モードを設定します。

undo certificate request mode コマンドはデフォルトに戻します。

証明書要求はオフラインまたはオンラインのモードの中の CA に提出することができます。オンラインモードでは、証明書要求を自動もしくは手動で提出が可能です。

- **オート要求モード**–PKI エンティティは自動的に CA 証明書を取得して、以下の条件の両方が存在しているときに、証明書要求を CA に提出します:
  - 関連したアプリケーション(例：IKE)は identity 認証を実行します。
  - どの証明書も機器のアプリケーションで利用可能ではありません。

  オート要求モードで、CA ポリシによって必要とされている、証明書取消し用のパスワードを指定してください。
- **マニュアル要求モード**–手動で CA 証明書を得て、証明書要求を提出しなければなりません。

例

証明書要求モードを”auto"に設定します。

<AP> system-view

[AP] pki domain aaa

[AP-pki-domain-aaa] certificate request mode auto

証明書要求モードをオートにして、証明書取消しパスワードを"123456"に設定します。

<AP> system-view

[AP] pki domain aaa

[AP-pki-domain-aaa] certificate request mode auto password simple 123456

7.1.6 certificate request polling

Syntax

certificate request polling { **count** *count* | **interval** *interval* }

undo certificate request polling { **count** | **interval** }

デフォルト

ポーリング間隔：20 分、証明書要求ステータス最大リトライ数：50

Views

PKI domain view

定義済みユーザロール

network-admin

パラメータ

count *count*: 証明書要求ステータス最大リトライ数を 1～100 の範囲で指定します。

interval *interval*: ポーリング間隔(分)を 5～168 範囲で指定します。

説明

certificate request polling コマンドは、ポーリング間隔と証明書要求ステータスの最大リトライ数を設定します。

undo certificate request polling コマンドはデフォルトに戻します。

PKI エンティティが証明書要求を提出した後に、CA 管理者が手動で証明書要求を承認しなければならない場合、CA サーバが証明書を出すのに、しばらく時間がかかる可能性があります。この期間の間、PKI エンティティは周期的に CA サーバに要求をします。PKI エンティティが証明書を得るか、証明書要求ステータスの最大リトライ数に達すると、周期的な要求が止まります。証明書要求ステータスの最大リトライ数に達しても承認されなければ、証明書要求は失敗します。

CA サーバが自動的に証明書要求を承認できるならば、証明書要求を提出したすぐ後に、PKI エンティティは証明書を得ることができます。

例

ポーリングインターバルを 15 分、証明書要求ステータス最大リトライ数を 40 回に設定します。

<AP> system-view

[AP] pki domain aaa

[AP-pki-domain-aaa] certificate request polling interval 15

[AP-pki-domain-aaa] certificate request polling count 40

7.1.7 certificate request url

Syntax

certificate request url *url-string*

undo certificate request url

デフォルト

PKI ドメインに指定された URL はありません。

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

url-string: 証明書を要求するサーバの URL を指定します。設定範囲は 1～511 文字です。大文字、小文字を区別します。証明書を要求するサーバの URL のフォーマットは、サーバの位置情報と CGI コマンドインタフェーススクリプトの位置情報から構成される http://*server_location*/*ca_script_location* です。

説明

certificate request url コマンドは、SCEP を用いて証明書を要求するサーバの URL を指定します。

undo certificate request url コマンドはデフォルトに戻します。

例

証明書要求サーバの URL を指定します。

<AP> system-view

[AP] pki domain 1

[AP-pki-domain-1] certificate request url http://169.254.0.100/certsrv/mscep/mscep.dll

7.1.8 common-name

Syntax

common-name *name*

undo common-name

デフォルト

指定された共通名はありません。

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

name : エンティティの共通名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。コンマは含まれません。

説明

common-name コマンドは、エンティティの共通名を設定します。たとえば、ユーザ名です。

undo common-name コマンドは、デフォルトに戻します。

例

#エンティティの共通名として、**test** を設定します。

<AP> system-view

[AP] pki entity 1

[AP-pki-entity-1] common-name test

7.1.9 country

Syntax

country *country-code-str*

undo country

デフォルト

国コードは指定されていません。

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

country-code-str: エンティティの国コードを指定します。2 文字で指定します。大文字、小文字を区別します。

説明

country コマンドは、エンティティの属する国コードを指定します。国コードはスタンダードな 2 文字のコードです。たとえば日本の場合は JP です。

undo country コマンドはデフォルトに戻します。

例

エンティティの国コードを JP に設定します。

<AP> system-view

[AP] pki entity 1

[AP-pki-entity-1] country JP

7.1.10 crl check enable

Syntax

crl check enable

undo crl check enable

デフォルト

CRL チェックは有効です。

View

PKI domain view

定義済みユーザロール

network-admin

説明

crl check enable コマンドは、CRL チェックを有効にします。

undo crl check enable コマンドは、CRL チェックを無効にします。

CRL は取り消したすべての証明書を公開するために CA によって発行されたファイルです。

証明書の取り消しは証明書失効以前に起こります。CRL チェックは証明書が取り消されたかどうかをチェックすることを目的としています。

例

CRL チェックを無効にします。

<AP> system-view

[AP] pki domain 1

[AP-pki-domain-1] undo crl check enable

7.1.11 crl url

Syntax

crl url *url-string*

undo crl url

デフォルト

CRL 配布ポイントの URL は指定されていません。

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

url-string：CRL 配布ポイントの URL を指定します。ldap://*server_location* または http://*server_location* のフォーマットで指定します。設定範囲は 1～511 文字です。大文字、小文字を区別します。*server_location* は IP アドレスまたはドメイン名を指定できます。URL の長さは、CLI 文字列制限または url-string パラメータのいずれか小さい方によって制限されます。

説明

crl url コマンドは、CRL 配布ポイントの URL を指定します。

undo crl url コマンドはデフォルトに戻します。

CRL 配布ポイントの URL が設定されていないときは、CA 証明書とローカル証明書を取得し、SCEP により CRL を取得してください。

例

CRL 配布ポイントの URL を指定します。

<AP> system-view

[AP] pki domain 1

[AP-pki-domain-1] crl url ldap://169.254.0.30

7.1.12 display pki certificate access-control-policy

Syntax

display pki certificate access-control-policy [*policy-name*]

Views

Any view

定義済みユーザロール

network-admin

network-operator

パラメータ

policy-name: ポリシ名を 1～31 文字で指定します。大文字、小文字は区別しません。このパラメータを省略した場合、すべての証明書ベースのアクセス制御ポリシの情報を表示します。

説明

display pki certificate access-control-policy コマンドは、証明書ベースのアクセス制御ポリシ情報を表示します。

例

ポリシ名 mypolicy の証明書ベース アクセス制御ポリシ情報を表示します。

<AP> display pki certificate access-control-policy mypolicy

```
Access control policy name: mypolicy
   Rule 1  deny    mygroup1
   Rule 2  permit  mygroup2
```

すべての証明書ベース アクセス制御ポリシ情報を表示します。

<AP> display pki certificate access-control-policy

```
Total PKI certificate access control policies: 2
Access control policy name: mypolicy1
   Rule 1  deny    mygroup1
   Rule 2  permit  mygroup2
Access control policy name: mypolicy2
   Rule 1  deny    mygroup3
   Rule 2  permit  mygroup4
```

表 7-1 コマンド出力

フィールド	説明
Total PKI certificate access control policies	証明書ベースのアクセス制御ポリシの総数。
permit	許可しているアクセス制御ルール
deny	制限されているアクセス制御ルール

7.1.13 display pki certificate attribute-group

Syntax

display pki certificate attribute-group [*group-name*]

Views

Any view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-name:証明書属性グループ名を 1～31 文字で指定します。大文字と小文字は区別しません。このパラメータを省略した場合、すべての証明書属性グループについての情報を表示します。

説明

display pki certificate attribute-group コマンドは、証明書属性グループの情報を表示します。

例

証明書属性グループ”mygroup”についての情報を表示します。

<AP> display pki certificate attribute-group mygroup

```
Attribute group name: mygroup
    Attribute  1 subject-name    dn   ctn   abc
    Attribute  2 issuer-name     fqdn  nctn  app
```

すべての証明書属性グループ情報を表示します。

<AP> display pki certificate attribute-group

```
Total PKI certificate attribute groups: 2.
Attribute group name: mygroup1
```

```
     Attribute  1 subject-name    dn   ctn   abc
     Attribute  2 issuer-name     fqdn  nctn  app
Attribute group name: mygroup2
     Attribute  1 subject-name    dn   ctn   def
     Attribute  2 issuer-name     fqdn  nctn  fqd
```

表 7-2 **display pki certificate attribute-group** の出力情報

フィールド	説明
Total PKI certificate attribute groups	証明書属性グループ数
ctn	Contain operation.
nctn	Not-contain operation.
equ	Equal operation.
nequ	Not-equal operation.
Attribute 1 subject-name dn ctn abc	属性ルール: ● **alt-subject-name**–Alternative subject name. ● **issuer-name**–Certificate issuer name. ● **subject-name**–Certificate subject name. ● **fqdn**–PKI entity の FQDN. ● **ip**–PKI entity の IP アドレス ● **dn**–PKI entity の DN ● **ctn**–contain operation を示します。 ● **equ**–equal operation を示します。 ● **nctn**–not-contain operation を示します。 ● **nequ**–not-equal operation を示します。

7.1.14 display pki certificate domain

Syntax

display pki certificate domain *domain-name* { **ca** | **local** }

View

すべての view

定義済みユーザロール

network-admin

パラメータ

domain-name： PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字は区別しません。ドメイン名は表 7-3 に示す指定記号を設定することができません。

表 7-3 指定記号

名前	記号	名前	記号
チルダ	~	ドット	.
アスタリスク	*	左アングルブラケット	<
バックスラッシュ	¥	右アングルブラケット	>
垂直バー	|	ダブルクォーテーション	"
コロン	:	アポストロフィー	'

ca： CA 証明書を表示します。

local： ローカル証明書を表示します。

説明

display pki certificate コマンドは、証明書の内容を表示します。

ca パラメータを指定した場合、ドメインのすべての証明書の内容を表示します。

local パラメータを指定した場合、ドメインのすべてのローカル証明書の内容を表示します。

例

PKI ドメイン aaa の CA 証明書を表示します。

<AP> display pki certificate local domain aaa ca

```
Certificate:
   Data:
      Version: 1 (0x0)
      Serial Number:
         5c:72:dc:c4:a5:43:cd:f9:32:b9:c1:90:8f:dd:50:f6
      Signature Algorithm: sha1WithRSAEncryption
      Issuer: C=cn, O=docm, OU=rnd, CN=rootca
      Validity
         Not Before: Jan  6 02:51:41 2011 GMT
         Not After : Dec  7 03:12:05 2013 GMT
      Subject: C=cn, O=ccc, OU=ppp, CN=rootca
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
            Public-Key: (1024 bit)
            Modulus:
               00:c4:fd:97:2c:51:36:df:4c:ea:e8:c8:70:66:f0:
               28:98:ec:5a:ee:d7:35:af:86:c4:49:76:6e:dd:40:
               4a:9e:8d:c0:cb:d9:10:9b:61:eb:0c:e0:22:ce:f6:
               57:7c:bb:bb:1b:1d:b6:81:ad:90:77:3d:25:21:e6:
               7e:11:0a:d8:1d:3c:8e:a4:17:1e:8c:38:da:97:f6:
```

```
                6d:be:09:e3:5f:21:c5:a0:6f:27:4b:e3:fb:9f:cd:
                c1:91:18:ff:16:ee:d8:cf:8c:e3:4c:a3:1b:08:5d:
                84:7e:11:32:5f:1a:f8:35:25:c0:7e:10:bd:aa:0f:
                52:db:7b:cd:5d:2b:66:5a:fb
            Exponent: 65537 (0x10001)
    Signature Algorithm: sha1WithRSAEncryption
        6d:b1:4e:d7:ef:bb:1d:67:53:67:d0:8f:7c:96:1d:2a:03:98:
        3b:48:41:08:a4:8f:a9:c1:98:e3:ac:7d:05:54:7c:34:d5:ee:
        09:5a:11:e3:c8:7a:ab:3b:27:d7:62:a7:bb:bc:7e:12:5e:9e:
        4c:1c:4a:9f:d7:89:ca:20:46:de:c5:b3:ce:36:ca:5e:6e:dc:
        e7:c6:fe:3f:c5:38:dd:d5:a3:36:ad:f4:3d:e6:32:7f:48:df:
        07:f0:a2:32:89:86:72:22:cd:ed:e5:0f:95:df:9c:75:71:e7:
        fe:34:c5:a0:64:1c:f0:5c:e4:8f:d3:00:bd:fa:90:b6:64:d8:
        88:a6
```

PKI ドメイン aaa のローカル証明書を表示します。

<AP> display pki certificate domain aaa local

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            bc:05:70:1f:0e:da:0d:10:16:1e
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CN, O=sec, OU=software, CN=abdfdc
        Validity
            Not Before: Jan  7 20:05:44 2011 GMT
            Not After : Jan  7 20:05:44 2012 GMT
        Subject: O=OpenCA Labs, OU=Users, CN=fips fips-sec
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b2:38:ad:8c:7d:78:38:37:88:ce:cc:97:17:39:
                    52:e1:99:b3:de:73:8b:ad:a8:04:f9:a1:f9:0d:67:
                    d8:95:e2:26:a4:0b:c2:8c:63:32:5d:38:3e:fd:b7:
                    4a:83:69:0e:3e:24:e4:ab:91:6c:56:51:88:93:9e:
                    12:a4:30:ad:ae:72:57:a7:ba:fb:bc:ac:20:8a:21:
                    46:ea:e8:93:55:f3:41:49:e9:9d:cc:ec:76:13:fd:
                    a5:8d:cb:5b:45:08:b7:d1:c5:b5:58:89:47:ce:12:
                    bd:5c:ce:b6:17:2f:e0:fc:c0:3e:b7:c4:99:31:5b:
                    8a:f0:ea:02:fd:2d:44:7a:67
                Exponent: 65537 (0x10001)
        X509v3 extensions:
```

```
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Client, S/MIME
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection, Microsoft
Smartcardlogin
            Netscape Comment:
                User Certificate of OpenCA Labs
            X509v3 Subject Key Identifier:
                91:95:51:DD:BF:4F:55:FA:E4:C4:D0:10:C2:A1:C2:99:AF:A5:CB:30
            X509v3 Authority Key Identifier:

keyid:DF:D2:C9:1A:06:1F:BC:61:54:39:FE:12:C4:22:64:EB:57:3B:11:9F

            X509v3 Subject Alternative Name:
                email:fips@ccc.com
            X509v3 Issuer Alternative Name:
                email:pki@openca.org
            Authority Information Access:
                CA Issuers - URI:http://titan/pki/pub/cacert/cacert.crt
                OCSP - URI:http://titan:2560/
                1.3.6.1.5.5.7.48.12 - URI:http://titan:830/

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://titan/pki/pub/crl/cacrl.crl

    Signature Algorithm: sha256WithRSAEncryption
        94:ef:56:70:48:66:be:8f:9d:bb:77:0f:c9:f4:65:77:e3:bd:
        ea:9a:b8:24:ae:a1:38:2d:f4:ab:e8:0e:93:c2:30:33:c8:ef:
        f5:e9:eb:9d:37:04:6f:99:bd:b2:c0:e9:eb:b1:19:7e:e3:cb:
        95:cd:6c:b8:47:e2:cf:18:8d:99:f4:11:74:b1:1b:86:92:98:
        af:a2:34:f7:1b:15:ee:ea:91:ed:51:17:d0:76:ec:22:4c:56:
        da:d6:d1:3c:f2:43:31:4f:1d:20:c8:c2:c3:4d:e5:92:29:ee:
        43:c6:d7:72:92:e8:13:87:38:9a:9c:cd:54:38:b2:ad:ba:aa:
        f9:a4:68:b5:2a:df:9a:31:2f:42:80:0c:0c:d9:6d:b3:ab:0f:
        dd:a0:2c:c0:aa:16:81:aa:d9:33:ca:01:75:94:92:44:05:1a:
        65:41:fa:1e:41:b5:8a:cc:2b:09:6e:67:70:c4:ed:b4:bc:28:
        04:50:a6:33:65:6d:49:3c:fc:a8:93:88:53:94:4c:af:23:64:
```

```
cb:af:e3:02:d1:b6:59:5f:95:52:6d:00:00:a0:cb:75:cf:b4:
50:c5:50:00:65:f4:7d:69:cc:2d:68:a4:13:5c:ef:75:aa:8f:
3f:ca:fa:eb:4d:d5:5d:27:db:46:c7:f4:7d:3a:b2:fb:a7:c9:
de:18:9d:c1
```

関連コマンド

- **pki retrieval-certificate**
- **pki domain**

7.1.15 display pki certificate request-status

Syntax

display pki certificate request-status [domain *domain-name***]**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

domain-name： PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字は区別しません。ドメイン名は表 7-4 に示す指定記号を設定することができません。

表 7-4 指定記号

名前	記号	名前	記号
チルダ	~	ドット	.
アスタリスク	*	左アングルブラケット	<
バックスラッシュ	¥	右アングルブラケット	>
垂直バー	|	ダブルクォーテーション	"
コロン	:	アポストロフィー	'

説明

display pki certificate コマンドは、証明書要求ステータスを表示します。

例

すべての PKI ドメインの証明書要求ステータスを表示します。

<AP> display pki certificate request-status

```
Certificate Request Transaction 1
    Domain name: domain1
    Status: Pending
    Key usage: General
    Remain polling attempts: 10
    Next polling attempt after : 1191 seconds
Certificate Request Transaction 2
    Domain name: domain2
    Status: Pending
    Key usage: Signature
    Remain polling attempts: 10
    Next polling attempt after : 188 seconds
```

表 7-5 コマンド出力

フィールド	説明
Certificate Request Transaction number	証明書要求の処理番号です。1から開始します。
Status	証明書要求の状態です。接続状態のみが含まれます。
Key usage	証明書の目的です。 • **General**–署名と暗号化です。 • **Signature**–署名のみです。 • **Encryption**–暗号のみです。
Remain polling attempts	証明書要求の状態を要求できる残り回数です。
Next polling attempt after	次の要求状態の確認を行う前の残り時間です。

関連コマンド

- **pki retrieval-certificate**
- **pki domain**
- **certificate request polling**

7.1.16 display pki crl domain

Syntax

display pki crl domain *domain-name*

View

すべての view

定義済みユーザロール

network-admin

パラメータ

domain-name： PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字は区別しません。

説明

display pki crl domain コマンドは、PKI ドメインのローカルに保存された CRL に関する情報を表示します。

例

ローカルに保存された PKI ドメイン 1 の CRL に関する情報を表示します。

<AP> display pki crl domain 1

```
Certificate Revocation List (CRL):
      Version 2 (0x1)
      Signature Algorithm: sha1WithRSAEncryption
      Issuer:
         C=JP
         O=abc
         OU=soft
         CN=A Test Root
      Last Update: Jan  5 08:44:19 2004 GMT
      Next Update: Jan  5 21:42:13 2004 GMT
      CRL extensions:
         X509v3 Authority Key Identifier:
         keyid:0F71448E E075CAB8 ADDB3A12 0B747387 45D612EC
         Revoked Certificates:
         Serial Number: 05a234448E…
         Revocation Date: Sep 6 12:33:22 2004 GMT
         CRL entry extensions:…
         Serial Number: 05a278445E…
         Revocation Date: Sep 7 12:33:22 2004 GMT
         CRL entry extensions:…
```

表 7-6 コマンド出力

フィールド	説明
Version	CRLのバージョンです。
Signature Algorithm	CRLで使用される署名アルゴリズムです。
Issuer	CRLを発行するCAです。
Last Update	最新のアップデート時間です。
Next Update	次のアップデート時間です。
CRL extensions	CRLの拡張です。

フィールド	説明
X509v3 Authority Key Identifier	CRLを発行するCAです。証明書バージョンは X.509 v3です。
keyid	公開鍵IDです。CAは複数の鍵ペアを持っている可能性があります。このフィールドはCRLの署名で使用される鍵ペアを示します。
Revoked Certificates	取り消された証明書です。
Serial Number	取り消された証明書のシリアル番号です。
Revocation Date	証明書を取り消した日時です。

関連コマンド

- **pki retrieval-crl**
- **pki domain**

7.1.17 fqdn

Syntax

fqdn *name-str*

undo fqdn

デフォルト

FQDN はエンティティに指定されていません。

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

name-str: エンティティのドメイン名をすべて省略しない記述形式(FQDN、Fully qualified domain name)を指定します。設定範囲は 1～255 文字です。大文字、小文字を区別します。

説明

fqdn コマンドは、エンティティの FQDN を設定します。

undo fqdn コマンドはデフォルトに戻します。

FQDN はネットワーク上のエンティティの固有な識別子です。その固有な識別子はホスト名とドメイン名から構成されており、IP アドレスを解決できます。

例

PKI エンティティ 1 の FQDN を pki.domain-name.com に設定します。

<P> system-view

[AP] pki entity 1

[AP-pki-entity-1] fqdn pki.domain-name.com

7.1.18 ip

Syntax

ip *ip-address* { *ip-address* | **interface** *interface-type interface-number* }

undo ip

デフォルト

IP アドレスはエンティティに指定されていません。

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

ip-address： エンティティの IP アドレスを指定します。

interface *interface-type interface-number*:インタフェースのタイプと番号を指定します。インタフェースのプライマリ IPv4 アドレスは PKI エンティティの IP アドレスとして使われます。

説明

ip コマンドは、エンティティの IP アドレスを設定します。

undo ip コマンドはデフォルトに戻します。

例

PKI エンティティ 1 の IP アドレスを 11.0.0.1.として設定します。

<AP> system-view

[AP] pki entity 1

[AP-pki-entity-1] ip 11.0.0.1

7.1.19 locality

Syntax

locality *locality-name*

undo locality

デフォルト

所在地はエンティティに指定されていません。

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

locality-name： 所在地を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。コンマは含まれません。

説明

locality コマンドは、エンティティの所在地を設定します。たとえば都市名などです。

undo locality コマンドはデフォルトに戻します。

例

PKI エンティティ 1 の所在地を city として設定します。

<AP> system-view

[AP] pki entity 1

[AP-pki-entity-1] locality city

7.1.20 organization

Syntax

organization *org-name*

undo organization

デフォルト

組織名はエンティティに指定されていません。

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

org-name：組織名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。その文字列にコンマは含まれません。

説明

organization コマンドは、エンティティが属する組織の名前を設定します。

undo organization コマンドはデフォルトに戻します。

例

PKI エンティティ 1 が属する組織の名前を test-lab として設定します。

<AP> system-view

[AP] pki entity 1

[AP-pki-entity-1] organization test-lab

7.1.21 organization-unit

Syntax

organization-unit *org-unit-name*

undo organization-unit

デフォルト

組織単位名はエンティティに指定されていません。

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

org-unit-name： 組織ユニット名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。その文字列にコンマは含まれません。

説明

organization-unit コマンドは、エンティティが属する組織ユニット名を指定します。

undo organization-unit コマンドはデフォルトに戻します。

例

PKI エンティティ 1 が属する組織ユニット名を group1 に設定します。

<AP> system-view

[AP] pki entity 1

[AP-pki-entity-1] organization-unit group1

7.1.22 pki abort-certificate-request

Syntax

pki abort-certificate-request domain *domain-name*

Views

System view

定義済みユーザロール

network-admin

パラメータ

domain-name: PKI ドメイン名を 1～31 文字で指定します。表 7-7 に記載している指定記号は使用できません.

表 7-7 指定記号

名前	記号	名前	記号
チルダ	~	ドット	.
アスタリスク	*	左アングルブラケット	<
バックスラッシュ	¥	右アングルブラケット	>
垂直バー	|	ダブルクォーテーション	"
コロン	:	アポストロフィー	'

説明

pki abort-certificate-request コマンドは、PKI ドメインの証明書要求を中止します。

証明書要求を中止し、証明書要求の名前、国コード、または FQDN などのいくつかのパラメータを変更することができます。証明書要求ステータスを表示するには、**display pki certificate request-status** コマンドを使ってください。

例

PKI ドメイン 1 の証明書要求を中止します。

<AP> system-view

[AP] pki abort-certificate-request domain 1

```
The certificate request is in process.
Confirm to abort it? [Y/N]:y
```

7.1.23 pki certificate access-control-policy

Syntax

pki certificate access-control-policy *policy-name*

undo pki certificate access-control-policy *policy-name*

デフォルト

設定なし

Views

System view

定義済みユーザロール

network-admin

パラメータ

policy-name: ポリシ名を 1～31 文字で指定します。大文字、小文字は区別しません。

説明

pki certificate access-control-policy コマンド は、証明書ベースのアクセス制御ポリシを作成し、その View に移行するか、既存の証明書ベースのアクセス制御ポリシ view に移行します。

undo pki certificate access-control-policy コマンドは、証明書ベースのアクセス制御ポリシを削除します。

証明書ベースのアクセス制御ポリシは、属性に基づいて許可もしくは、否定するアクセス制御ポリシを含んでいます。

例

”mypolicy”という名の証明書ベースのアクセス制御ポリシを作成し、その view に入ります。

<AP> system-view

[AP] pki certificate access-control-policy mypolicy

[AP-pki-cert-acp-mypolicy]

7.1.24 pki certificate attribute-group

Syntax

pki certificate attribute-group *group-name*

undo pki certificate attribute-group *group-name*

デフォルト

設定なし

Views

System view

定義済みユーザロール

network-admin

パラメータ

group-name: グループ名を 1～31 文字で指定します。大文字、小文字は区別しません。

説明

pki certificate attribute-group コマンドは、証明書属性グループを作成し、その View に移行するか、既存の証明書属性グループの View に移行します。

undo pki certificate attribute-group コマンドは、証明書属性グループを削除します。

証明書属性グループは、**attribute** コマンドを使って設定された属性規則のセットです。各属性規則は発行人名、証明書の対象の名前、または代わりの対象の名前のフィールドにおいて属性を定義します。

証明書属性グループはアクセスコントロールルールと関連しなければなりません（**rule** コマンドを使って設定された許可証または否定ステートメント）。証明書属性グループが属性ルールを持っていないならば、システムは、すべての証明書が関連したアクセス制御ルールとマッチしていると判断します。

例

"mygroup"という名の証明書属性グループを作成し、その View に入ります。

<AP> system-view

[AP] pki certificate attribute-group mygroup

[AP-pki-cert-attribute-group-mygroup]

7.1.25 pki delete-certificate

Syntax

pki delete-certificate domain *domain-name* { **ca** | **local | peer [serial** *serial-num***]** }

View

System view

定義済みユーザロール

network-admin

パラメータ

ca： CA 証明書を指定します。

local：ローカル証明書を指定します。

domain-name：証明書を削除する PKI ドメインの名前を指定します。設定範囲は 1～127 文字です。大文字、小文字は区別しません。ドメイン名は表 7-8 に示す指定記号を設定することができません。

表 7-8 指定記号

名前	記号	名前	記号
チルダ	~	ドット	.
アスタリスク	*	左アングルブラケット	<
バックスラッシュ	¥	右アングルブラケット	>
垂直バー	|	ダブルクォーテーション	"
コロン	:	アポストロフィー	'

peer： ローカルに記録されたピア証明書を削除します。

serial *serial-num*： ピア証明書をシリアル番号で指定します。設定範囲は 1～127 文字です。大文字、小文字は区別しません。シリアル番号を指定しない場合、このコマンドは PKI ドメイン内のすべてのピア証明書を削除します。

説明

pki delete-certificate コマンドは、PKI ドメインから証明書を削除します。

PKI ドメインから CA 証明書を削除すると、PKI ドメイン内のローカル証明書、ピア証明書、CRL も同時に削除されます。

例

PKI ドメイン cer のローカル証明書を削除します。

<AP> system-view

[AP] pki delete-certificate domain cer local

7.1.26 pki domain

Syntax

pki domain *domain-name*

undo pki domain *domain-name*

デフォルト

PKI ドメインはありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-name： PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。ドメイン名には表 7-9 に示す指定記号を設定することができません。

表 7-9 指定記号

名前	記号	名前	記号
チルダ	~	ドット	.
アスタリスク	*	左アングルブラケット	<
バックスラッシュ	¥	右アングルブラケット	>
垂直バー	|	ダブルクォーテーション	"
コロン	:	アポストロフィー	'

説明

pki domain コマンドは、PKI ドメインを作成し、その view に移行するか、既存の PKI domain view に移行します。

undo pki domain コマンドは、PKI ドメインを削除します。

例

PKI ドメインを作成し、その view へ移行します。

<AP> system-view

[AP] pki domain 1

[AP-pki-domain-1]

7.1.27 pki entity

Syntax

pki entity *entity-name*

undo pki entity *entity-name*

デフォルト

エンティティはありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

entity-name： エンティティ名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

説明

pki entity コマンドは、PKI エンティティを作成し、その view に移行するか、既存の PKI エンティティの view に移行します。

undo pki entity コマンドは、PKI エンティティを削除します。

PKI entity view でエンティティの属性の多様性を設定することができます。エンティティは他コマンドによる参照の利便性だけを意図されています。

例

PKI エンティティ名を作成し、その view へ移行します。

<AP> system-view

[AP] pki entity en

[AP-pki-entity-en]

7.1.28 pki import

Syntax

pki import domain *domain-name* { **der** { **ca** | **local** | **peer** } **filename** *filename* | **p12 local filename** *filename* | **pem** { **ca** | **local** | **peer** } [**filename** *filename*] }

View

System view

定義済みユーザロール

network-admin

パラメータ

ca： CA 証明書を指定します。

local： local 証明書を指定します。

peer: ピア証明書を指定します。

domain-name： PKI ドメイン名を指定します。設定範囲は 1～31 文字です。ドメイン名は表 7-10 に示す指定記号を設定することができません。

表 7-10 指定記号

名前	記号	名前	記号
チルダ	~	ドット	.
アスタリスク	*	左アングルブラケット	<
バックスラッシュ	¥	右アングルブラケット	>
垂直バー	|	ダブルクォーテーション	"
コロン	:	アポストロフィー	'

der： DER フォーマットの証明書を指定します。

p12： P12 フォーマットの証明書を指定します。

pem： PEM フォーマットの証明書を指定します。

filename *filename* : 証明書ファイル名を指定します。設定範囲は 1～127 文字です。大文字、小文字は区別しません。PEM フォーマットの証明書のために、ファイルからインポートせずにターミナルの上に証明書内容を貼りつけることもできます。

説明

pki import-certificate コマンドは、CA 証明書またはローカル証明書をファイルからインポートし、ローカルに保存します。

以下の状況で証明書をインポートするために、**pki import** コマンドを使います。

- CRL リポジトリを指定しない CA サーバは、SCEP をサポートしません。
- 証明書がサーバで一杯にした使用は 1 つのファイルの中で重要なペアを生成しました。PKCS12 だけを含む証明書であるか、PEM フォーマットは重要なペアを含むかもしれません。

証明書をインポートする前に、以下を完了させてください。

- 機器のフラッシュメモリに証明書ファイルをアップロードしてください。この場合に、PEM フォーマットの証明書だけがインポートできるので、証明書が PEM フォーマットであることを確かめてください。
- ローカル証明書またはインポートするピア証明書のために、対応する CA 証明書チェーンが存在しなければなりません。CA 証明書チェーンは機器に蓄えられるか、ローカル証明書またはピア証明書に含まれて運ばれることができます。PKI ドメイン、ローカル証明書、またはピア証明書が CA 証明書チェーンを持っていないならば、最初に CA 証明書をインポートする必要があります。

ローカル証明書またはピア証明書をインポートするとき

- ローカル証明書またはインポートされるピア証明書が CA 証明書チェーンを含んでいれば、同時に CA 証明書とローカル証明書またはピア証明書のインポートができます。すでに CA 証明書が PKI ドメインで存在している場合、既存の CA 証明書を上書きするか、システムはプロンプトを表示します。
- ローカルな証明書またはインポートするピア証明書が CA 証明書チェーンを含まないが、すでに CA 証明書が PKI ドメインで存在しているならば、直接ローカル証明書またはピア証明書をインポートできます。

CA 証明書をインポートするとき

- インポートされる CA 証明書が CA ルート証明書であるか、ルート証明書チェーンを含んでいる場合、CA 証明書をインポートができます。
- インポートされる CA 証明書がルート証明書なしで証明書チェーンを含んでいるが、機器の CA 証明書によって完全な証明書チェーンを形成することができる場合は、CA 証明書をインポートすることができます。

以下のシナリオで情報を得るために、CA サーバ管理者に連絡してください。

- インポートする証明書ファイルがルート証明書を含んでいるけれどもルート証明書とフィンガープリントが指定されない。
- インポートするローカル証明書が重要なペアを含んでいるならば、システムは秘密鍵を暗号化するためにチャレンジパスワードの入力を要求します。

重要なペアを含むローカル証明書ファイルをインポートする場合、重要なペアによってドメインをアップデートすることができます。重要なペアの目的に依存して、以下の条件があてはまります。

- 重要なペアの目的が一般的ならば、機器は重要なペアを使います：汎用キーペア、サインキーペア、および暗号化キーペア。
- 重要なペアの目的がサインであるならば、機器は重要なペアを使います：汎用キーペア、サインキーペア。
- 重要なペアの目的が暗号化であるならば、機器はドメインで暗号化キーペアを探します。

マッチが見つかった場合、機器の既存の重要なペアに上書きするかどうかを確認するために、プロンプトを表示します。マッチが見つからないならば、機器は重要なペアの名(デフォルト：PKI ドメインネーム)を入力するように頼みます。そして、証明書ファイルの中で定義された重要なペアのアルゴリズムと目的に従ってそれは重要なペアを生成します。

インポート操作は自動的に正しい重要なペアをアップデートするか、生成します。インポート操作を実行する前に、必ずコンフィギュレーションファイルを保存してください。

例

PEM のフォーマットの CA 証明書を PKI ドメイン cer へインポートします。

<AP> system-view

[AP] pki import-certificate ca domain cer pem

関連コマンド

pki domain

7.1.29 pki request-certificate

Syntax

pki request-certificate domain *domain-name* [**password** *password*] [**pkcs10** [**filename** *filename*]]

Views

System view

定義済みユーザロール

network-admin

パラメータ

domain-name: PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字は区別しません。ドメイン名は表 7-11 に示す指定記号を設定することができません。

表 7-11 指定記号

名前	記号	名前	記号
チルダ	~	ドット	.
アスタリスク	*	左アングルブラケット	<
バックスラッシュ	¥	右アングルブラケット	>
垂直バー	|	ダブルクォーテーション	"
コロン	:	アポストロフィー	'

password *password*: 証明書の取り消しパスワードを、1～31 文字で設定します。大文字、小文字を区別します。パスワードは証明書要求に含まれ、証明書の取り消しをするならば、設定をしてください。

pkcs10: BASE64 でエンコードされた PKCS#10 証明書要求情報を表示します

filename *filename*: PKCS#10 フォーマットの証明書要求を保存する、ローカルファイルを指定します。

説明

pki request-certificate コマンドは、ローカル証明書要求の提出もしくは、PKCS#10 フォーマットの証明書要求を行います。

SCEP が失敗する場合は、以下のタスクのいずれかを実行することができます:

- BASE64 でエンコードされた要求情報を表示するために、**pkcs10** キーワードを使用する。
- 要求情報をローカルファイルに保存し、out-of-band を使ってファイルを CA に転送するために、**pkcs10 filename** *filename* オプションを使ってください。ファイル名は絶対パスを含むことができます。指定されたパスが存在しているならば、要求情報は保存されることができません。

このコマンドはコンフィギュレーションに保存されません。

例

証明書要求の情報を PKCS#10 フォーマットで表示させます。

<AP> system-view

[AP] pki request-certificate domain aaa pkcs10

```
*** Request for general certificate ***
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBTDCBtgIBADANMQswCQYDVQQDEwJqajCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAw5Drj8ofs9THA4ezkDcQPBy8pvH1kumampPsJmx8sGG52NFtbrDTnTT5
ALx3LJijB3d/ndKpcHT/DfbJVDCn5gdw32tBZyCkEwMHZN3ol2z7Nmdcu5TED6iN8
4m+hfp1QWoV6lty3o9pxAXuQl8peUDcfN6WV3LBXYyl1WCtkLkECAwEAAaAAMA0G
CSqGSIb3DQEBBAUAA4GBAA8E7BaIdmT6NVCZgv/I/1tqZH3TS4e4H9Qo5NiCKiEw
R8owVmA0XVtGMbyqBNcDTG0f5NbHrXZQT5+MbFJOnm5K/mn1ro5TJKMTKV46PlCZ
JUjsugaY02GBY0BVcylpC9iIXLuXNIqjh1MBIqVsa1lQOHS7YMvnop6hXAQlkM4c
-----END NEW CERTIFICATE REQUEST-----
```

ローカル証明書をリクエストします。

[AP] pki request-certificate domain openca

```
Start to request general certificate ...
...
Request certificate of domain openca successfully
```

7.1.30 pki retrieve-certificate

Syntax

pki retrieve-certificate domain *domain-name* { **ca** | **local** | **peer** *entity-name* }

View

System view

定義済みユーザロール

network-admin

パラメータ

ca： CA 証明書を読み出します。

local： ローカル証明書を読み出します。

peer *entity-name*： ピアエンティティ名を指定します。設定範囲は 1～31 文字です。大文字、小文字は区別しません。

domain-name： 証明書要求に利用される PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字は区別しません。 ドメイン名は表 7-12 に示す指定記号を設定することができません。

表 7-12 指定記号

名前	記号	名前	記号
チルダ	~	ドット	.
アスタリスク	*	左アングルブラケット	<
バックスラッシュ	¥	右アングルブラケット	>
垂直バー	|	ダブルクォーテーション	"
コロン	:	アポストロフィー	'

説明

pki retrieve-certificate コマンドは、証明書配布サーバから証明書を読み出します。

オンラインモードでは、以下となります。

- SCEP プロトコルを通して CA 証明書を取得することができます。ローカルですでに CA 証明書がある場合、再度 CA 証明書を取得しません。新しい証明書を取得する場合、**pki delete-certificate** コマンドを使用して、CA 証明書、ローカル証明書を削除します。そして再度 CA 証明書を取得します。
- PKI ドメインですでにローカル証明書がある場合、処理を実行し続けます。ローカル証明書は既存の証明書に上書きします。RSA を使用した場合、PKI ドメインは 2 つのローカル証明書を持つことができます。1 つは署名用で、もう一つは暗号化用です。異なる目的のための証明書は上書きされません。

取得した CA 証明書、ローカル証明書は保存する前に自動で確認されます。確認に失敗した場合、保存されません。

このコマンドは設定ファイルに保存されません。

例

証明書発行サーバから CA 証明書を読み出します。（この処理はルート CA 証明局のフィンガープリントを確認することをユーザに要求します。）

<AP> system-view

[AP] pki retrieve-certificate domain aaa ca

```
The trusted CA's finger print is:
   MD5  fingerprint:5C41 E657 A0D6 ECB4 6BD6 1823 7473 AABC
   SHA1 fingerprint:1616 E7A5 D89A 2A99 9419 1C12 D696 8228 87BC C266
Is the finger print correct?(Y/N):y
```

証明書発行サーバからローカル証明書を読み出します。

<AP> system-view

[AP] pki retrieve-certificate domain aaa local

関連コマンド

pki domain

7.1.31 pki retrieve-crl domain

Syntax

pki retrieve-crl domain *domain-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-name： PKI ドメイン名を指定します。設定範囲は 1～31 文字です。ドメイン名は表 7-13 に示す指定記号を設定することができません。

表 7-13 指定記号

名前	記号	名前	記号
チルダ	~	ドット	.
アスタリスク	*	左アングルブラケット	<
バックスラッシュ	¥	右アングルブラケット	>
垂直バー	|	ダブルクォーテーション	"
コロン	:	アポストロフィー	'

説明

pki retrieve-crl domain コマンドは、CRL 配布サーバから最新の CRL を読み出します。

CRL は証明書の有効性を検証します。

例

CRL を読み出します。

<AP> system-view

[AP] pki retrieve-crl domain 1

関連コマンド

pki domain

7.1.32 pki storage

Syntax

pki storage { **certificates** | **crls** } *dir-path*

undo pki storage { **certificates** | **crls** }

デフォルト

証明書と CRL は cfa0:の PKI ディレクトリに保存します。

Views

System view

定義済みユーザロール

network-admin

パラメータ

certificates: 証明書を保存するストレージパスを指定します。

crls: CRL を保存するストレージパスを指定します。

dir-path: ストレージパスを指定します。スラッシュ(/)もしくは、2 つのドット+スラッシュ(../)を含むことはできません。dir-path は絶対パスまたは相対パスで指定し、存在しなければなりません。

説明

pki storage コマンドは、証明書または CRL のストレージパスを指定します。

undo pki storage コマンドは、デフォルトに戻します。

指定されたストレージパスはマスタデバイス上になければなりません。

指定するパスが存在していないならば、最初に **mkdir** コマンドを使ってパスを作成してください。証明書ファイルは.cer または.p12 拡張子を使います。CRL ファイルは.crl ファイル拡張子を使います。

証明書または CRL にストレージパスを変更した後に、証明書ファイルと CRL ファイルは新しいパスに移動します。

例

証明書のストレージパスとして **cfa0:/pki-new** を指定します。

<AP> system-view

[AP] pki storage certificates cfa0:/pki-new

CRL のストレージパスとして **pki-new** を指定します。

<AP> system-view

[AP] pki storage crls pki-new

7.1.33 pki validate-certificate

Syntax

pki validate-certificate domain *domain-name* { **ca** | **local** }

View

System view

定義済みユーザロール

network-admin

パラメータ

ca： CA 証明書を検証します。

local：ローカル証明書を検証します。

domain-name： 検証する証明書が属する PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字は区別しません。ドメイン名は表 7-14 に示す指定記号を設定することができません。

表 7-14 指定記号

名前	記号	名前	記号
チルダ	~	ドット	.
アスタリスク	*	左アングルブラケット	<
バックスラッシュ	¥	右アングルブラケット	>
垂直バー	|	ダブルクォーテーション	"
コロン	:	アポストロフィー	'

説明

pki validate-certificate コマンドは、証明書の有効性を検証します。

通常、証明書は要求、取得、インポートした場合、あるいは PKI を使用している場合、自動で確認されます。

コマンドを使用して証明書の以下の項目を手動で確認することができます。

- 証明書がトラステッド CA であるかを確認します。
- 証明書の有効期限があるかどうかを確認します。
- 証明書が廃止されたかどうかを確認します。CRL の確認が有効な場合のみ、実行します。

CRL チェックが有効な場合、以下のことを行います。

- ローカル証明書を確認する際、PKI ドメインに CRL がない場合、装置はローカルに保存された CRL を確認します。CRL が正しい場合、PKI ドメインに CRL を読み込みます。CRL が正しくない場合、CA サーバから正しい CRL を取得し、ローカルに保存します。
- CA 証明書を確認する際、CRL チェックは、現在の CA からルート CA までの連続した CA 証明書の確認を行います。

例

ローカル証明書の有効性を検証します。

<AP> system-view

[AP] pki validate-certificate local domain 1

関連コマンド

pki domain

7.1.34 public-key dsa

Syntax

public-key dsa name *key-name* [**length** *key-length*]

undo public-key

デフォルト

設定なし

Views

PKI domain view

定義済みユーザロール

network-admin

パラメータ

name *key-name*:キーペアの名前を 1～64 文字で指定します。大文字、小文字は区別しません。キーペアの名はアルファベット，数字、およびハイフン(-)だけを含むことができます。

length *key-length*:キー長を指定します。値範囲は 512～2048 で、デフォルトは 1024 です。

説明

public-key dsa コマンドは、証明書要求のために DSA キーペアを指定します。

undo public-key コマンドは、デフォルトに戻します。

このコマンドで存在しないキーペアを指定することができます。キーペアは以下の方法でも得られることができます。:

- **public-key local create** コマンドでキーペアを生成します。
- アプリケーションは、デジタル署名認証を使っている IKE のように、機器を引き起こして、キーペアを生成します。
- **pki import** コマンドでキーペアを含んでいる証明書をインポートします。

PKI ドメインは、DSA、ECDSA、RSA のいずれかの暗号アルゴリズムを使って、キーペアを持ちます。

複数回 PKI ドメインの DSA キーペアを設定するならば、最後に実行したコンフィギュレーションだけが有効です。

存在しないキーペアを指定した場合に、**length** *key-length* オプションが効果します。機器は、証明書要求を提出する前に指定された name と length を使って自動的にキーペアを作成します。指定したキーペアがすでに存在していると **length** *key-length* オプションは無視されるか、インポート済み証明書に含まれています。

例

2048-bit の DSA キーペア abc の証明書要求をします。

<AP> system-view

[AP] pki domain aaa

[AP-pki-domain-aaa] public-key dsa name abc length 2048

7.1.35 public-key ecdsa

Syntax

public-key ecdsa name *key-name* [**secp192r1** | **secp256r1** | **secp384r1** | **secp521r1**]

undo public-key

デフォルト

設定なし

Views

PKI domain view

定義済みユーザロール

network-admin

パラメータ

name *key-name*: キーペアの名前を 1～64 文字で指定します。大文字、小文字は区別しません。キーペアの名はアルファベット，数字、およびハイフン(-)だけを含むことができます。

secp192r1:キーペアの生成に、secp192r1 を使います。

secp256r1:キーペアの生成に、secp256r1 を使います。

secp384r1: キーペアの生成に、secp384r1 を使います。

secp521r1:キーペアの生成に、secp521r1 を使います。

説明

public-key ecdsa コマンドは、証明書要求の ECDSA キーペアを指定します。

undo public-key コマンドは、デフォルトに戻します。

PKI ドメインに存在しないキーペアを指定することができます。

キーペアは以下のどの方法でも得ることができます。:

- **public-key local create** コマンドでキーペアを生成します。
- アプリケーションは、デジタル署名認証を使っている IKE のように、機器を引き起こして、キーペアを生成します。
- **pki import** コマンドでキーペアを含んでいる証明書をインポートします。

PKI ドメインは、DSA、ECDSA、RSA のいずれかの暗号アルゴリズムを使って、キーペアを持ちます。

存在しないキーペアを指定するならば、指定された設定が効果を生じます。機器は、指定された名前を使って自動的にキーペアを作成し、証明書要求を提出する前に変化させるでしょう。指定された重要なペアがすでに存在しているならば、パラメータは無視されるか、インポート済の証明書にすでに含まれています。

例

#証明書要求に、384bit の ECDSA キーペア"abc"を指定します。

<AP> system-view

[AP] pki domain aaa

[AP-pki-domain-aaa] public-key ecdsa name abc secp384r1

7.1.36 public-key rsa

Syntax

public-key rsa { { **encryption name** *encryption-key-name* [**length** *key-length*] | **signature name** *signature-key-name* [**length** *key-length*] } * | **general name** *key-name* [**length** *key-length*] }

undo public-key

デフォルト

設定なし

Views

PKI domain view

定義済みユーザロール

network-admin

パラメータ

encryption:暗号化のためのキーペアを指定します。

name *encryption-key-name*:キーペアの名前を 1～64 文字で指定します。大文字、小文字は区別しません。キーペアの名はアルファベット，数字、およびハイフン(-)だけを含むことができます。

signature:サインする、キーペアを指定します。

name *signature-key-name*:キーペアの名前を 1～64 文字で指定します。大文字、小文字は区別しません。キーペアの名はアルファベット，数字、およびハイフン(-)だけを含むことができます。

general:サインと暗号化の両方のキーペアを指定します。

name *key-name*: キーペアの名前を 1～64 文字で指定します。大文字、小文字は区別しません。キーペアの名はアルファベット，数字、およびハイフン(-)だけを含むことができます。

length *key-length*: キー長を指定します。値範囲は 512～2048 で、デフォルトは 1024 です。

説明

public-key rsa コマンドは、証明書要求のために RSA キーペアを指定します。

undo public-key コマンドは、デフォルトに戻します。

このコマンドで存在しないキーペアを指定することができます。キーペアは以下の方法でも得られることができます。:

- **public-key local create** コマンドでキーペアを生成します。
- アプリケーションは、デジタル署名認証を使っている IKE のように、機器を引き起こして、キーペアを生成します。
- **pki import** コマンドでキーペアを含んでいる証明書をインポートします。

PKI ドメインは、DSA、ECDSA、RSA のいずれかの暗号アルゴリズムを使って、キーペアを持ちます。

PKI ドメインは、異なる目的の 2 つの RSA キーペアを持つことができます。:一つはサインキーペアであり、もう一つは暗号化キーペアです。複数回サインキーペアまたは RSA 暗号化キーペア設定するならば、最後のコンフィギュレーションだけが効果します。RSA サインキーペアと暗号化キーペアは互いに上書きしません。

サインキーペアと暗号化キーペアを別々に指定する場合、それらのキー長は違うかもしれません。

存在しないキーペアを指定するならば、「**length** *key-length*」オプションは効果を生じます。機器は、証明書要求を提出する前に指定された名前と長さを使って自動的にキーペアを作成するでしょう。指定されたキーペアがすでに存在しているならば、「**length** *key-length*」オプションは無視されるか、輸入証明書の中にすでに含まれています。

例

証明書要求で 2048bit の汎用 RSA キーペア "abc"を指定します。

<AP> system-view

[AP] pki domain aaa

[AP-pki-domain-aaa] public-key rsa general name abc length 2048

証明書要求に以下の RSA キーペアを指定します。:

- 2048bit の RSA 暗号化キーペア "rsa1"
- 2048bit の RSA サインキーペア "sig1"

<AP> system-view

[AP] pki domain aaa

[AP-pki-domain-aaa] public-key rsa encryption name rsa1 length 2048

[AP-pki-domain-aaa] public-key rsa signature name sig1 length 2048

7.1.37 root-certificate fingerprint

Syntax

root-certificate fingerprint { **md5** | **sha1** } *string*

undo root-certificate fingerprint

デフォルト

設定なし

Views

PKI domain view

定義済みユーザロール

network-admin

パラメータ

md5:フィンガープリントを指定します。

sha1:フィンガープリントを指定します。

string: フィンガープリントを 16 進数で指定します。 MD5 を指定した場合は 32 文字、SHA1 指定した場合は、40 文字のフィンガープリントを設定します。

説明

root-certificate fingerprint コマンドは、ルート CA 証明書を確認するフィンガープリントを設定します。

undo root-certificate fingerprint コマンドは、デフォルトに戻します。

CA 証明書を持っていない PKI ドメインのために、証明書要求モードをオートに設定したならば、ルート CA 証明書立証のためにフィンガープリントを設定しなければなりません。ローカル証明書を要求するために、アプリケーション(例えば IKE)をトリガとして機器は自動的に以下を実行します。:

1) CA 証明書を CA サーバから得ます。
2) ルート CA 証明書の中に含まれているフィンガープリントを、以下の条件のどちらかが存在してれば PKI ドメインで設定されたフィンガープリントと比較します。:
   - 得られた CA 証明書がルート証明書
   - 得られた CA 証明書は証明書チェーンであり、機器の上に存在していないルート証明書を含んでいます。

2 つのフィンガープリントがマッチしていない、または PKI ドメインでフィンガープリントが設定されないならば、機器は CA 証明書を拒絶し、ローカル証明書要求が失敗します。

機器が以下の操作を実行するときに、このコマンドによって設定されたフィンガープリントはルート CA 証明書立証のために使われます。:

- **pki import** コマンドで CA 証明書をインポートします。
- pki retrieve-certificate コマンドで、CA 証明書の取得要求をします。

機器はルート CA 証明書に含まれているフィンガープリントを、以下の条件のどちらかが存在していれば PKI ドメインで設定されたフィンガープリントと比較します。:

- インポート、もしくは得られた CA 証明書は、機器上に存在していないルート証明書
- インポート、もしくは得られた CA 証明書は証明書チェーンであり、機器上に存在していないルート証明書を含んでいます。

2 つのフィンガープリントがマッチしていないならば、機器は CA 証明書を拒絶します。PKI ドメインにフィンガープリントが設定されないならば、機器は、手動でルート CA 証明書のフィンガープリントを確認するように促します。

例

#ルート CA 証明書を確認するために、MD5 フィンガープリントを指定します。

<AP> system-view

[AP] pki domain aaa

[AP-pki-domain-aaa] root-certificate fingerprint md5 12EF53FA355CD23E12EF53FA355CD23E

#ルート CA 証明書を確認するために、SHA1 フィンガープリントを指定します。

<AP> system-view

[AP] pki domain aaa

[AP-pki-domain-aaa] root-certificate fingerprint sha1 D1526110AAD7527FB093ED7FC037B0B3CDDDAD93

7.1.38 state

Syntax

state *state-name*

undo state

デフォルト

設定なし

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

state-name : State 名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。コンマは含まれません。

説明

state コマンドは、エンティティが属する state 名を指定します。

undo state コマンドはデフォルトに戻します。

例

エンティティが属する State 名に country を指定します

<AP> system-view

[AP] pki entity 1

[AP-pki-entity-1] state country

目次

このセクションのページは **9-x-x** です。

8 章 SSL 8-1
8.1 SSL 設定コマンド 8-1
8.1.1 certificate-chain-sending enable 8-1
8.1.2 display ssl client-policy 8-2
8.1.3 display ssl server-policy 8-3
8.1.4 pki-domain 8-5
8.1.5 server-verify enable 8-6
8.1.6 ssl client-policy 8-7
8.1.7 ssl server-policy 8-8
8.1.8 ssl version disable 8-9
8.1.9 version 8-10

8章 SSL

8.1 SSL設定コマンド

8.1.1 certificate-chain-sending enable

Syntax

certificate-chain-sending enable

undo certificate-chain-sending enable

デフォルト

SSL ネゴシエーションの実行中、SSL サーバは、完全な証明書チェーンではなくサーバ証明書をクライアントに送信します。

View

SSL server policy view

定義済みユーザロール

network-admin

説明

certificate-chain-sending enable コマンドは SSL ネゴシエーションの実行中に SSL サーバが完全な証明書チェーンをクライアントに送信できるようにします。

undo certificate-chain-sending enable コマンドはデフォルトに戻します。

この機能により、SSL ネゴシエーションプロセスで追加の処理が発生します。SSL クライアントがサーバ証明書を確認するための完全な証明書チェーンを持っていない場合のみ、有効にします。

例

SSL サーバが SSL ネゴシエーションの実行中に完全な証明書チェーンをクライアントに送信できるようにします。

<AP> system-view

[AP] ssl server-policy policy1

[AP-ssl-server-policy-policy1] certificate-chain-sending enable

8.1.2 display ssl client-policy

Syntax

display ssl client-policy [*policy-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

policy-name： SSL クライアントポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字は区別しません。このパラメータを省略した場合、すべての SSL クライアントポリシーに関する情報を表示します。

説明

display ssl client-policy コマンドは、指定された SSL クライアントポリシーまたはすべての SSL クライアントポリシーについての情報を表示します。

例

SSL クライアントポリシーpolicy1 についての情報を表示します。

<AP> display ssl client-policy policy1

```
SSL Client Policy: policy1
    SSL version: TLS 1.0
    PKI domain:
    Preferred ciphersuite:
        DHE_RSA_AES_256_CBC_SHA
        RSA_AES_256_CBC_SHA
        DHE_RSA_AES_128_CBC_SHA
        RSA_AES_128_CBC_SHA
        RSA_3DES_EDE_CBC_SHA
    Server-verify: enabled
```

表8-1 コマンド出力

フィールド	説明
SSL Client Policy	SSLクライアントポリシー名です。

フィールド	説明
SSL version	SSLクライアントポリシーで使用するSSLプロトコルのバージョンです。 • SSL3.0 • TLS1.0 • TLS1.1 • TLS1.2
PKI Domain	SSLクライアントポリシーに使用されるPKIドメインです。
Preferred ciphersuite	SSLクライアントポリシーに使用される暗号スイートの優先順位です。
Server-verify	SSLクライアントが、デジタル証明書を使用してサーバを認証するかを示します。

8.1.3 display ssl server-policy

Syntax

display ssl server-policy [*policy-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

policy-name： SSL サーバポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字は区別しません。このパラメータを省略した場合、すべての SSL サーバポリシーに関する情報を表示します。

説明

display ssl server-policy コマンドは、指定された SSL サーバポリシーまたはすべての SSL サーバポリシーについての情報を表示します。

例

SSL サーバポリシーpolicy1 についての情報を表示します。

<AP> display ssl server-policy policy1

```
SSL server policy: policy1
    Version info:
```

```
    SSL3.0: Disabled
    TLS1.0: Enabled
    TLS1.1: Disabled
    TLS1.2: Enabled
    TLS1.3: Disabled
PKI domains: server-domain
Ciphersuites:
    DHE_RSA_AES_128_CBC_SHA
    RSA_AES_128_CBC_SHA
Session cache size: 600
Caching timeout: 3600 seconds
Client-verify: Enabled
Ciphersuite server-perferred: Disabled
```

表8-2 コマンド出力

フィールド	説明
SSL Server Policy	SSLサーバポリシー名です。
Version info	SSLサーバポリシーで使用するSSLプロトコルのバージョンです。SSLサーバは、有効になっているSSLプロトコルバージョンでのみ、セッションネゴシエーションを行います。 • **SSL3.0** • **TLS1.0** • **TLS1.1** • **TLS1.2** • **TLS1.3** TLS 1.3は、現在のソフトウェアバージョンではサポートされていません。
PKI Domain	SSLサーバポリシーに使用されるPKIドメインです。
Ciphersuite	SSLサーバポリシーにサポートされる暗号スイートです。
Session Timeout	SSLサーバポリシーのセッションタイムアウト時間です(秒) 。
Caching timeout	SSLサーバポリシーのセッションキャッシュタイムアウト時間です(秒)。
Client-verify	デジタル証明書を使用してSSLクライアントを認証するかを示します。 • **Disabled**－クライアント認証は無効。 • **Enabled**－クライアント認証は必須。 • **Optimal**－クライアント認証は任意。

フィールド	説明
Ciphersuite server-perferred	SSLサーバとSSLクライアント間の暗号スイートネゴシエーションで、サーバの優先順位使用の状態を示します。 • **Enabled**－サーバの暗号スイート優先順位を使用します。 • **Disabled**－クライアントの暗号スイート優先順位を使用します。

8.1.4 pki-domain

Syntax

pki-domain *domain-name*

undo pki-domain

デフォルト

設定なし

View

SSL server policy view

SSL client policy view

定義済みユーザロール

network-admin

パラメータ

domain-name: PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字は区別しません。

説明

pki-domain コマンドは、SSL サーバポリシーまたは SSL クライアントポリシーの PKI ドメインを指定します。

undo pki-domain コマンドは、デフォルトに戻します。

例

SSL サーバポリシー **policy1** に、PKI ドメイン **server-domain** を設定します。

<AP> system-view

[AP] ssl server-policy policy1

[AP-ssl-server-policy-policy1] pki-domain server-domain

SSL クライアントポリシー **policy1** に、PKI ドメイン **client-domain** を設定します。

<AP> system-view

[AP] ssl client-policy policy1

[AP-ssl-client-policy-policy1] pki-domain client-domain

関連コマンド

- **display ssl client-policy**
- **display ssl server-policy**

8.1.5 server-verify enable

Syntax

server-verify enable

undo server-verify enable

デフォルト

有効

View

SSL client policy view

定義済みユーザロール

network-admin

説明

server-verify enable コマンドは、デジタル証明書を使用した SSL サーバの認証を有効にします。

undo server-verify enable コマンドはデジタル証明書を使用した SSL サーバの認証を無効にします。

この機能により、SSL クライアントは、デジタル証明書を使用して SSL サーバを認証します。SSL サーバの認証を有効にする場合、SSL サーバは認証のためにデジタル証明書を SSL クライアントに送信する必要があります。SSL クライアントは、サーバが認証に合格した後にのみ、SSL サーバへアクセスできます。

例

SSL クライアントが、デジタル証明書を使用して SSL サーバを認証できるようにします。

<AP> system-view

[AP] ssl client-policy policy1

[AP-ssl-client-policy-policy1] server-verify enable

関連コマンド

display ssl client-policy

8.1.6 ssl client-policy

Syntax

ssl client-policy *policy-name*

undo ssl client-policy *policy-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-name： SSL クライアントポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字は区別しません。

説明

ssl client-policy コマンドは、SSL クライアントポリシーを作成しその view へ移行するか、既存の SSL クライアントポリシーの view へ移行します。

undo ssl client-policy コマンドは、指定された SSL クライアントポリシー、またはすべての SSL クライアントポリシーを削除します。

SSL クライアントポリシーには、クライアントがサーバへの接続を確立するための使用する SSL パラメータを設定します。パラメータには、PKI ドメイン、優先暗号スイートが含まれます。

SSL クライアントポリシーがアプリケーションに関連付けられている場合、SSL クライアントポリシーを削除することはできません。

例

SSL クライアントポリシー **policy1** を作成し、その view へ移行します。

<AP> system-view

[AP] ssl client-policy policy1

[AP-ssl-client-policy-policy1]

関連コマンド

display ssl client-policy

8.1.7 ssl server-policy

Syntax

ssl server-policy *policy-name*

undo ssl server-policy *policy-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-name： SSL サーバポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字は区別しません。

説明

ssl server-policy コマンドは、SSL サーバポリシーを作成しその view へ移行するか、既存の SSL サーバポリシーの view へ移行します。

undo ssl server-policy コマンドは、指定された SSL サーバポリシー、またはすべての SSL サーバポリシーを削除します。

SSL サーバポリシーがアプリケーションに関連付けられている場合、SSL サーバポリシーを削除することはできません。

例

SSL サーバポリシーpolicy1 を作成し、その view へ移行します。

<AP> system-view

[AP] ssl server-policy policy1

[AP-ssl-server-policy-policy1]

関連コマンド

display ssl server-policy

8.1.8 ssl version disable

注意:

SSL Version 設定を変更する場合、**ssl version disable** コマンドあるいは **undo ssl version disable** コマンドを設定したのち、HTTPS サービスを有効にする必要があります。すでに HTTPS サービスが有効である場合、無効にした後、再度有効にしてください。

Syntax

ssl version { **ssl3.0 | tls1.0** | **tls1.1** | **tls1.2** } **disable**

undo ssl version { **ssl3.0 | tls1.0** | **tls1.1** | **tls1.2** } **disable**

デフォルト

SSL3.0、TLS1.0、TLS1.1、TLS1.2 が有効。

View

System view

定義済みユーザロール

network-admin

パラメータ

ssl3.0: SSL3.0 を指定します。

tls1.0: TLS1.0 を指定します。

tls1.1: TLS1.1 を指定します。

tls1.2: TLS1.2 を指定します。

説明

ssl version disable コマンドは SSL サーバがセッションネゴシエーションに特定の SSL プロトコルバージョンを使用しないようにします。

undo ssl version disable コマンドはデフォルトに戻します。

システムセキュリティを強化するために、SSL サーバがセッションネゴシエーションに 特定の SSL プロトコルバージョン(SSL3.0、TLS1.0、TLS1.1 および TLS1.2)を使用しないよう にすることができます。

例

装置で SSL 3.0 を無効にします。

<AP> system-view

[AP] ssl version ssl3.0 disable

8.1.9 version

Syntax

version { **ssl3.0 | tls1.0** | **tls1.1** | **tls1.2** }

undo version { **ssl3.0 | tls1.0** | **tls1.1** | **tls1.2** }

デフォルト

SSL クライアントポリシーでは、SSL プロトコルバージョン TLS1.0 を使用します。

View

SSL client policy view

定義済みユーザロール

network-admin

パラメータ

ssl3.0: SSL3.0 を指定します。

tls1.0: TLS1.0 を指定します。

tls1.1: TLS1.1 を指定します。

tls1.2: TLS1.2 を指定します。

説明

version コマンドは SSL クライアントポリシーで使用する SSL プロトコルバージョンを指定します。

undo version コマンドはデフォルトに戻します。

システムセキュリティを強化するため、SSL プロトコルバージョンに SSL3.0 を指定しないでください。

このコマンドを複数回実行すると、最後に設定した内容が有効になります。

例

SSL クライアントポリシー **policy1** の SSL プロトコルバージョンに TLS1.0 を設定します。

<AP> system-view

[AP] ssl client-policy policy1

[AP-ssl-client-policy-policy1] version tls1.0

目次

このセクションのページは **9-x-x** です。

9 章 接続制限の設定 9-1
9.1 接続制限の設定コマンド 9-1
9.1.1 connection-limit 9-1
9.1.2 connection-limit apply 9-2
9.1.3 connection-limit apply global 9-3
9.1.4 description 9-3
9.1.5 display connection-limit 9-4
9.1.6 display connection-limit statistics 9-7
9.1.7 display connection-limit stat-nodes 9-8
9.1.8 limit 9-10
9.1.9 reset connection-limit statistics 9-12

9章 接続制限の設定

9.1 接続制限の設定コマンド

9.1.1 connection-limit

Syntax

connection-limit { **policy** } *policy-id*

undo connection-limit { **policy** } *policy-id*

デフォルト

接続制限ポリシは存在しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

policy: IPv4 接続制限ポリシを指定します。

policy-id: 接続制限ポリシの ID を指定します。IPv4 接続制限ポリシには独自の番号があります。この引数の値は 1～32 です。

説明

接続制限ポリシを作成してビューに移行するには、**connection-limit** コマンドを使用します。

設定を削除するには、**undo connection-limit** コマンドを使用します。

例

IPv4 接続制限ポリシ 1 を作成してビューに移行します。

<AC> system-view

[AC] connection-limit policy 1

[AC-connlmt-policy-1]

関連コマンド

- **connection-limit apply**
- **connection-limit apply global**
- **display connection-limit**

- **limit**

9.1.2 connection-limit apply

Syntax

connection-limit apply { **policy** } *policy-id*

undo connection-limit apply { **policy** }

デフォルト

接続制限ポリシはインタフェースに適用されていません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

policy: IPv4 接続制限ポリシを指定します。

policy-id: 接続制限ポリシの ID を指定します。本引数の値は 1～32 です。

説明

接続制限ポリシをインタフェースに適用するには、**connection-limit apply** コマンドを使用します。

適用を解除するには、**undo connection-limit apply** コマンドを使用します。

IPv4 接続制限ポリシがインタフェースに適用可能です。新しい IPv4 接続制限ポリシは古いものを上書きします。

例

IPv4 接続制限ポリシ 1 を VLAN インタフェース 2 に適用します。

<AC> system-view

[AC] interface vlan-interface 2

[AC-Vlan-interface2] connection-limit apply policy 1

関連コマンド

- **connection-limit**
- **limit**

9.1.3 connection-limit apply global

Syntax

connection-limit apply global { **policy** } *policy-id*

undo connection-limit apply global { **policy** }

デフォルト

接続制限ポリシはグローバルに適用されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

policy: IPv4 接続制限ポリシを指定します。

policy-id: 接続制限ポリシの ID を指定します。本引数の値は 1～32 です。

説明

接続制限ポリシをグローバルに適用するには、**connection-limit apply global** コマンドを使用します。

適用を解除するには、**undo connection-limit apply global** コマンドを使用します。

IPv4 接続制限ポリシのみがグローバルに適用可能です。新しい IPv4 接続制限ポリシは古いものを上書きします。

例

IPv4 接続制限ポリシ 1 をグローバルに適用します。

<AC> system-view

[AC] connection-limit apply global policy 1

関連コマンド

- **connection-limit**
- **limit**

9.1.4 description

Syntax

description *text*

undo description

デフォルト

接続制限ポリシに説明はありません。

View

IPv4 connection limit policy view

定義済みユーザロール

network-admin

パラメータ

text: 大文字小文字を区別する 1～127 文字の文字列で、接続制限ポリシの説明を指定します。

説明

接続制限ポリシの説明を設定するには、**description** コマンドを使用します。

デフォルトに戻すには、**undo description** コマンドを使用します。

本コマンドを複数回実行した場合、最新の設定が有効になります。

例

IPv4 接続制限ポリシ 1 の説明を CenterToA に設定します。

<AC> system-view

[AC] connection-limit policy 1

[AC-connlmt-policy-1] description CenterToA

関連コマンド

display connection-limit

9.1.5 display connection-limit

Syntax

display connection-limit { **policy** } { *policy-id* | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

policy: IPv4 接続制限ポリシを指定します。

policy-id: 接続制限ポリシの ID を指定します。本引数の値は 1～32 です。

all: すべての接続制限ポリシを指定します。

説明

接続制限ポリシの情報を表示するには、**display connection-limit** コマンドを使用します。

例

すべての IPv4 接続制限ポリシの情報を表示します。

<AC> display connection-limit policy all

```
3 policies in total:
Policy  Rule    Stat Type  HiThres  LoThres  Rate    ACL
--------------------------------------------------------------------------------
     0     1  Src-Dst-Port    2000     1800    10     3000
          12      Src-Dst     500       45     0     3001
         255           --  1000000   980000     0     2001

     1     2     Dst-Port     800      70      0     3010
           3      Src-Dst     100      90      0     3000
          10  Src-Dst-Port      50      45      0     3003
          11          Src     200     200      0     3004
         200           --    500000  498000      0     2002

    28     4         Port    1500    1400      0     3100
           5          Dst    3000     280      0     3101
          21      Src-Dst     200     180      0     3102
          25     Src-Port      50      35      0     3200
Description list:
 Policy     Description
--------------------------------------------------------------------------------
     1      IPv4Description1
    28     Description for IPv4 28
```

IPv4 接続制限ポリシ 1 の情報を表示します。

<AC> display connection-limit policy 1

```
IPv4 connection limit policy 1 has been applied 5 times, and has 5 limit rules.
Description: IPv4Description1
Limit rule list:
Policy  Rule    Stat Type  HiThres  LoThres    Rate   ACL
--------------------------------------------------------------------------------
     1     2     Dst-Port     800      700     10     3010
```

```
          3      Src-Dst     100       90     0      3000
         10  Src-Dst-Port      50       45     0      3003
         11           Src     200      200     0      3004
        200            --  500000   498000     0      2002
Application list:
   Vlan-interface2
   Global
```

表 9-1 コマンド出力

フィールド	説明
Limit rule list	接続制限ポリシ情報
Policy	接続制限ポリシ数
Rule	接続制限ルール数
Stat Type	統計情報タイプ ● Src-Dst-Port—送信元IP、宛先IP、サービスの組合せで接続を制限する ● Src-Dst—送信元IPアドレス、宛先IPアドレスの組合せで接続を制限する ● Src-Port—送信元IP、サービスの組合せで接続を制限する ● Dst-Port—宛先IP、サービスの組合せで接続を制限する ● Src—送信元IPアドレスで接続を制限する ● Dst—宛先IPアドレスで接続を制限する ● Port—サービスで接続を制限する ● --—特定の送信元IP、宛先IP、サービスで接続を制限しない、ルールによって使用されるACLにマッチするすべての接続は制限される
HiThres	接続の上限
LoThres	接続の下限
Rate	確立された1秒あたりの接続数。
ACL	ルールによって使用されるACL番号または名前
Application list	接続制限ポリシの適用リストで、インタフェース名とGlobalを含む。Globalは接続制限ポリシがグローバル胃適用されることを示す。
Description	接続制限ポリシの説明
Description list	接続制限ポリシ説明のリスト

関連コマンド

- **connection-limit**
- **connection-limit apply**
- **connection-limit apply global**
- **limit**

9.1.6 display connection-limit statistics

Syntax

display connection-limit statistics { **global** | **interface** *interface-type interface-number* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

global: グローバル接続統計情報を表示します。

interface *interface-type interface-number*: タイプと番号でインタフェースを指定します。

説明

グローバルまたはインタフェースの接続制限統計情報を表示するには、**display connection-limit statistics** コマンドを使用します。

例

グローバル接続制限統計情報を表示します。

<AC> display connection-limit statistics global

```
Connection limit statistics (Global, slot 1):
   Dropped IPv4 packets:  54781
   Dropped IPv6 packets:  11457
```

表 9-2 コマンド出力

フィールド	説明
Dropped IPv4 packet	IPv4接続制限ポリシがグローバルまたはインタフェースで設定されている場合に、接続上限を超過したために廃棄されたIPv4パケット数
Dropped IPv6 packet	IPv6接続制限ポリシがグローバルまたはインタフェースで設定されている場合に、接続上限を超過したために廃棄されたIPv6パケット数

関連コマンド

- **connection-limit**
- **connection-limit apply**
- **connection-limit apply global**
- **limit**

9.1.7 display connection-limit stat-nodes

Syntax

display connection-limit stat-nodes { **global** | **interface** *interface-type interface-number* } [**destination** *destination-ip* | **service-port** *port-number* | **source** *source-ip*] * [**count**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

global:接続制限ルールにグローバルに合致する IPv4 接続の統計情報を表示します。

interface *interface-type interface-number*: タイプと番号でインタフェースを指定します。

destination *destination-ip*: IP アドレスで宛先を指定します。

service-port *port-number*: ポート番号でサービスポートを指定します。

source *source-ip*: IP アドレスで送信元を指定します。

count: 制限ルールベースの統計情報セット数のみを表示します。指定した IPv4 接続に関する詳細情報は表示されません。本キーワードを指定しなかった場合、本コマンドは接続制限ルールにマッチする指定された IPv4 接続に関する詳細情報を表示します。

説明

グローバルまたはインタフェースの接続制限ルールに合致する IPv4 接続に関する統計情報を表示するには、**display connection-limit stat-nodes** コマンドを使用します。

接続制限ルールにマッチする接続の統計情報は、以下の情報を含みます。

- 接続情報、接続の送信元/宛先 IP アドレス、サービスポート、トランスポート層プロトコルを含みます。
- マッチする接続制限ルール
- 現在の接続数
- 新規接続が作成可能か否か

出力情報をさらにフィルタリングするには、コマンドで以下のオプションを指定します。

- source source-ip
- destination destination-ip
- service-port port-number

例えば、source source-ip と destination destination-ip の組合せを指定した場合、本コマンドは送信元 IP アドレスと宛先 IP アドレスにより接続制限ルールにマッチする IPv4 接続に関する統計情報を表示します。

source source-ip、destination destination-ip、service-port port-number オプションのいずれも指定しなかった場合、本コマンドは接続制限ルールにマッチするすべての IPv4 接続に関する統計情報を表示します。

例

VLAN インタフェース 2 上で接続制限ルールにマッチするすべての IPv4 接続に関する統計情報を表示します。

<AC> display connection-limit stat-nodes interface vlan-interface 2

```
Src IP address         : 100.100.100.100
   VPN instance        : 01234567890123456789012345678901
Dst IP address         : 200.200.200.200
   VPN instance        : abcdefghijklmnopqrstuvwxyzabcde
Tunnel ID              : 1234567890
Service                : tcp/12345
Limit rule ID          : 12345(ACL: 3001)
Sessions threshold Hi/Lo: 1100000/980000
Sessions count         : 1050000
Sessions limit rate    : 0
New session flag       : Permit
```

グローバルのルールベース統計情報セットの数を表示します。

<AC> display connection-limit stat-nodes global count

```
     Current limit statistic nodes count is 5.
```

表 9-3 コマンド出力

フィールド	説明
Src IP address	送信元IPアドレス
Dst IP address	宛先IPアドレス
VPN instance	IPアドレスが所属するMPLS L3VPN。2つのハイフン（--）は、IPアドレスがパブリックネットワーク上にあることを示す。本フィールドは、現ソフトウェアバージョンではサポートされない。
Tunnel ID	DS-Liteトンネルの IDです。2つのハイフン（--）は、IPアドレスがパブリックネットワーク上にあることを示す。本フィールドは、現ソフトウェアバージョンではサポートされない。
Service	プロトコル名とサービスポート番号 well-knownでないプロトコルでは、本フィールドはunknown(xx)と表示される。(xx)はプロトコル番号を示す。ICMPプロトコルでは、プロトコル番号は、type、codeフィールドの十六進の内容から変換された十進数。
Sessions threshold Hi/Lo	接続制限の上限および下限
Sessions count	現在の接続数
Sessions limit rate	1秒あたりに確立された最大接続数。
New session flag	新規接続が作成可能か否か • Permit—新規接続は作成可能 • Deny—新規接続は作成不可能

関連コマンド

- **connection-limit apply global policy**
- **connection-limit apply policy**
- **connection-limit policy**
- **limit**

9.1.8 limit

Syntax

limit *limit-id* **acl** { *acl-number* | **name** *acl-name* } [**per-destination** | **per-service** | **per-source**] * { **amount** *max-amount min-amount* | **rate** *rate* } * [**description** *text*]

undo limit *limit-id*

デフォルト

接続制限ポリシには接続制限ルールは存在しません。

View

IPv4 connection limit policy view

定義済みユーザロール

network-admin

パラメータ

limit-id: ID で接続制限ルールを指定します。本引数の値の範囲は 1～256 です。

acl: ユーザレンジにマッチする ACL を指定します。ACL にマッチするユーザ接続のみが制限されます。

acl-number: ACL を番号で指定します。範囲は 2000～3999 です。

name *acl-name*: ACL を名前で指定します。

per-destination: 宛先 IP アドレスで接続を制限します。

per-service: トランスポート層プロトコルとサービスポートに基づいて、サービスで接続を制限します。

per-source: 送信元 IP アドレスで接続を制限します。

amount: 接続数を制限します。

max-amount: 接続上限を指定します。範囲は 1～4294967294 です。ユーザ接続が接続上限を超過すると、新規の接続が作成できません。

min-amount: 接続下限を指定します。範囲は 1～4294967294 です。接続下限は接続上限よりも大きな値を取ってはいけません。接続数が接続下限を下回るまで、新規の接続は作成できません。

rate: 接続確立レートを制限します。

rate: 1 秒あたりに確立される接続の最大数を指定します。範囲は 5～10000000 です。

description *text*: 接続制限ルールの説明を指定します。大文字と小文字を区別する 1～127 文字の文字列です。デフォルトでは、接続制限ルールには説明がありません。

説明

接続制限ルールを設定するには、**limit** コマンドを使用します。

指定した接続制限ルールを削除するには、**undo limit** コマンドを使用します。

それぞれの接続制限ポリシは複数のルールを定義可能で、それぞれのルールは使用される ACL、ルールタイプ、接続上限／下限と接続確立レート制限のいずれかを指定する必要があります。

1 つのルール内では、**per-destination**、**per-source**、**per-service** キーワードのうち 1 つまたは複数を指定可能です。例えば、**per-destination** と **per-source** の組合せが指定された場合、接続は送信元 IP アドレスと宛先 IP アドレスにより制限されます。同一の送信元 IP アドレスと宛先 IP アドレスの接続は同一のタイプです。

接続制限ルールを設定するときは、次の制約事項とガイドラインに従ってください。

- 同一の接続制限ポリシ内での異なるルールは、異なる ACL を使用する必要があります。
- **per-destination**、**per-source**、**per-service** キーワードを 1 つも指定しなかった場合、指定された ACL にマッチするすべての接続が指定された値で制限されます。
- 装置上で確立している接続が接続制限ポリシにマッチした場合、ポリシ内の制限ルールはルール ID の昇順でマッチされます。
- 指定されている ACL が変更された場合、確立している接続は新しい接続制限ポリシによって制限されます。

例

IPv4 接続制限ポリシ 1 に接続制限ルール 1 を設定します。

1)　ACL3000 を設定します。

<AC> system-view

[AC] acl advanced 3000

[AC-acl-ipv4-adv-3000] rule permit ip source 192.168.0.0 0.0.0.255

[AC-acl-ipv4-adv-3000] quit

2)　送信元および宛先 IP アドレスによる接続上限 2000、接続下限 1800、確立レート 10 /秒の ACL3000 にマッチする接続を制限します。

[AC] connection-limit policy 1

[AC-connlmt-policy-1] limit 1 acl 3000 per-destination per-source amount 2000 1800 rate 10

3)　接続数が 2000 を越えると、接続数が 1800 を下回らなければ新規の接続が確立できないことを確認します（詳細は示しません）。

関連コマンド

- **connection-limit**
- **display connection-limit**

9.1.9 reset connection-limit statistics

Syntax

reset connection-limit statistics { **global** | **interface** *interface-type interface-number* }

View

User view

定義済みユーザロール

network-admin
network-operator

パラメータ

global: グローバル接続制限統計情報をクリアします。

interface *interface-type interface-number*: タイプと番号でインタフェースを指定します。

説明

グローバルまたはインタフェースの接続制限統計情報をクリアするには、**reset connection-limit statistics** コマンドを使用します。

例

VLAN インタフェース 2 の接続制限統計情報をクリアします。

<AC> reset connection-limit statistics interface vlan-interface 2

関連コマンド

display connection-limit statistics

目次

このセクションのページは **9-x-x** です。

10 章 IP ソースガード 10-1
10.1 IP ソースガード設定コマンド 10-1
10.1.1 ip verify source 10-1

10章 IP ソースガード

10.1 IPソースガード設定コマンド

10.1.1 ip verify source

Syntax

ip verify source

undo ip verify source

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

説明

ip verify source コマンドは IPSG（IPv4 ソースガード）機能を有効にします。

undo ip verify source コマンドはデフォルトに戻します。

この機能は WLAN スヌーピングエントリを使用して、AP から受信する IPv4 パケットをフィルタします。WLAN スヌーピングエントリに一致しないパケットを廃棄します。WLAN スヌーピングエントリは IP-MAC バインディングです。

IPv4 ネットワークにおいて、IPSG は DHCP パケットから取得した WLAN スヌーピングエントリのみを使用します。

例

IPv4 に対して IPSG 機能を有効にします。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] ip verify source

目次

このセクションのページは **9-x-x** です。

11 章 ARP アタックプロテクション 11-1
11.1 送信元 MAC ベース ARP アタック detection 設定コマンド 11-1
11.1.1 arp source-mac 11-1
11.1.2 arp source-mac aging-time 11-2
11.1.3 arp source-mac exclude-mac 11-2
11.1.4 arp source-mac threshold 11-3
11.1.5 display arp source-mac 11-4
11.2 ARP パケット送信元 MAC アドレス整合性チェック設定コマンド 11-5
11.2.1 arp valid-check enable 11-5
11.3 ARP 確認応答設定コマンド 11-6
11.3.1 arp active-ack enable 11-6
11.4 ARP アタック detection 設定コマンド 11-6
11.4.1 arp detection enable 11-6
11.4.2 arp detection trust 11-7
11.4.3 arp detection validate 11-8
11.4.4 arp restricted-forwarding enable 11-9
11.4.5 display arp detection 11-9
11.4.6 display arp detection statistics 11-10
11.5 ARP ゲートウェイプロテクション設定コマンド 11-11
11.5.1 arp filter source 11-11
11.6 ARP フィルタリング設定コマンド 11-12
11.6.1 arp filter binding 11-12

11章 ARP アタックプロテクション

11.1 送信元MACベースARPアタックdetection設定コマンド

11.1.1 arp source-mac

Syntax

arp source-mac { **filter** | **monitor** }

undo arp source-mac [**filter** | **monitor**]

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

filter: ログメッセージの生成を行い、MAC アドレスから後続の ARP パケットを破棄します。

monitor: ログメッセージの生成のみを行います。

説明

arp source-mac コマンドは送信元 MAC アドレスにもとづいた ARP アタック detection を有効にし、処理方法を指定します。

undo arp source-mac コマンドはデフォルトに戻します。

本コマンドはゲートウェイで設定します。

本機能は CPU に送信された ARP パケットの数を確認します。同一 MAC アドレスから 5 秒以内に受信された ARP パケットの数がしきい値を超えた場合、装置は攻撃に対処するため、事前に設定された方式を使用します。

undo arp anti-attack source-mac コマンドで **filter** パラメータ、**monitor** パラメータのどちらも指定されなかった場合、本機能は無効になります。

例

送信元 MAC アドレスにもとづいた ARP アタック detection を有効にし、処理方法を filter に指定します。

<AC> system-view

[AC] arp source-mac filter

11.1.2 arp source-mac aging-time

Syntax

arp source-mac aging-time *time*

undo arp source-mac aging-time

デフォルト

300 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

time: ARP アタックエントリのエージングタイマを設定します。設定範囲は 60～6000 秒です。

説明

arp source-mac aging-time コマンドは ARP アタックエントリのエージングタイマを設定します。

undo arp anti-attack source-mac aging-time コマンドはデフォルトに戻します。

例

ARP アタックエントリのエージングタイマを 60 秒に設定します。

<AC> system-view

[AC] arp source-mac aging-time 60

11.1.3 arp source-mac exclude-mac

Syntax

arp source-mac exclude-mac *mac-address*&<1-10>

undo arp source-mac exclude-mac [*mac-address*&<1-10>]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-address&<1-10>: 除外する MAC アドレスのリストを指定します。形式は H-H-H です。&<1-10>は除外する MAC アドレスを 10 まで設定できることを示します。

説明

arp source-mac exclude-mac コマンドは送信元 MAC アドレスにもとづいた ARP アタック detection から指定された MAC アドレスを除外します。

undo arp source-mac exclude-mac コマンドは除外する MAC アドレスを削除します。

undo arp source-mac exclude-mac コマンドで MAC アドレスを指定しない場合、除外されたすべての MAC アドレスを削除します。

例

送信元 MAC にもとづいた ARP アタック detection から指定された MAC アドレスを除外します。

<AC> system-view

[AC] arp source-mac exclude-mac 2-2-2

11.1.4 arp source-mac threshold

Syntax

arp source-mac threshold *threshold-value*

undo arp source-mac threshold

デフォルト

50

View

System view

定義済みユーザロール

network-admin

パラメータ

threshold-value: 送信元 MAC アドレスにもとづいた ARP アタック detection のしきい値を指定します。設定範囲は 1～5000 です。

説明

arp source-mac threshold コマンドは送信元 MAC アドレスにもとづいた ARP アタック detection のしきい値を指定します。同一 MAC アドレスから 5 秒以内に受信された ARP パケットの数が上限を超えた場合、装置はこれを攻撃と判断します。

undo arp source-mac threshold コマンドはデフォルトに戻します。

例

送信元 MAC アドレスにもとづいた ARP アタック detection のしきい値を 30 に指定します。

<AC> system-view

[AC] arp source-mac threshold 30

11.1.5 display arp source-mac

Syntax

display arp source-mac interface *interface-type interface-number*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

説明

display arp source-mac コマンドは送信元 MAC アドレスにもとづいた ARP アタック detection によって検出された ARP アタックエントリを表示します。

例

GigabitEthernet 1/0/1 で送信元 MAC アドレスにもとづいた ARP アタック detection によって検出された ARP アタックエントリを表示します。

<AC> display arp source-mac interface gigabitethernet 1/0/1

```
Source-MAC        VLAN ID  Interface            Aging-time
```

```
23f3-1122-3344     4094    GE1/0/1              10
23f3-1122-3355     4094    GE1/0/2              30
23f3-1122-33ff     4094    GE1/0/3              25
23f3-1122-33ad     4094    GE1/0/4              30
23f3-1122-33ce     4094    GE1/0/5              2
```

11.2 ARPパケット送信元MACアドレス整合性チェック設定コマンド

11.2.1 arp valid-check enable

Syntax

arp valid-check enable

undo arp valid-check enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

arp valid-check enable コマンドはゲートウェイで ARP パケット送信元 MAC アドレス整合性チェックを有効にします。

undo arp valid-check enable コマンドは ARP パケット送信元 MAC アドレス整合性チェックを無効にします。

本コマンドはゲートウェイで設定します。ゲートウェイは Ethernet ヘッダの送信元 MAC アドレスが ARP メッセージの送信 MAC アドレスと異なる場合、破棄します。

例

ARP パケット送信元 MAC アドレス整合性チェックを有効にします。

<AC> system-view

[AC] arp valid-check enable

11.3 ARP確認応答設定コマンド

11.3.1 arp active-ack enable

Syntax

arp active-ack enable

undo arp active-ack enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

arp active-ack enable コマンドは ARP 確認応答機能を有効にします。

undo arp active-ack enable コマンドはデフォルトに戻します。

本コマンドはゲートウェイでユーザのなりすましを防止します。

例

ARP 確認応答機能を有効にします。

<AC> system-view

[AC] arp active-ack enable

11.4 ARPアタックdetection設定コマンド

11.4.1 arp detection enable

Syntax

arp detection enable

undo arp detection enable

デフォルト

無効

View

VLAN view

定義済みユーザロール

network-admin

説明

arp detection enable コマンドは ARP アタック detection を有効にします。

undo arp detection enable コマンドはデフォルトに戻します。

例

VLAN 2 で ARP アタック detection を有効にします。

<AC> system-view

[AC] vlan 2

[AC-vlan2] arp detection enable

関連コマンド

arp detection rule

11.4.2 arp detection trust

Syntax

arp detection trust

undo arp detection trust

デフォルト

インタフェースは非 ARP トラステッドポートです。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

arp detection trust コマンドはインタフェースを ARP トラステッドポートとして設定します。

undo arp detection trust コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 を ARP トラステッドポートとして設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] arp detection trust

11.4.3 arp detection validate

Syntax

arp detection validate { **dst-mac** | **ip** | **src-mac** } *

undo arp detection validate [**dst-mac** | **ip** | **src-mac**] *

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

dst-mac: ARP 応答の宛先 MAC アドレスを確認します。宛先 MAC アドレスがすべて 0、すべて 1、イーサネットヘッダ内の送信先 MAC アドレスに矛盾があった場合、パケットは無効と見なされ、破棄されます。

ip: ARP 応答の送信元 IP アドレスと宛先 IP アドレスを確認します。ARP 要求の送信元 IP アドレスがすべて 1 かマルチキャスト IP アドレスである場合、パケットは無効と見なされ、破棄されます。

src-mac: ARP パケットの送信元 MAC アドレスがイーサネットヘッダ内の送信元 MAC アドレスと同一かどうかをチェックします。同一だった場合、パケットは有効と見なされ、同一でなかった場合は、パケットは破棄されます。

説明

arp detection validate コマンドは ARP パケットの正当性の確認を有効にします。

undo arp detection validate コマンドは ARP パケットの正当性の確認を無効にします。

1 つのコマンドで確認する 1 つあるいは複数のオブジェクトを指定することができます。**undo arp detection validate** コマンドでパラメータを指定しない場合、すべてのオブジェクトについて、ARP パケットの正当性の確認を無効にします。

例

ARP パケットの MAC アドレスと IP アドレスを確認する ARP パケットの正当性の確認を有効にします。

<AC> system-view

[AC] arp detection validate dst-mac src-mac ip

11.4.4 arp restricted-forwarding enable

Syntax

arp restricted-forwarding enable

undo arp restricted-forwarding enable

デフォルト

無効

View

VLAN view

定義済みユーザロール

network-admin

説明

arp restricted-forwarding enable コマンドは ARP 制限転送を有効にします。

undo arp restricted-forwarding enable コマンドは ARP 制限転送を無効にします。

例

VLAN 2 で ARP 制限転送を有効にします。

<AC> system-view

[AC] vlan 2

[AC-vlan2] arp restricted-forwarding enable

11.4.5 display arp detection

Syntax

display arp detection

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display arp detection コマンドは ARP アタック detection が有効な VLAN を表示します。

例

ARP アタック detection が有効な VLAN を表示します。

<AC> display arp detection

```
ARP detection is enabled in the following VLANs:
1-2, 4-5
```

関連コマンド

arp detection enable

11.4.6 display arp detection statistics

Syntax

display arp detection statistics [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースの ARP detection の統計情報を表示します。

説明

display arp detection statistics コマンドは ARP アタック detection の統計情報を表示します。

本コマンドはユーザの正当性の確認および ARP パケットの正当性の確認で廃棄されたパケットの数を表示します。インタフェースを指定しなかった場合、すべてのインタフェースの統計情報を表示します

例

すべてのインタフェースの ARP アタック detection の統計情報を表示します。

<AC> display arp detection statistics

```
State: U-Untrusted  T-Trusted
ARP packets dropped by ARP inspect checking:
```

```
Interface(State)            IP        Src-MAC   Dst-MAC   Inspect
GE1/0/1(U)                  40        0         0         78
GE1/0/2(U)                  0         0         0         0
GE1/0/3(T)                  0         0         0         0
GE1/0/4(U)                  0         0         30        0
```

表 11-1 コマンド出力

フィールド	説明
State	インタフェースの状態 ● **U**—非ARPトラステッドインタフェースです。 ● **T**— ARPトラステッドインタフェースです。
Interface(State)	ARPパケットの受信インタフェース Stateはポートの状態を示します。**trusted**あるいは**untrusted**です。
IP	送信元IPアドレスと宛先IPアドレスが無効であるため、廃棄されたARPパケットの数
Src-MAC	送信元MACアドレスが無効であるため、廃棄されたARPパケットの数
Dst-MAC	宛先MACアドレスが無効であるため、廃棄されたARPパケットの数
Inspect	ユーザの正当性の確認が無効であるため、廃棄されたARPパケットの数です。

11.5 ARPゲートウェイプロテクション設定コマンド

11.5.1 arp filter source

Syntax

arp filter source *ip-address*

undo arp filter source *ip-address*

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: プロテクトされるゲートウェイの IP アドレスを指定します。

説明

arp filter source コマンドは ARP ゲートウェイプロテクションを有効にします。

undo arp filter source コマンドは ARP ゲートウェイプロテクションを無効にします。

インタフェースで最大 8 つの ARP ゲートウェイプロテクションを有効にすることができます。

arp filter source コマンドと **arp filter binding** コマンドを同一インタフェースに設定することはできません。

例

IP アドレス 1.1.1.1 のゲートウェイに ARP ゲートウェイプロテクションを有効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] arp filter source 1.1.1.1

11.6 ARPフィルタリング設定コマンド

11.6.1 arp filter binding

Syntax

arp filter binding *ip-address mac-address*

undo arp filter binding *ip-address*

デフォルト

ARP フィルタリングエントリは設定されていません。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: 許可された送信元 IP アドレスを指定します。

mac-address: 許可された送信元 MAC アドレスを指定します。

説明

arp filter binding コマンドは許可される ARP フィルタリングエントリを設定します。ARP パケットの送信元 IP アドレスと送信元 MAC アドレスが許可された ARP フィルタリングエントリに一致した場合、ARP パケットは許可されます。一致しなかった場合は破棄されます。

undo arp filter binding コマンドは ARP フィルタリングエントリを削除します。

インタフェースで最大 8 つの ARP フィルタリングエントリを設定することができます。

arp filter binding コマンドと **arp filter source** コマンドを同一インタフェースに設定することはできません。

例

許可される ARP フィルタリングエントリを設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] arp filter binding 1.1.1.1 2-2-2

目次

このセクションのページは **9-x-x** です。

12 章 ユーザアイソレーション 12-1
12.1 ユーザアイソレーションコマンド 12-1
12.1.1 display user-isolation statistics 12-1
12.1.2 reset user-isolation statistics 12-2
12.1.3 user-isolation enable 12-3
12.1.4 user-isolation permit-broadcast 12-4
12.1.5 user-isolation vlan enable 12-4
12.1.6 user-isolation vlan permit-mac 12-5

12章 ユーザアイソレーション

12.1 ユーザアイソレーションコマンド

12.1.1 display user-isolation statistics

🕮 メモ：

slot のパラメータは、ソフトウェアバージョン 7.2.82 を含む以降のソフトウェアからサポートしています。

Syntax

display user-isolation statistics [**vlan** *vlan-id*] [**slot** *slot-number*]

Views

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan *vlan-id*: VLAN を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のユーザアイソレーションの統計情報を表示します。

slot *slot-number*: slot を指定します。設定範囲は 1～2 です。指定しない場合、すべての slot のユーザアイソレーションの統計情報を表示します。

説明

display user-isolation statistics コマンドは VLAN、あるいはすべての VLAN のユーザアイソレーションの統計情報を表示します。

例

すべての VLAN のユーザアイソレーションの統計情報を表示します。

<AC> display user-isolation statistics

```
Number of VLANs enabled with user isolation: 2
Number of VLANs disabled with user isolation: 1

VLAN     State       Drops          Permit unicast       Permitted MAC list
4        Enabled     0              Y                    N/A
6        Disabled    0              N                    0023-89a2-3d4d
```

```
                                                    0033-89a2-3d4a
5       Enabled     0             Y                 N/A
```

表 12-1 コマンド出力

フィールド	説明
VLAN	VLAN IDです。
State	VLANのユーザアイソレーションの状態です。 • **Enabled**－有効です。 • **Disabled**－無効です。
Drops	VLANで廃棄したパケット数です。
Permit unicast	VLANのユーザ間でユニキャストパケットが許可されるかどうかを示します。 • **Y**－許可します。ブロードキャスト、マルチキャストパケットのみ隔離されます。 • **N**－許可しません。ユニキャスト、ブロードキャスト、マルチキャストパケットのすべてのパケットが隔離されます。
Permitted MAC list	VLANの許可されているMACアドレスリストです。

関連コマンド

- **user-isolation vlan enable**
- **user-isolation vlan permit-mac**

12.1.2 reset user-isolation statistics

Syntax

reset user-isolation statistics [**vlan** *vlan-id*]

View

User view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id*: VLAN を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のユーザアイソレーションの統計情報を削除します。

説明

reset user-isolation statistics コマンドは VLAN、あるいはすべての VLAN のユーザアイソレーションの統計情報を削除します。

例

VLAN 1 のユーザアイソレーションの統計情報を削除します。

<AC> reset user-isolation statistics vlan 1

関連コマンド

- **user-isolation vlan enable**
- **user-isolation vlan permit-mac**

12.1.3 user-isolation enable

Syntax

user-isolation enable

undo user-isolation enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

user-isolation enable コマンドは SSID ベースのユーザアイソレーションを有効にします。

undo user-isolation enable コマンドはデフォルトに戻します。

例

SSID ベースのユーザアイソレーションを有効にします。

<AC> system-view

[AC] wlan service-template 1

[AC -wlan-st-1] user-isolation enable

12.1.4 user-isolation permit-broadcast

Syntax

user-isolation permit-broadcast

undo user-isolation permit-broadcast

デフォルト

ユーザアイソレーションが有効の場合、装置はブロードキャストトラフィックとマルチキャストトラフィックを転送しません。

View

System view

定義済みユーザロール

network-admin

説明

user-isolation permit-broadcast コマンドは有線のユーザから無線のユーザに送信されたブロードキャストトラフィックとマルチキャストトラフィックを許可します。

undo user-isolation permit-broadcast コマンドはデフォルトに戻します。

有線のユーザと無線のユーザが同一の VLAN に属しているときのみ、無線のユーザから有線のユーザへのブロードキャストパケットとマルチキャストパケットを隔離します。

例

有線のユーザから無線のユーザに送信されたブロードキャストトラフィックとマルチキャストトラフィックを許可します。

<AC> system-view

[AC] user-isolation permit-broadcast

関連コマンド

user-isolation vlan enable

12.1.5 user-isolation vlan enable

Syntax

user-isolation vlan *vlan-list* **enable** [**permit-unicast**]

undo user-isolation vlan *vlan-list* **enable**

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: VLAN を指定します。半角スペースで区切ることで 10 の VLAN を指定することができます。各 VLAN は VLAN ID で VLAN を指定あるいは *vlan-id1* **to** *vlan-id2* の形式で指定します。VLAN ID の設定範囲は 1～4094 です。VLAN の範囲を指定する場合、*vlan-id2* は *vlan-id1* よりも大きい値にしてください。

permit-unicast: ユーザ間のユニキャストパケットを許可します。指定しない場合、ブロードキャストパケット、マルチキャストパケットと同様にユニキャストパケットをユーザ間で隔離します。

説明

user-isolation vlan enable コマンドは VLAN リストのユーザアイソレーションを有効にします。

undo user-isolation vlan enable コマンドは VLAN リストのユーザアイソレーションを無効にします。

外部ネットワークへの切断を防ぐため、ゲートウェイの MAC アドレスを許可された MAC アドレスリストに割り当てます。許可された MAC アドレスを追加する場合、**user-isolation vlan permit-mac** コマンドを使用します。

user-isolation vlan enable コマンドを複数実行した場合、最後に行った設定を適用します。

例

VLAN 1 のユーザアイソレーションを有効にします。

<AC> system-view

[AC] user-isolation vlan 1 enable

12.1.6 user-isolation vlan permit-mac

Syntax

user-isolation vlan vlan-list permit-mac *mac-list*

undo user-isolation vlan vlan-list permit-mac { *mac-list* | **all** }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: VLAN を指定します。半角スペースで区切ることで 10 の VLAN を指定することができます。各 VLAN は VLAN ID で VLAN を指定あるいは *vlan-id1* **to** *vlan-id2* の形式で指定します。VLAN ID の設定範囲は 1～4094 です。VLAN の範囲を指定する場合、*vlan-id2* は *vlan-id1* よりも大きい値にしてください。

mac-list: MAC アドレスを指定します。半角スペースで区切ることで 16 の MAC アドレスを指定することができます。MAC アドレスの形式は H-H-H で指定します。ブロードキャスト MAC アドレス、マルチキャスト MAC アドレスを指定することはできません。

説明

user-isolation vlan permit-mac コマンドは VLAN リストで許可された MAC アドレスリストを設定します。

undo user-isolation vlan enable コマンドは VLAN の許可された MAC アドレスリストを削除します。

許可された MAC アドレスをもつユーザからのパケットは対応する VLAN で隔離されません。

user-isolation vlan permit-mac コマンドは最大 16 の MAC アドレスを登録できます。

ソフトウェアバージョン 7.2.13 を含む以降のバージョンでは、最大 64 の MAC アドレスを登録できます。

例

VLAN 1 で MAC アドレス 00bb-ccdd-eeff、0022-3344-5566 を許可するように設定します。

<AC> system-view

[AC] user-isolation vlan 1 permit-mac 00bb-ccdd-eeff 0022-3344-5566

関連コマンド

- **display user-isolation statistics**
- **user-isolation vlan enable**

目次

このセクションのページは **9-x-x** です。

13 章 TCP フラグメントアタックプロテクション 13-1
13.1 アタック検出およびアタック防止設定コマンド 13-1
13.1.1 attack-defense tcp fragment enable 13-1

13章 TCP フラグメントアタックプロテクション

13.1 アタック検出およびアタック防止設定コマンド

13.1.1 attack-defense tcp fragment enable

Syntax

attack-defense tcp fragment enable

undo attack-defense tcp fragment enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

attack-defense tcp fragment enable コマンドは TCP フラグメントアタックプロテクションを有効にします。

undo attack-defense tcp fragment enable コマンドは TCP フラグメントアタックプロテクションを無効にします。

このコマンドは TCP フラグメント攻撃を防ぐために、パケットフィルタ機能で検出できない TCP フラグメント攻撃のパケットを廃棄します。RFC1858 で定義されています。TCP フラグメントアタックプロテクションは以下の TCP フラグメントを調査します。

- TCP ヘッダが 20 バイトよりも小さい、最初のフラグメント
- 8 バイトのフラグメントオフセット（FO=1）の 2 番目以降のフラグメント

TCP フラグメントアタック防止は、シングルパケットアタック防止よりも優先されます。両方使用する場合、受信した TCP パケットは、最初に TCP フラグメントアタック防止に処理され、次にシングルパケットアタック守備ポリシーに処理されます。

例

TCP フラグメントアタックプロテクションを有効にします。

<AC> system-view

[AC] attack-defense tcp fragment enable

目次

このセクションのページは **9-x-x** です。

14 章 ユーザプロファイル 14-1
14.1 ユーザプロファイル設定コマンド 14-1
14.1.1 display user-profile 14-1
14.1.2 user-profile 14-3

14章 ユーザプロファイル

14.1 ユーザプロファイル設定コマンド

14.1.1 display user-profile

Syntax

display user-profile [name *profile-name* **] [slot** *slot-number* **]**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *profile-name*: ユーザプロファイル名を指定します。設定範囲は 1 から 31 文字です。大文字と小文字を区別します。英字、数字、アンダースコア (_) を使用可能です。名前は英字で始まり、一意である必要があります。このオプションを指定しない場合、すべてのユーザプロファイルの設定およびオンラインユーザ情報が表示されます。

slot *slot-number*: IRF スタックメンバ装置をメンバ ID で指定します。指定しない場合、このコマンドは、すべてのメンバ装置のユーザプロファイル設定およびオンラインユーザ情報を表示します。

説明

display user-profile コマンドはユーザプロファイルの設定およびオンラインユーザ情報を表示します。

例

#ユーザプロファイル aaa の設定とオンラインユーザ情報を表示します。

```
<AC> display user-profile aaa
    User-Profile: aaa
     Inbound:
       CIR 64 (kbps), CBS 512 (Bytes)
       Policy: p1
     Outbound:
```

```
  CIR 64 (kbps), CBS 512 (Bytes)

User user_1:
  Authentication type: 802.1X
  Network attributes:
    Interface      : GigabitEthernet1/0/1
    MAC address    : 0000-1111-2222
  Failed action list:
    Inbound: Policy p1
    Inbound: CIR 64 (kbps), CBS 2048 (Bytes)
```

表 14-1 コマンド出力

フィールド	説明
User-Profile	ユーザプロファイル名です。
Inbound	受信トラフィックに適用されるポリシーです。
Outbound	送信トラフィックに適用されるポリシーです。
CIR	適用されるCIRを表示します
CBS	適用されるCBSを表示します。
Policy	ポリシー名です。
User user_1	ユーザプロファイルが関連付けられているユーザアカウントのユーザ名です。
Authentication type	認証の種類です。 ・ 802.1X–802.1X認証です。 ・ Portal–ポータル認証です。 ・ PPP–PPP認証です。
Network attributes	オンラインユーザ情報です。
Failed action list	ユーザに適用できなかったアクションです。

14.1.2 user-profile

Syntax

user-profile *profile-name*

undo user-profile *profile-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

profile-name: ユーザプロファイル名を指定します。設定範囲は 1 から 31 文字です。大文字と小文字を区別します。英字、数字、アンダースコア (_) を使用でき、英字で始まる必要があります。名前は一意である必要があります。

説明

user-profile コマンドはユーザプロファイルを作成し、その view に移行するか、既存のユーザプロファイルの view に移行します。

undo user-profile コマンドはユーザプロファイルを削除します。

例

#ユーザプロファイル a123 を作成し、a123 の View に移行します。

<AC> system view

[AC] user-profile name a123

[AC-user-profile-a123]

QX-W2230AC アクセスコントローラ

コマンドマニュアル

10. 高可用性

本マニュアルは以下に示す章で構成されています。

01-Track

目次

このセクションのページは **10-x-x** です。

1 章 Track 1-1
1.1 Track 設定コマンド 1-1
1.1.1 display track 1-1
1.1.2 track interface 1-5
1.1.3 track interface protocol 1-6
1.1.4 track nqa 1-7

1章 Track

1.1 Track設定コマンド

1.1.1 display track

Syntax

display track { *track-entry-number* | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

all: すべての track エントリの情報を表示します。

説明

display track コマンドは track エントリの情報を表示します。

例

すべての track エントリの情報を表示します。

<AC> display track all

```
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 7 seconds
  Tracked object type: NQA
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object：
    NQA entry: admin test
    Reaction: 10
    Remote IP/URL: 2.2.2.2
    Local IP: 1.1.1.1
    Interface: GigabitEthernet1/0/1
  Tracked by:
    Track-list 6
```

```
    Track-list 7
Track ID: 2
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    Interface:  Vlan-interface3
    Protocol: IPv4
  Tracked by:
    Track-list 6
    Track-list 7
Track ID: 3
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: Percentage threshold list
  Notification delay: Positive 20, Negative 30 (in seconds)
  Threshold: Positive 40, Negative 30
  Percentage of positive objects: 50%
  Tracked objects:
    Object 1: Positive
    Object 3: Negative
Track ID: 4
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: Weight threshold list
  Notification delay: Positive 20, Negative 30 (in seconds)
  Threshold: Positive 50, Negative 30
  Positive weight/total weight: 50/80
  Tracked objects:
    Object 1: Positive, Weight: 50
Object 3: Negative, Weight: 30
Track ID: 5
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: Boolean and list
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked objects:
    Object 1: Positive
    Object 3: Negative(not)
    Object 10: NotReady(not)
```

表 1-1 コマンド出力

フィールド	説明
Track ID	trackエントリのIDです。
State	trackエントリの状態です。 • **Positive**—正常にtrackオブジェクトが動作しています。 • **NotReady**—trackオブジェクトが無効です。 • **Negative**—trackオブジェクトが異常です。
Duration	trackエントリが状態を保持する時間間隔です。
Type	trackのオブジェクトタイプです。 • Interface. • NQA. • List このフィールドは、**display track brief**コマンドが実行された場合にのみ表示されます。
Tracked object type	trackのオブジェクトタイプです。 • Interface. • NQA. • Boolean and list • Boolean or list • Percentage threshold list. • Weight threshold list.
Notification delay: Positive 20, Negative 30 (in seconds)	• trackモジュールは、trackエントリ状態が20秒の遅延時間後、Positiveに変更するとアプリケーションモジュールに通知します。 • trackモジュールは、trackエントリ状態が30秒の遅延時間後、Negativeに変更するとアプリケーションモジュールに通知します。
Threshold: Positive 40, Negative 30	ポジティブおよびネガティブ状態のしきい値です。 このフィールドは、trackのオブジェクトタイプが **Percentage threshold list** または **Weight threshold list** の場合にのみ表示されます。
Percentage of positive objects	trackリスト内のポジティブオブジェクトの割合です。 このフィールドは、trackのオブジェクトタイプが **Percentage threshold list** の場合にのみ表示されます。
Positive weight/total weight: 50/80	trackリスト内のすべてのオブジェクトの総Weightに対するポジティブオブジェクトの割合です。 このフィールドは、trackのオブジェクトタイプが **Weight threshold list** の場合にのみ表示されます。

フィールド	説明
Tracked object	trackエントリに関連づけられたtrackオブジェクトです。
NQA entry	trackエントリに関連づけられたNQAオペレーションです。
Reaction	trackエントリに関連づけられたリアクションエントリです。
IP route	trackエントリに関連づけられたルートです。
Remote IP/URL	リモートIPアドレスまたはURLです。リモートIPアドレスまたはURLが存在しない場合、2つの連続したハイフン（-）が表示されます。
Local IP	ローカルIPアドレスです。ローカルIPアドレスが存在しない場合、2つの連続するハイフン（-）が表示されます。
Interface	モニタ対象のインタフェースです。インタフェースをモニタしない場合は、2つの連続したハイフン（-）が表示されます。
Protocol	ルートのプロトコルタイプです。ルートが存在しないとき、**N/A**を表示します。
Nexthop interface	ルートのネクストホップです。ルートが存在しないとき、**N/A**を表示します。
Object 10 : Positive	trackのオブジェクトの状態です。 • Positive • NotReady • Negative trackのオブジェクトタイプが **Weight threshold list** の場合、オブジェクトのWeightも表示されます。 **（not）**属性が表示されている場合、trackリストはオブジェクトの状態をネガティブにします。
Tracked by	他のトラックエントリです。 オブジェクトタイプがtrackリストである場合、このフィールドは表示されません。

関連コマンド

- **track interface**
- **track interface protocol**
- **track nqa**

1.1.2 track interface

Syntax

track *track-entry-number* **interface** *interface-type interface-number*

undo track *track-entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

interface-type interface-number: インタフェースのタイプと番号を指定します。

説明

track interface コマンドを使用して、トラックエントリを作成し、インタフェースのリンク状態を監視し、トラックエントリビューを入力するか、既存のトラックエントリのビューを入力します。

undo track コマンドを使用して、トラックエントリとすべての設定をビューから削除します。

トラックエントリを作成するには、このコマンドの **interface** であるトラックオブジェクトタイプを指定する必要があります。

既存のトラックエントリのビューに入るには、**track** *track-entry-number* コマンドを使用します。トラックオブジェクトタイプは必須ではありません。

トラックエントリの設定を変更するには、**undo track** コマンドを実行してトラックエントリを削除し、**track interface** コマンドを再度実行します。

インタフェースのリンクステータスを監視するトラックエントリの場合、トラックエントリの状態は次のように変化します。

- インタフェースのリンク状態が up である場合、track エントリの状態は Positive です。
- インタフェースのリンク状態が down である場合、track エントリの状態は Negative です。

インタフェースのリンク状態を表示する場合、**display ip interface brief** コマンドを使用します。

例

トラックエントリ 1 を作成して、VLAN インタフェース 10 のリンク状態を監視し、track entry view に移行します。

<AC> system-view

[AC] track 1 interface vlan-interface 10

[AC-track-1]

関連コマンド

- **display track**
- **display ip interface brief (セクション 5 *IP サービス コマンドマニュアル*)**

1.1.3 track interface protocol

Syntax

track *track-entry-number* **interface** *interface-type interface-number* **protocol** { **ipv4** }

undo track *track-entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

interface-type interface-number: インタフェースのタイプと番号を指定します。

ipv4: IPv4 プロトコル状態をモニタします。インタフェースの IPv4 プロトコル状態が up である場合、track エントリの状態は Positive です。インタフェースの IPv4 プロトコル状態が down である場合、track エントリの状態は Negative です。インタフェースの IPv4 プロトコル状態を表示する場合、**display ip interface brief** コマンドを使用します。

説明

track interface protocol コマンドを使用して、トラックエントリを作成し、インタフェースのプロトコル状態を監視し、track entry view に移行するか、既存の track entry view に移行します。

undo track コマンドを使用して、トラックエントリとすべての設定をビューから削除します。

トラックエントリを作成するには、このコマンドの **interface protocol** であるトラックオブジェクトタイプを指定する必要があります。

既存のトラックエントリのビューに入るには、**track** *track-entry-number* コマンドを使用します。トラックオブジェクトタイプは必須ではありません。

トラックエントリの設定を変更するには、**undo track** コマンドを実行してトラックエントリを削除し、**track interface protocol** コマンドを再度実行します。

例

トラックエントリ 1 を作成して、VLAN インタフェース 2 の IPv4 プロトコル状態を監視し、track entry view に移行します。

<AC> system-view

[AC] track 1 interface vlan-interface 2 protocol ipv4

[AC-track-1]

関連コマンド

- **display track**
- **display ip interface brief (セクション 5 *IP サービス コマンドマニュアル*)**

1.1.4 track nqa

Syntax

track *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-number*

undo track *track-entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

entry *admin-name operation-tag*: track エントリに関連づけられる NQA オペレーションを指定します。*admin-name* は NQA オペレーションを作成する NQA オペレーションの管理者名です。設定範囲は 1～32 文字です。大文字、小文字を区別しません。*operation-*

tag は NQA オペレーションのタグです。設定範囲は 1～32 文字です。大文字、小文字を区別しません。

reaction *item-number*: track エントリに関連づけられるリアクションエントリを指定します。*item-number* はリアクションエントリの ID です。設定範囲は 1～10 です。

説明

track nqa コマンドを使用して、トラックエントリを作成し、NQA 操作のリアクションを監視し、track entry view に移行するか、既存の track entry view に移行します。

undo nqa コマンドを使用して、トラックエントリとすべての設定をビューから削除します。

トラックエントリを作成するには、このコマンドの **nqa** であるトラックオブジェクトタイプを指定する必要があります。

既存のトラックエントリのビューに入るには、**track** *track-entry-number* コマンドを使用します。トラックオブジェクトタイプは必須ではありません。

トラックエントリの設定を変更するには、**undo track** コマンドを実行してトラックエントリを削除し、**track nqa** コマンドを再度実行します。

例

トラックエントリ 1 を作成して、NQA テスト admin-test のリアクションエントリ 3 を監視し、track entry view に移行します。

<AC> system-view

[AC] track 1 nqa entry admin test reaction 3

[AC-track-1]

関連コマンド

display track

QX-W2230AC アクセスコントローラ

コマンドマニュアル

11. システム管理

本マニュアルは以下に示す章で構成されています。

01-システムの保守とデバッグ

02-NQA

03-NTP

04-SNMP

05-RMON

06-NETCONF

07-プロセスモニタリングとメンテナンス

08-パケットキャプチャ

09-Information Center

10-ポートミラーリング

11-NetMeister

目次

このセクションのページは **11-x-x** です。

1 章 システムの保守とデバッグ 1-1
1.1 システムの保守とデバッグ設定コマンド 1-1
1.1.1 debugging 1-1
1.1.2 display debugging 1-2
1.1.3 ping 1-2
1.1.4 tracert 1-6

1章 システムの保守とデバッグ

1.1 システムの保守とデバッグ設定コマンド

1.1.1 debugging

Syntax

debugging *module-name* [*option*]

undo debugging { all | *module-name* [*option*] }

デフォルト

無効

View

User view

定義済みユーザロール

network-admin

パラメータ

module-name: arp、device のようなモジュール名を指定します。現在のモジュール名を表示する場合、**debugging ?**コマンドを使用します。

option: モジュールのデバッグオプションを指定します。オプションの番号と内容はモジュールによって異なります。サポートされるオプションを表示する場合、**debugging** *module-name* **?**コマンドを使用します。

all: すべてのモジュールにデバッグを無効にします。

説明

debugging コマンドは指定したモジュールのデバッグを有効にします。

undo debugging コマンドは指定したモジュールあるいはすべてのモジュールのデバッグを無効にします。

デバッグ情報を出力すると、メモリの消費量が激しくなります。システムのパフォーマンスを保証するため、異常な状態のモジュールのみデバッグを有効にしてください。

システムは生成されたデバッグメッセージを Information Center に送信します。ログの出力設定にもとづいて適切な宛先に送信します。Information Center の詳細はオペレーションマニュアルのセクション 11 *システム管理 “Information Center”*を参照してください。

例

装置管理モジュールのデバッグを有効にします。

<AC> debugging dev

関連コマンド

display debugging

1.1.2 display debugging

Syntax

display debugging [*module-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

module-name: モジュール名を指定します。現在のモジュール名を表示する場合、**debugging ?**コマンドを使用します。

説明

display debugging コマンドは有効になっているデバッグを表示します。

例

有効になっているすべてのデバッグを表示します。

<AC> display debugging

```
DEV debugging switch is on
```

関連コマンド

debugging

1.1.3 ping

Syntax

ping [**ip**] [**-a** *source-ip* | **-c** *count* | **-f** | **-h** *ttl* | **-i** *interface-type interface-number* | **-m** *interval* | **-n** | **-p** *pad* | **-q** | **-r** | **-s** *packet-size* | **-t** *timeout* | **-tos** *tos* | **-v**] * *host*

View

すべての view

定義済みユーザロール

network-admin

パラメータ

ip: 宛先ホストの名前が **i**、**ip**、**ipv**、**ipv6**、**l**、**ls**、**lsp** であるとき、宛先ホスト名と **ping** コマンドのパラメータを区別します。たとえば、宛先ホスト名が ip である場合、**ping** *ip* の代わりに **ping ip** *ip* の形式を使用する必要があります。

-a *source-ip*: ICMP エコー要求の送信元 IP アドレスとして装置の IP アドレスを指定します。指定しない場合、ICMP エコー要求の送信元 IP アドレスは送信インタフェースのプライマリ IP アドレスです。

-c *count*: 宛先に送信する ICMP エコー要求の数を指定します。設定範囲は 1～4294967295 です。デフォルトは 5 です。

-f: IP ヘッダの DF ビットを設定します。

-h *ttl*: ICMP エコー要求の TTL を指定します。設定範囲は 1～255 です。デフォルトは 255 です。

-i *interface-type interface-number*: ICMP エコー要求の送信元インタフェースを指定します。指定しない場合、ICMP エコー要求の送信元インタフェースとしてルートの出力インタフェースに一致するプライマリ IP アドレスを使用します。

-m *interval*: ICMP エコー要求を送信する間隔を指定します。設定範囲は 1～65535 ミリ秒です。デフォルトは 200 ミリ秒です。

-n: *host* のドメイン名解決を無効にします。*host* は宛先のホスト名を示します。指定しない場合、装置はホストをアドレスに変換します。

-p *pad*: ICMP エコー要求のパディングフィールドの値を指定します。設定範囲は 16 進数、1～8 ビットで 0～ffffffff です。指定した値が 8 ビット未満の場合、上位ビットに 0 が追加され 8 ビットに拡張されます。たとえば、*pad* が 0x2f に設定されている場合、装置が要求するパケット長にするために、パケットは 0x0000002f のパディングフィールドで埋められます。パディングの値のデフォルトは 0x01 で始まり 0xff までです。必要があれば、再度繰り返します。たとえば 0x010203…feff01….です。

-q: 統計情報の概要を表示します。指定しない場合、ping のすべての統計情報を表示します。

-r: パスの ICMP エコー要求の Hop アドレス（9 まで）を記録します。指定しない場合、パスの ICMP エコー要求の Hop アドレス（9 まで）を記録しません。

-s *packet-size*: IP パケットヘッダと ICMP パケットヘッダを除く ICMP エコー要求の長さを指定します。設定範囲は 20～8100 バイトです。デフォルトは 56 バイトです。

-t *timeout*: ICMP エコー応答のタイムアウト時間を指定します。設定範囲は 0～65535 ミリ秒です。デフォルトは 2000 ミリ秒です。タイムアウト時間内に送信元が ICMP エコー応答を受信しない場合、ICMP エコー応答がタイムアウトしたと認識します。

-tos *tos*: ICMP エコー要求の ToS を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

-v: ICMP 以外のエコー応答を表示します。指定しない場合、システムは ICMP 以外のエコー応答を表示しません。

host: 宛先の IP アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1～253 文字です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含むことができます。

説明

ping コマンドは IP ネットワーク内の宛先装置が到達可能かどうかを検証し、関連する統計情報を表示します。

ping コマンドで宛先ホストの名前を使用する場合、装置の DNS の設定を行う必要があります。そうでなければ **ping** コマンドは失敗します。

ping コマンドを実行中、**Ctrl+C** を押下することで中止することができます。

例

IP アドレス 1.1.2.2 の装置が到達可能かどうかを検証します。

<AC> ping 1.1.2.2

```
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=2.137 ms
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=1.996 ms
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=1.991 ms

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms
```

IP アドレス 1.1.2.2 の装置が到達可能かどうかを検証します。統計情報のみを表示します。

<AC> ping -q 1.1.2.2

```
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.962/2.196/2.665/0.244 ms
```

IP アドレス 1.1.2.2 の装置が到達可能かどうかを検証します。パスの ICMP パケットが通過する Hop アドレスを表示します。

<AC> ping -r 1.1.2.2

```
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=4.685 ms
RR:     1.1.2.1
```

```
        1.1.2.2
        1.1.1.2
        1.1.1.1
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=4.834 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=4.770 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=4.812 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=4.704 ms  (same route)

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.685/4.761/4.834/0.058 ms
```

出力は以下のことを示します。

- 宛先装置へ到達可能です。
- ルートは 1.1.1.1 <-> {1.1.1.2; 1.1.2.1} <-> 1.1.2.2 です。

表 1-1 コマンド出力

フィールド	説明
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break	IPアドレス1.1.2.2の装置に到達可能かどうかを検証します。各ICMPエコー要求のパケット長は56バイトです。pingを中止する場合、**Ctrl+C**を押下します。
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=4.685 ms	IPアドレス1.1.2.2の装置からICMPエコー応答を受信しました。タイムアウト時間内にエコー応答がない場合、表示されません。 • **bytes**—ICMPエコー応答のバイト数です。 • **icmp_seq**—セグメントが紛失、順番が異常、繰り返ししているかどうかを確認するために使用されるパケットシーケンスです。 • **ttl**—ICMPエコー応答のTTLです。 • **time**—応答時間です。
RR:	ICMPエコー要求を通過したルータです。遠いところから順番に表示されます。宛先にもっとも近いルータが最初に表示されます。
--- Ping statistics for 1.1.2.2 ---	pingで送受信した統計情報です。
5 packet(s) transmitted	送信したICMPエコー要求の数です。
5 packet(s) received	受信したICMPエコー要求の数です。
0.0% packet loss	送信したパケットに対して応答がないパケットの割合です。
round-trip min/avg/max/std-dev = 4.685/4.761/4.834/0.058 ms	最小/平均/最大/標準の応答時間です。単位はミリ秒です。

1.1.4 tracert

Syntax

tracert [**-a** *source-ip* | **-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-t** *tos* | **-w** *timeout*] * *host*

View

すべての view

定義済みユーザロール

network-admin

パラメータ

-a *source-ip*: プローブパケットの送信元 IP アドレスとして装置の IP アドレスを指定します。指定しない場合、プローブパケットの送信元 IP アドレスは送信インタフェースのプライマリ IP アドレスです。

-f *first-ttl*: 宛先に送信された最初のパケットの TTL を指定します。設定範囲は 1～255 です。デフォルトは 1 です。この値は *max-ttl* 以下の値でなければなりません。

-m *max-ttl*: プローブパケットで許可される最大 Hop 数を指定します。設定範囲は 1～255 です。デフォルトは 30 です。この値は *first-ttl* 以上の値でなければなりません。

-p *port*: 宛先の無効の UDP ポートを指定します。設定範囲は 1～65535 です。デフォルトは 33434 です。宛先アドレスがリモート LISP サイトで EID アドレスの場合、ポート番号を指定してください。設定範囲は 33434～65535 です。

-q *packet-number*: ホップごとに送信されるプローブパケット数を指定します。設定範囲は 1～65535 です。デフォルトは 3 です。

-t *tos*: プローブパケットの ToS を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

-w *timeout*: プローブパケットの応答パケットのタイムアウト時間を指定します。設定範囲は 1～65535 ミリ秒です。デフォルトは 5000 ミリ秒です。

host: 宛先の IP アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1～253 文字です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含むことができます。

説明

tracert コマンドはパケットが送信元から宛先に向かう間に通過するルートを追跡します。

ping コマンドでネットワークの故障を識別したのち、**tracert** コマンドで故障したノードの位置を見つけることができます。

tracert コマンドの出力情報には、パケットが送信元から宛先に向かう間に通過するすべてのルートの IP アドレスが含まれます。ICMP エラーメッセージで装置が応答しない場

合、アスタリスク（*.*.*）が表示されます。（宛先が到達不能あるいは ICMP タイムアウト/宛先到達不能パケットの送信が無効であることを示します。）

tracert コマンドを実行中、**Ctrl+C** を押下することで中止することができます。

例

パケットが送信元から宛先（IP アドレス 1.1.2.2）へ向かうルートを表示します。

<AC> tracert 1.1.2.2

```
traceroute to 1.1.2.2 (1.1.2.2), 30 hops at most, 40 bytes each packet, press
CTRL_C to break
 1  1.1.1.2 (1.1.1.2) 673 ms 425 ms 30 ms
 2  1.1.2.2 (1.1.2.2) 580 ms 470 ms 80 ms
```

表 1-2 コマンド出力

フィールド	説明
traceroute to 1.1.2.2 (1.1.2.2)	現在の装置からIPアドレスが1.1.2.2の装置へ向かうIPパケットのルートを表示します。
hops at most	プローブパケットの最大Hop数です。このフィールドを表示する場合、**-m**を指定する必要があります。
bytes each packet	プローブパケットのバイト数です。
press CTRL_C to break	**tracert**コマンドを実行中、中止する場合、**Ctrl+C**を押下します。
2　1.1.2.2 (1.1.2.2) 580 ms 470 ms 80 ms	TTLが2のプローブパケットの結果です。2番目のホップは以下の情報が含まれます。 ● 最初のHopのドメイン名です。ドメイン名が設定されていない場合、IPアドレスが表示されます。 ● ホップのIPアドレスです。IPアドレスは括弧で表示されます。 ● プローブパケットのラウンドトリップ時間です。 各プローブが送信したパケット数を表示する場合、**-q**を指定する必要があります。
1　1.1.1.2 (1.1.1.2) 673 ms 425 ms 30 ms	TTLが1のプローブパケットの結果です。1番目のホップは以下の情報が含まれます。 ● 最初のHopのドメイン名です。ドメイン名が設定されていない場合、IPアドレスが表示されます。 ● ホップのIPアドレスです。IPアドレスは括弧で表示されます。 ● プローブパケットのラウンドトリップ時間です。 各プローブが送信したパケット数を表示する場合、**-q**を指定する必要があります。

目次

このセクションのページは **11-x-x** です。

2 章 NQA 2-1
2.1 NQA クライアント設定コマンド 2-1
2.1.1 advantage-factor 2-1
2.1.2 codec-type 2-2
2.1.3 data-fill 2-2
2.1.4 data-size 2-4
2.1.5 description (すべての NQA operation type view) 2-5
2.1.6 destination ip 2-6
2.1.7 destination port 2-6
2.1.8 display nqa history 2-7
2.1.9 display nqa result 2-9
2.1.10 display nqa statistics 2-13
2.1.11 filename 2-19
2.1.12 frequency 2-20
2.1.13 history-record enable 2-21
2.1.14 history-record keep-time 2-22
2.1.15 history-record number 2-22
2.1.16 next-hop ip 2-23
2.1.17 nqa 2-24
2.1.18 nqa agent enable 2-25
2.1.19 nqa schedule 2-26
2.1.20 operation (FTP operation view) 2-27
2.1.21 operation (HTTP operation view) 2-28
2.1.22 password 2-29
2.1.23 probe count 2-30
2.1.24 probe packet-interval 2-31
2.1.25 probe packet-number 2-32
2.1.26 probe packet-timeout 2-33
2.1.27 probe timeout 2-33
2.1.28 reaction checked-element probe-fail (for trap) 2-34
2.1.29 reaction trap 2-36
2.1.30 resolve-target 2-37
2.1.31 route-option bypass-route 2-38
2.1.32 source interface 2-39
2.1.33 source ip 2-40
2.1.34 source port 2-41

2.1.35 statistics interval 2-42
2.1.36 statistics max-group 2-42
2.1.37 tos 2-43
2.1.38 ttl 2-44
2.1.39 type 2-45
2.1.40 url 2-46
2.1.41 username 2-47
2.1.42 version 2-48
2.2 NQA サーバ設定コマンド 2-49
2.2.1 display nqa server 2-49
2.2.2 nqa server enable 2-50
2.2.3 nqa server tcp-connect 2-51
2.2.4 nqa server udp-echo 2-52

2章 NQA

2.1 NQAクライアント設定コマンド

2.1.1 advantage-factor

Syntax

advantage-factor *factor*

undo advantage-factor

デフォルト

0

View

Voice operation view

定義済みユーザロール

network-admin

パラメータ

factor: アドバンテージファクタを指定します。設定範囲は 0～20 です。

説明

advantage-factor コマンドは MOS（Mean Opinion Scores）値と ICPIF（Calculated Planning Impairment Factor）値をカウントするのに使用されるアドバンテージファクタを設定します。

undo advantage-factor コマンドはデフォルトに戻します。

音声品質の評価は、ユーザの音声品質の許容度に依存します。音声品質に高い許容度を持つユーザの場合、アドバンテージファクタの設定を行う **advantage-factor** コマンドを使用します。システムが ICPIF 値を計算する場合、音声品質の評価用に ICPIF と MOS の値を修正するため、アドバンテージファクタが取りはずされます。

例

音声テストのアドバンテージファクタを 10 に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type voice

[AC-nqa-admin-test-voice] advantage-factor 10

2.1.2 codec-type

Syntax

codec-type { **g711a** | **g711u** | **g729a** }

undo codec-type

デフォルト

G.711 A-law

View

Voice operation view

定義済みユーザロール

network-admin

パラメータ

g711a: G.711 A-law コーデックタイプを指定します。

g711u: G.711 μ-law コーデックタイプを指定します。

g729a: G.729 A-law コーデックタイプを指定します。

説明

codec-type コマンドは音声テストのコーデックタイプを設定します。

undo codec-type コマンドはデフォルトに戻します。

例

音声テストのコーデックタイプを g729a に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type voice

[AC-nqa-admin-test-voice] codec-type g729a

2.1.3 data-fill

Syntax

data-fill *string*

undo data-fill

デフォルト

00010203040506070809

View

ICMP/UDP echo operation view

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

string: 文字列を指定します。設定範囲は 1～200 文字です。大文字、小文字を区別します。

説明

data-fill コマンドは各プローブパケットのペイロードに埋め込まれる文字列を設定します。

undo data-fill コマンドはデフォルトに戻します。

ペイロード長が埋め込みデータより小さい場合、文字列の最初の部分を使用します。たとえば、埋め込みデータが **abcd** で、テストパケットのデータサイズが 3 バイトの場合、**abc** がパケットに埋め込まれます。

ペイロード長が埋め込みデータより大きい場合、一杯になるまで文字列を繰り返し埋め込みます。たとえば、埋め込みデータが **abcd** で、テストパケットのデータサイズが 6 バイトの場合、**abcdab** がパケットに埋め込まれます。

テストタイプに依存して文字列が埋め込まれます。

- ICMP エコーテストでは、設定された文字列は ICMP エコー要求の全ペイロードに埋め込まれます。
- UDP エコーテストでは、UDP パケットのペイロードの最初の 5 バイトは特定の用途に使用されます。設定された文字列はペイロードの残りの部分を埋め込むのに使用されます。
- UDP ジッタテストでは、UDP パケットのペイロードの最初の 68 バイトは特定の用途に使用されます。設定された文字列はペイロードの残りの部分を埋め込むのに使用されます。

例

ICMP エコー要求のペイロードに埋め込まれる文字列 **abcd** を設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] data-fill abcd

2.1.4 data-size

Syntax

data-size *size*

undo data-size

デフォルト

異なるテストのプローブパケットのデフォルトのペイロードサイズを表 2-1 に示します。

表 2-1 プローブパケットのデフォルトのペイロードサイズ

テストタイプ	コーデックタイプ	デフォルトサイズ（バイト）
ICMP echo	—	100
UDP echo	—	100
UDP jitter	—	100

View

ICMP/UDP echo operation view

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

size: 各プローブパケットのペイロードサイズを指定します。以下に設定範囲を示します。

- ICMP エコーあるいは UDP エコーテストのプローブパケットの設定範囲は 20～65507 バイトです。
- UDP ジッタテストのプローブパケットの設定範囲は 68～65507 バイトです。

説明

data-size コマンドは各プローブパケットのペイロードサイズを設定します。

undo data-size コマンドはデフォルトに戻します。

ICMP エコーテストではコマンドは各エコー要求のペイロードサイズを設定します。

UDP エコーテスト、UDP ジッタテストではコマンドは各エコーUDP パケットのペイロードサイズを設定します。

例

各 ICMP エコー要求のペイロードサイズを 80 バイトに設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] data-size 80

2.1.5 description (すべての NQA operation type view)

Syntax

description *text*

undo description

デフォルト

設定なし

View

すべての NQA operation type view

定義済みユーザロール

network-admin

パラメータ

text: 文字列を指定します。設定範囲は 1～200 文字です。大文字、小文字を区別します。

説明

description コマンドはテストタイプや目的などの NQA テストの説明を設定します。

undo description コマンドは説明を削除します。

例

NQA テストの説明を **icmp-probe** に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] description icmp-probe

2.1.6 destination ip

Syntax

destination ip *ip-address*

undo destination ip

デフォルト

設定なし

View

SNMP/TCP operation view

ICMP/UDP echo operation view

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

ip-address: テストの宛先 IPv4 アドレスを指定します。

説明

destination ip コマンドはテストの宛先 IPv4 アドレスを設定します。

undo destination ip コマンドは宛先 IPv4 アドレスを削除します。

例

ICMP エコーテストの宛先 IPv4 アドレスを 10.1.1.1 に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] destination ip 10.1.1.1

2.1.7 destination port

Syntax

destination port *port-number*

undo destination port

デフォルト

設定なし

View

TCP operation view

UDP echo operation view

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

port-number: テストの宛先ポート番号を指定します。設定範囲は 1～65535 です。

説明

destination port コマンドはテストの宛先ポート番号を設定します。

undo destination port コマンドは宛先ポート番号を削除します。

例

UDP エコーテストの宛先ポート番号を 9000 に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type udp-echo

[AC-nqa-admin-test-udp-echo] destination port 9000

2.1.8 display nqa history

Syntax

display nqa history [*admin-name operation-tag*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はテストタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小

文字を区別しません。ハイフン（-）を使用することができません。NQA テストを指定しない場合、すべての NQA テストの履歴記録を表示します。

説明

display nqa history コマンドは NQA テストの履歴記録を表示します。

display nqa history コマンドは UDP ジッタテストの結果あるいは統計情報を表示しません。UDP ジッタテストを確認する場合、**display nqa result** コマンドあるいは **display nqa statistics** コマンドを使用します。

例

管理者名が **administrator**、テストタグが **test** の NQA テストグループの履歴記録を表示します。

<AC> display nqa history administrator test

```
NQA entry (admin administrator, tag test) history records:
Index      TTL  Response  Hop IP         Status         Time
  10        329         Succeeded       2011-04-29 20:54:26.5
  9         344         Succeeded       2011-04-29 20:54:26.2
  8         328         Succeeded       2011-04-29 20:54:25.8
  7         328         Succeeded       2011-04-29 20:54:25.5
  6         328         Succeeded       2011-04-29 20:54:25.1
  5         328         Succeeded       2011-04-29 20:54:24.8
  4         328         Succeeded       2011-04-29 20:54:24.5
  3         328         Succeeded       2011-04-29 20:54:24.1
  2         328         Succeeded       2011-04-29 20:54:23.8
  1         328         Succeeded       2011-04-29 20:54:23.4
```

表 2-2 コマンド出力

フィールド	説明
Index	履歴記録のID
TTL	プローブパケットのTTL
Response	テストが成功した場合、ラウンドトリップの時間を表示します。テストがタイムアウトしたとき、タイムアウト時間を表示します。テストが完了しない場合、**0**を表示します。単位はミリ秒です。
Hop IP	応答パケットを送信したノードのIPアドレス

フィールド	説明
Status	テスト結果の状態 • **Succeeded**－成功しました。 • **Unknown error**－未知のエラーです。 • **Internal error**－内部エラーです。 • **Timeout**－タイムアウトしました。
Time	テストが完了したときの時間

2.1.9 display nqa result

Syntax

display nqa result [*admin-name operation-tag*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はテストタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。NQA テストを指定しない場合、すべての NQA テストの最新の結果を表示します。

説明

display nqa result コマンドは、NQA テストの最新の結果を表示します。

例

TCP テストの最新の結果を表示します。

<AC> display nqa result admin test

```
NQA entry (admin admin, tag test) test results:
   Send operation times: 1            Receive response times: 1
   Min/Max/Average round trip time: 35/35/35
   Square-Sum of round trip time: 1225
   Last succeeded probe time: 2011-05-29 10:50:33.2
  Extended results:
```

```
  Packet loss ratio: 0%
  Failures due to timeout: 0
  Failures due to disconnect: 0
  Failures due to no connection: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
```

UDP ジッタテストの最新の結果を表示します。

<AC> display nqa result admin test

```
NQA entry (admin admin, tag test) test results:
   Send operation times: 10          Receive response times: 10
   Min/Max/Average round trip time: 15/46/26
   Square-Sum of round trip time: 8103
   Last packet received time: 2011-05-29 10:56:38.7
 Extended results:
   Packet loss ratio: 0%
   Failures due to timeout: 0
   Failures due to internal error: 0
   Failures due to other errors: 0
   Packets out of sequence: 0
   Packets arrived late: 0
 UDP-jitter results:
  RTT number: 10
   Min positive SD: 8                Min positive DS: 8
   Max positive SD: 18               Max positive DS: 8
   Positive SD number: 5             Positive DS number: 2
   Positive SD sum: 75               Positive DS sum: 32
   Positive SD average: 15           Positive DS average: 16
   Positive SD square-sum: 1189      Positive DS square-sum: 640
   Min negative SD: 8                Min negative DS: 1
   Max negative SD: 24               Max negative DS: 30
   Negative SD number: 4             Negative DS number: 7
   Negative SD sum: 56               Negative DS sum: 99
   Negative SD average: 14           Negative DS average: 14
   Negative SD square-sum: 946       Negative DS square-sum: 1495
 One way results:
   Max SD delay: 22                  Max DS delay: 23
   Min SD delay: 7                   Min DS delay: 7
   Number of SD delay: 10            Number of DS delay: 10
   Sum of SD delay: 125              Sum of DS delay: 132
   Square-Sum of SD delay: 1805      Square-Sum of DS delay: 1988
   SD lost packets: 0                DS lost packets: 0
   Lost packets for unknown reason: 0
```

表 2-3 コマンド出力

フィールド	説明
Send operation times	テスト数
Receive response times	受信した応答パケット数
Min/Max/Average round trip time	最小/最大/平均ラウンドトリップタイム 単位はミリ秒です。
Square-Sum of round trip time	ラウンドトリップタイムの2乗和
Last succeeded probe time	連続した最後のプローブが完了した時間 テストでプローブが連続していない場合、0と表示されます。 本フィールドはUDPジッタテストでは無効です。
Last packet received time	連続した最後の応答パケットを受信した時間 プローブで応答パケットを受信しない場合、0と表示されます。 本フィールドはUDPジッタテストでのみ有効です。
Packet loss ratio	平均パケット損失レート
Failures due to timeout	テストでタイムアウトが発生した回数
Failures due to disconnect	ピアが切断した数
Failures due to no connection	ピアとの接続に失敗した数
Failures due to internal error	内部エラーに起因する失敗の数
Failures due to other errors	他のエラーに起因する失敗の数
Packets out of sequence	パケット順序入れ替わりに起因する失敗の数
Packets arrived late	プローブのタイムアウト後に受信した応答パケットの数
UDP-jitter results	UDPジッタテストの結果 本フィールドはUDPジッタテストでのみ有効です。
RTT number	応答パケットを受信した数
Min positive SD	送信元から宛先への最小ポジティブジッタ
Min positive DS	宛先から送信元への最小ポジティブジッタ
Max positive SD	送信元から宛先への最大ポジティブジッタ
Max positive DS	宛先から送信元への最大ポジティブジッタ

フィールド	説明
Positive SD number	送信元から宛先へのポジティブジッタの数
Positive DS number	宛先から送信元へのポジティブジッタの数
Positive SD sum	送信元から宛先へのポジティブジッタの合計
Positive DS sum	宛先から送信元へのポジティブジッタの合計
Positive SD average	送信元から宛先への平均ポジティブジッタ
Positive DS average	宛先から送信元への平均ポジティブジッタ
Positive SD square-sum	送信元から宛先へのポジティブジッタの2乗和
Positive DS square-sum	宛先から送信元へのポジティブジッタの2乗和
Min negative SD	送信元から宛先へのネガティブジッタの絶対値の最小値
Min negative DS	宛先から送信元へのネガティブジッタの絶対値の最小値
Max negative SD	送信元から宛先へのネガティブジッタの絶対値の最大値
Max negative DS	宛先から送信元へのネガティブジッタの絶対値の最大値
Negative SD number	送信元から宛先へのネガティブジッタの数
Negative DS number	宛先から送信元へのネガティブジッタの数
Negative SD sum	送信元から宛先へのネガティブジッタの絶対値の合計
Negative DS sum	宛先から送信元へのネガティブジッタの絶対値の合計
Negative SD average	送信元から宛先へのネガティブジッタの絶対値の平均
Negative DS average	宛先から送信元へのネガティブジッタの絶対値の平均
Negative SD square-sum	送信元から宛先へのネガティブジッタの2乗和
Negative DS square-sum	宛先から送信元へのネガティブジッタの2乗和
One way results	片方向遅延 本フィールドはUDPジッタテストでのみ有効です。
Max SD delay	送信元から宛先への最大遅延
Max DS delay	宛先から送信元への最大遅延
Min SD delay	送信元から宛先への最小遅延

フィールド	説明
Min DS delay	宛先から送信元への最小遅延
Number of SD delay	送信元から宛先への遅延の数
Number of DS delay	宛先から送信元への遅延の数
Sum of SD delay	送信元から宛先への遅延の合計
Sum of DS delay	宛先から送信元への遅延の合計
Square-Sum of SD delay	送信元から宛先への遅延の2乗和
Square-Sum of DS delay	宛先から送信元への遅延の2乗和
SD lost packets	送信元から宛先への損失したパケット数
DS lost packets	宛先から送信元への損失したパケット数
Lost packets for unknown reason	不明な理由で損失したパケット数

2.1.10 display nqa statistics

Syntax

display nqa statistics [*admin-name operation-tag*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はテストタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。NQA テストを指定しない場合、すべての NQA テストの統計情報を表示します。

説明

display nqa statistics コマンドは NQA テストの統計情報を表示します。

NQA テストが完了した後、統計情報が作成されます。テストが完了する前に **display nqa statistics** コマンドを実行した場合、統計情報はすべて 0 で表示されます。

リアクションエントリが設定されている場合、**statistics interval** コマンドで指定された期間、リアクションエントリをモニタリングした結果を表示します。

例

TCP テストの統計情報を表示します。

<AC> display nqa statistics admin test

```
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
    Start time: 2007-01-01 09:30:20.0
    Life time: 2 seconds
    Send operation times: 1            Receive response times: 1
    Min/Max/Average round trip time: 13/13/13
    Square-Sum of round trip time: 169
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

UDP ジッタテストの統計情報を表示します。

<AC> display nqa statistics admin test

```
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
    Start time: 2007-01-01 09:33:22.3
    Life time: 23 seconds
    Send operation times: 100          Receive response times: 100
    Min/Max/Average round trip time: 1/11/5
    Square-Sum of round trip time: 24360
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  UDP-jitter results:
   RTT number: 550
    Min positive SD: 1                 Min positive DS: 1
    Max positive SD: 7                 Max positive DS: 1
```

```
  Positive SD number: 220             Positive DS number: 97
  Positive SD sum: 283                Positive DS sum: 287
  Positive SD average: 1              Positive DS average: 2
  Positive SD square-sum: 709          Positive DS square-sum: 1937
  Min negative SD: 2                  Min negative DS: 1
  Max negative SD: 10                 Max negative DS: 1
  Negative SD number: 81              Negative DS number: 94
  Negative SD sum: 556                Negative DS sum: 191
  Negative SD average: 6              Negative DS average: 2
  Negative SD square-sum: 4292         Negative DS square-sum: 967
One way results:
  Max SD delay: 5                    Max DS delay: 5
  Min SD delay: 1                    Min DS delay: 1
  Number of SD delay: 550             Number of DS delay: 550
  Sum of SD delay: 1475               Sum of DS delay: 1201
  Square-Sum of SD delay: 5407         Square-Sum of DS delay: 3959
  SD lost packets: 0                 DS lost packets: 0
  Lost packets for unknown reason: 0
Reaction statistics:
  Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
  1      jitter-DS       accumulate      90           25
  2      jitter-SD       average         -            -
  3      OWD-DS          -               100          24
  4      OWD-SD          -               100          13
  5      packet-loss     accumulate      0            0
  6      RTT             accumulate      100          52
```

表 2-4 コマンド出力

フィールド	説明
No.	統計情報のグループID
Start time	テスト開始時間
Life time	テスト所要時間
Send operation times	プローブパケット送信数
Receive response times	受信した応答パケット数
Min/Max/Average round trip time	最小/最大/平均ラウンドトリップタイム 単位はミリ秒です。
Square-Sum of round trip time	ラウンドトリップタイムの2乗和
Packet loss ratio	平均パケット損失レート

フィールド	説明
Failures due to timeout	テストでタイムアウトが発生した回数
Failures due to disconnect	ピアが切断した数
Failures due to no connection	ピアとの接続に失敗した数
Failures due to internal error	内部エラーに起因する失敗の数
Failures due to other errors	他のエラーに起因する失敗の数
Packets out of sequence	パケット順序入れ替わりに起因する失敗の数
Packets arrived late	プローブのタイムアウト後に受信した応答パケットの数
UDP-jitter results	UDPジッタテストの結果 本フィールドはUDPジッタテストでのみ有効です。
RTT number	応答パケットを受信した数
Min positive SD	送信元から宛先への最小ポジティブジッタ
Min positive DS	宛先から送信元への最小ポジティブジッタ
Max positive SD	送信元から宛先への最大ポジティブジッタ
Max positive DS	宛先から送信元への最大ポジティブジッタ
Positive SD number	送信元から宛先へのポジティブジッタの数
Positive DS number	宛先から送信元へのポジティブジッタの数
Positive SD sum	送信元から宛先へのポジティブジッタの合計
Positive DS sum	宛先から送信元へのポジティブジッタの合計
Positive SD average	送信元から宛先への平均ポジティブジッタ
Positive DS average	宛先から送信元への平均ポジティブジッタ
Positive SD square-sum	送信元から宛先へのポジティブジッタの2乗和
Positive DS square-sum	宛先から送信元へのポジティブジッタの2乗和
Min negative SD	送信元から宛先へのネガティブジッタの絶対値の最小値
Min negative DS	宛先から送信元へのネガティブジッタの絶対値の最小値
Max negative SD	送信元から宛先へのネガティブジッタの絶対値の最大値

フィールド	説明
Max negative DS	宛先から送信元へのネガティブジッタの絶対値の最大値
Negative SD number	送信元から宛先へのネガティブジッタの数
Negative DS number	宛先から送信元へのネガティブジッタの数
Negative SD sum	送信元から宛先へのネガティブジッタの絶対値の合計
Negative DS sum	宛先から送信元へのネガティブジッタの絶対値の合計
Negative SD average	送信元から宛先へのネガティブジッタの絶対値の平均
Negative DS average	宛先から送信元へのネガティブジッタの絶対値の平均
Negative SD square-sum	送信元から宛先へのネガティブジッタの2乗和
Negative DS square-sum	宛先から送信元へのネガティブジッタの2乗和
One way results	片方向遅延 本フィールドはUDPジッタテストでのみ有効です。
Max SD delay	送信元から宛先への最大遅延
Max DS delay	宛先から送信元への最大遅延
Min SD delay	送信元から宛先への最小遅延
Min DS delay	宛先から送信元への最小遅延
Number of SD delay	送信元から宛先への遅延の数
Number of DS delay	宛先から送信元への遅延の数
Sum of SD delay	送信元から宛先への遅延の合計
Sum of DS delay	宛先から送信元への遅延の合計
Square-Sum of SD delay	送信元から宛先への遅延の2乗和
Square-Sum of DS delay	宛先から送信元への遅延の2乗和
SD lost packets	送信元から宛先への損失したパケット数
DS lost packets	宛先から送信元への損失したパケット数
Lost packets for unknown reason	不明な理由で損失したパケット数

フィールド	説明
Reaction statistics	カウント期間中のリアクションエントリに関する統計情報
Index	リアクションエントリのID
Checked Element	モニタリングされる要素
Threshold Type	しきい値タイプ
Checked Num	データ収集用にモニタリングされているターゲットの数
Over-threshold Num	しきい値違反の数

表 2-5 しきい値モニタリングフィールドの説明

モニタリングされる性能メトリック	しきい値タイプ	収集データ	モニタリングされているターゲット数	しきい値違反数
probe-duration	accumulate	カウント期間のプローブ	完了したプローブ数	カウント期間中にしきい値を超過したプローブ数
	average	ー	ー	ー
	consecutive	カウント期間のプローブ	完了したプローブ数	カウント期間中にしきい値を超過したプローブ数
probe-fail	accumulate	カウント期間のプローブ	完了したプローブ数	プローブ失敗数
	consecutive	カウント期間のプローブ	完了したプローブ数	プローブ失敗数
RTT	accumulate	カウント期間のプローブ	送信したパケット数	ラウンドトリップタイムがしきい値を超過したパケット数
	average	ー	ー	ー
jitter-DS/jitter-SD	accumulate	カウント期間のプローブ	送信したパケット数	一方向ジッタがしきい値を超過したパケット数
	average	ー	ー	ー

モニタリングされる性能メトリック	しきい値タイプ	収集データ	モニタリングされているターゲット数	しきい値違反数
OWD-DS/OWD-SD	―	カウント期間のプローブ	送信したパケット数	一方向ジッタがしきい値を超過したパケット数
packet-loss	accumulate	カウント期間のプローブ	送信したパケット数	パケットロス数
ICPIF	―	―	―	―
MOS	―	―	―	―

関連コマンド

statistics interval

2.1.11 filename

Syntax

filename *filename*

undo filename

デフォルト

設定なし

View

FTP operation view

定義済みユーザロール

network-admin

パラメータ

filename: FTP サーバと FTP クライアント間で転送するファイル名を指定します。設定範囲は 1～200 文字です。大文字、小文字を区別します。スラッシュ（/）は含むことができません。

説明

filename コマンドは FTP サーバと FTP クライアント間で転送するファイル名を指定します。

undo filename コマンドはデフォルトに戻します。

例

FTP サーバと FTP クライアント間で転送するファイル名を **config.txt** に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type ftp

[AC-nqa-admin-test-ftp] filename config.txt

2.1.12 frequency

Syntax

frequency *interval*

undo frequency

デフォルト

0 ミリ秒

View

FTP/HTTP/SNMP/TCP operation view

ICMP/UDP echo operation view

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

interval: 2 つの連続するテスト間隔を指定します。設定範囲は 0～604800000 ミリ秒です。0 を指定した場合、テストは 1 回だけ実行され、統計情報は作成しません。

説明

frequency コマンドは NQA テストを繰り返す間隔を設定します。

undo frequency コマンドはデフォルトに戻します。

テストがテスト間隔に到達しても完了していなかった場合は、次のテストは開始されません。

例

ICMP エコーテストを繰り返す間隔を 1000 ミリ秒に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] frequency 1000

2.1.13 history-record enable

Syntax

history-record enable

undo history-record enable

デフォルト

無効

View

FTP/HTTP/SNMP/TCP operation view

ICMP/UDP echo operation view

定義済みユーザロール

network-admin

説明

history-record enable コマンドは NQA テストの履歴記録の保存を有効にします。

undo history-record enable コマンドは NQA テストの履歴記録の保存を無効にします。

NQA テストの履歴記録を表示する場合、**display nqa history** コマンドを使用します。

undo history-record enable コマンドは NQA テストの既存の履歴記録についても削除します。

例

NQA テストの履歴記録の保存を有効にします。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] history-record enable

関連コマンド

display nqa history

2.1.14 history-record keep-time

Syntax

history-record keep-time *keep-time*

undo history-record keep-time

デフォルト

120 分

View

FTP/HTTP/SNMP/TCP operation view

ICMP/UDP echo operation view

定義済みユーザロール

network-admin

パラメータ

keep-time: 履歴記録を保存する期間を指定します。設定範囲は 1～1440 分です。

説明

history-record keep-time コマンドは NQA テストの履歴記録の有効期限を指定します。

undo history-record keep-time コマンドはデフォルトに戻します。

NQA テストが完了するとタイマが開始します。すべての記録は有効期限になったとき、削除されます。

例

NQA テストの履歴記録の有効期限を 100 分に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] history-record keep-time 100

2.1.15 history-record number

Syntax

history-record number *number*

undo history-record number

デフォルト

50

View

FTP/HTTP/SNMP/TCP operation view

ICMP/UDP echo operation view

定義済みユーザロール

network-admin

パラメータ

number: NQA テストで履歴記録を保存できる最大数を指定します。設定範囲は 0～50 です。

説明

history-record number コマンドは NQA テストで履歴記録を保存できる最大数を設定します。

undo history-record number コマンドはデフォルトに戻します。

NQA テストの履歴記録の数が最大数を超過した場合、もっとも古い履歴記録が削除されます。

例

NQA テストで履歴記録を保存できる最大数を 10 に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] history-record number 10

2.1.16 next-hop ip

Syntax

next-hop ip *ip-address*

undo next-hop ip

デフォルト

設定なし

View

ICMP echo operation view

定義済みユーザロール

network-admin

パラメータ

ip-address: ネクストホップの IPv4 アドレスを指定します。

説明

next-hop コマンドは ICMP エコーテストのネクストホップの IP アドレスを設定します。

undo next-hop コマンドはネクストホップの IP アドレスを削除します。

ネクストホップの IP アドレスが設定されていない場合、装置は ICMP エコーパケットのネクストホップの IP アドレスを決定するためルーティングテーブルを検索します。

例

ICMP エコーテストのネクストホップの IPv4 アドレスを 10.1.1.1 に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] next-hop ip 10.1.1.1

2.1.17 nqa

Syntax

nqa entry *admin-name operation-tag*

undo nqa { **all** | **entry** *admin-name operation-tag* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はテストタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。

all: すべての NQA テストを削除します。

説明

nqa コマンドは NQA テストを作成し、その view に移行します。NQA テストがすでに存在する場合、その view に移行します。

undo nqa コマンドはテストを削除します。

テストタイプが設定されている場合、NQA operation view にすぐに移行します。

例

管理者 **admin** とテストタグ **test** の NQA テストを作成し、NQA operation view に移行します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test]

2.1.18 nqa agent enable

Syntax

nqa agent enable

undo nqa agent enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

nqa agent enable コマンドは NQA クライアントを有効にします。

undo nqa agent enable コマンドは NQA クライアントを無効にし、すべてのテストを停止します。

例

NQA クライアントを有効にします。

<AC> system-view

[AC] nqa agent enable

関連コマンド

nqa server enable

2.1.19 nqa schedule

Syntax

nqa schedule *admin-name operation-tag* **start-time** { *hh:mm:ss* [*yyyy/mm/dd* | *mm/dd/yyyy*] | **now** } **lifetime** { *lifetime* | **forever** } [**recurring**]

undo nqa schedule *admin-name operation-tag*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はテストタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。

start-time: NQA テストの開始日時を指定します。

hh:mm:ss: NQA テストの開始時間を指定します。

yyyy/mm/dd: NQA テストの開始日を指定します。デフォルトは現在のシステム時間です。yyy の設定範囲は 2000～2035 です。

mm/dd/yyyy: NQA テストの開始日を指定します。デフォルトは現在のシステム時間です。yyy の設定範囲は 2000～2035 です。

now: すぐにテストを開始します。

lifetime: テストの有効期限を指定します。

lifetime: 動作期間を指定します。設定範囲は 1～2147483647 秒です。

forever: **undo nqa schedule** コマンドを使用して手動で停止するまでテストを実行します。

recurring: 開始時間に自動でテストを開始し、指定した期間、実行し続けます。指定しない場合、指定した期間で 1 回のみ実行します。

説明

nqa schedule コマンドは NQA テストのスケジューリングのパラメータを設定します。

undo nqa schedule コマンドはテストを停止します。

スケジュールされた NQA テストの operation view あるいは operation type view に移行することはできません。

テストを完了するために十分に長い lifetime を指定する必要があります。

例

管理者 **admin** とテストタグ **test** の NQA テストをスケジューリングします。2008 年 8 月 8 日の 08 時 08 分 08 秒に開始し、1000 秒間テストを行うように設定します。

<AC> system-view

[AC] nqa schedule admin test start-time 08:08:08 2008/08/08 lifetime 1000 recurring

関連コマンド

- **destination ip**
- **nqa entry**
- **type**

2.1.20 operation (FTP operation view)

Syntax

operation { **get** | **put** }

undo operation

デフォルト

get

View

FTP operation view

定義済みユーザロール

network-admin

パラメータ

get: FTP サーバからファイルを取得します。

put: FTP サーバにファイルを転送します。

説明

operation コマンドは FTP テストのオペレーションタイプを指定します。

undo operation コマンドはデフォルトに戻します。

filename コマンドで **put** オペレーションを実行するとき、NQA クライアント上にファイルが存在していることを確認してください。

FTP サーバからファイルを取得する場合、FTP サーバの URL に指定されたファイルが存在していることを確認してください。NQA クライアントは FTP サーバから取得したファイルを保存しません。

FTP テストではファイルサイズが小さいファイルを使用してください。大きいサイズのファイルは、タイムアウトでテストが失敗したり、ネットワークの帯域幅以上を占有して他のサービスに影響を与えたりする可能性があります。

例

FTP テストのオペレーションタイプを **put** に指定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type ftp

[AC-nqa-admin-test-ftp] operation put

関連コマンド

- **password**
- **username**

2.1.21 operation (HTTP operation view)

Syntax

operation { **get** | **post** }

undo operation

デフォルト

get

View

HTTP operation view

定義済みユーザロール

network-admin

パラメータ

get: HTTP サーバからファイルを取得します。

post: HTTP サーバにファイルを転送します。

説明

operation コマンドは HTTP テストのオペレーションタイプを指定します。

undo operation コマンドはデフォルトに戻します。

HTTP テストはプローブパケットとして HTTP request を使用します。

HTTP の **get** あるいは **post** オペレーションの HTTP request の内容は **url** コマンドによって指定された URL から取得されます。

例

HTTP テストのオペレーションのタイプを **post** に指定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type http

[AC-nqa-admin-test-http] operation post

関連コマンド

- **password**
- **username**

2.1.22 password

Syntax

password { **cipher** | **simple** } *password*

undo password

デフォルト

設定なし

View

FTP/HTTP operation view

定義済みユーザロール

network-admin

パラメータ

cipher: 暗号パスワードを指定します。

simple: 平文パスワードを指定します。

password: パスワードを指定します。大文字、小文字を区別します。

- **simple** を指定した場合の設定範囲は 1～32 文字です

□ **cipher** を指定した場合の設定範囲は 1～73 文字です。

説明

password コマンドはパスワードを設定します。

undo password コマンドは設定を削除します。

セキュリティのため、平文で設定されたパスワードを含めたすべてのパスワードは暗号テキストで保存されます。

例

FTP ログインパスワードを **ftpuser** に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type ftp

[AC-nqa-admin-test-ftp] password simple ftpuser

関連コマンド

- **operation**
- **username**

2.1.23 probe count

Syntax

probe count *times*

undo probe count

デフォルト

1

View

FTP/HTTP/SNMP/TCP operation view

ICMP/UDP echo operation view

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

times: プローブ回数を指定します。設定範囲は 1～15 です。

説明

probe count コマンドは NQA テストのプローブ回数を設定します。

undo probe count コマンドはデフォルトに戻します。

以下に異なるタイプのテストを実行する方法を示します。

- TCP テストはコネクションをセットアップします。
- UDP ジッタテストは多数のプローブパケットを送信します。プローブパケットの数は **probe packet-number** コマンドによって設定されます。
- FTP テストはファイルをアップロードあるいはダウンロードします。
- HTTP テストは Web ページを取得します。
- ICMP エコーテストは ICMP エコー要求を送信します。
- UDP エコーテストは UDP パケットを送信します。
- SNMP テストは 1 つの SNMPv1 パケット、1 つの SNMPv2c パケット、1 つの SNMPv3 パケットを送信します。

例

ICMP エコーテストを実行するプローブ回数を 10 に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] probe count 10

2.1.24 probe packet-interval

Syntax

probe packet-interval *packet-interval*

undo probe packet-interval

デフォルト

20 ミリ秒

View

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

packet-interval: パケットを送信する間隔を指定します。設定範囲は 10～60000 ミリ秒です。

説明

probe packet-interval コマンドはプローブのパケット送信間隔を設定します。

undo probe packet-interval コマンドはデフォルトに戻します。

例

UDP ジッタテストのパケット送信間隔を 100 ミリ秒に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type udp-jitter

[AC-nqa-admin-test-udp-jitter] probe packet-interval 100

2.1.25 probe packet-number

Syntax

probe packet-number *packet-number*

undo probe packet-number

デフォルト

10

View

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

packet-number: プローブごとに送信するパケット数を指定します。設定範囲は 10～1000 です。

説明

probe packet-number コマンドは UDP ジッタテストで送信するパケットの数を設定します。

undo probe packet-number コマンドはデフォルトに戻します。

例

UDP ジッタテストで 100 パケットを送信するように設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type udp-jitter

[AC-nqa-admin-test-udp-jitter] probe packet-number 100

2.1.26 probe packet-timeout

Syntax

probe packet-timeout *packet-imeout*

undo probe packet-timeout

デフォルト

3000 ミリ秒

View

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

packet-timeout:タイムアウト時間を指定します。設定範囲は 10～3600000 ミリ秒です。

説明

probe packet-timeout コマンドは NQA クライアントが宛先デバイスからの応答を待つ時間を設定します。

undo probe packet-timeout コマンドはデフォルトに戻します。

例

UDP ジッタテストの応答待ちタイムアウト時間を 100 ミリ秒に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type udp-jitter

[AC-nqa-admin-test-udp-jitter] probe packet-timeout 100

2.1.27 probe timeout

Syntax

probe timeout *timeout*

undo probe timeout

デフォルト

3000 ミリ秒

View

FTP/HTTP/SNMP/TCP operation view

ICMP/UDP echo operation view

定義済みユーザロール

network-admin

パラメータ

timeout: プローブのタイムアウト時間を指定します。

- FTP テスト、HTTP テストの設定範囲は 10～86400000 ミリ秒です。
- ICMP エコーテスト、SNMP テスト、TCP テスト、UDP エコーテストの設定範囲は 10～3600000 ミリ秒です。

説明

probe timeout コマンドはプローブのタイムアウト時間を設定します。

undo probe timeout コマンドはデフォルトに戻します。

時間内にテストが完了しなかった場合、プローブはタイムアウトします。

例

ICMP エコーテストのプローブタイムアウト時間を 10000 ミリ秒に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] probe timeout 10000

2.1.28 reaction checked-element probe-fail (for trap)

Syntax

reaction *item-number* **checked-element probe-fail threshold-type** { **accumulate** *accumulate-occurrences* | **consecutive** *consecutive-occurrences* } [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

デフォルト

設定なし

View

FTP/HTTP/SNMP/TCP operation view

ICMP/UDP echo operation view

定義済みユーザロール

network-admin

パラメータ

item-number: リアクションエントリに ID を割り当てます。設定範囲は 1～10 です。

threshold-type: しきい値タイプを指定します。

accumulate *accumulate-occurrences*: プローブが失敗する総数を確認します。設定範囲は 1～15 です。

consecutive *consecutive-occurrences*: 連続してテストに失敗する最大数を指定します。設定範囲は 1～16 です。

action-type: トリガとなるアクションを指定します。デフォルトのアクションは **none** です。

none: 端末ディスプレイに結果を表示します。

trap-only: 端末ディスプレイに結果を表示し、NMS に SNMP トラップメッセージを送信します。

説明

reaction checked-element probe-fail コマンドはテストのプローブの失敗をモニタするためのリアクションエントリを設定します。

undo reaction コマンドは指定されたリアクションエントリを削除します。

リアクションを作成した後、修正することはできません。リアクションエントリの属性を変更する場合、**undo reaction** コマンドを使用して最初にエントリを削除し、新しいリアクションエントリを再度設定してください。

例

ICMP エコーテストのプローブ失敗をモニタするため、リアクションエントリ 1 を作成します。NQA テストを開始する前に、リアクションエントリの初期状態は無効です。プローブが失敗した回数が 10 以上になった場合、エントリの状態をしきい値超過に設定します。しきい値が下回った場合、エントリの状態をしきい値以下に設定します。一旦リアクションエントリの状態が変更するとトラップメッセージを作成し、NMS に送信します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type accumulate 10 action-type trap-only

ICMP エコーテストのプローブ失敗をモニタするため、リアクションエントリ 2 を作成します。NQA テストを開始する前に、リアクションエントリの初期状態は無効です。連続してプローブが失敗した回数が 10 以上になった場合、エントリの状態をしきい値超過に設定します。しきい値を下回った場合、エントリの状態をしきい値以下に設定します。一旦リアクションエントリの状態が変更するとトラップメッセージを作成し、NMS に送信します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] reaction 2 checked-element probe-fail threshold-type consecutive 10 action-type trap-only

2.1.29 reaction trap

Syntax

reaction trap { **probe-failure** *consecutive-probe-failures* | **test-complete** | **test-failure** [*cumulate-probe-failures*] }

undo reaction trap { **probe-failure** | **test-complete** | **test-failure** }

デフォルト

設定なし

View

FTP/HTTP/SNMP/TCP operation view

ICMP/UDP echo operation view

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

probe-failure *consecutive-probe-failures*: 連続してテストが失敗した後、NMS にトラップを送信するよう設定します。*consecutive-probe-failures* はテストにおける連続失敗数を設定します。設定範囲は 1～15 です。システムは複数のトラップを送信できるように各テストで連続して失敗した回数をカウントします。

test-complete: テストが完了したことを通知するためにトラップを送信します。

test-failure: テスト失敗時にトラップを送信します。システムはテストにおけるプローブ失敗の総数をカウントしています。回数が *cumulate-probe-failures* を越えた場合、テスト失敗のトラップが送信されます。

ccumulate-probe-failures: テストにおけるプローブ失敗の総数を指定します。設定範囲は 1～15 です。

説明

reaction trap コマンドは指定した状況で NMS にトラップを送信するように設定します。

undo reaction trap コマンドはデフォルトに戻します。

UDP ジッタテストは **test-complete** パラメータのみサポートします。

例

ICMP エコーテストで連続して 5 回以上失敗した場合、トラップを送信するように設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] reaction trap probe-failure 5

2.1.30 resolve-target

Syntax

resolve-target *domain-name*

undo resolve-target

デフォルト

設定なし

View

DNS operation view

定義済みユーザロール

network-admin

パラメータ

domain-name: 解決されるドメイン名を指定します。設定範囲は 1～255 文字です。ドットで区切り、大文字、小文字を区別します。英字、数字、ハイフン（-）、アンダーライン（_）を含むことができます（たとえば、aabbcc.com です）。各部分の設定範囲は 1～63 文字です。連続したドット（.）は使用できません。

説明

resolve-target コマンドは DNS テストのドメイン名を設定します。

undo resolve-target コマンドはデフォルトに戻します。

例

解決されるドメイン名 **domain1** を設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type dns

[AC-nqa-admin-test-dns] resolve-target domain1

2.1.31 route-option bypass-route

Syntax

route-option bypass-route

undo route-option bypass-route

デフォルト

無効

View

FTP/HTTP/SNMP/TCP operation view

ICMP/UDP echo operation view

UDP jitter operation view

定義済みユーザロール

network-admin

説明

route-option bypass-route コマンドはダイレクトな宛先への接続性を確認するため、ルーティングテーブルバイパス機能を有効にします。

undo route-option bypass-route コマンドはルーティングバイパス機能を無効にします。

ルーティングテーブルバイパス機能が有効であるとき、以下のイベントが発生します。

- ルーティングテーブルは検索されません。パケットは接続されたネットワークの宛先に直接送信されます。
- テストパケットの TTL が 1 に設定されます。**ttl** コマンドで設定された値は適用されません。

例

ルーティングテーブルバイパス機能を有効にします。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] route-option bypass-route

2.1.32 source interface

Syntax

source interface *interface-type interface-number*

undo source interface

デフォルト

プローブパケットに送信元 IP アドレスは設定されていません。プローブパケットは送信元 IP アドレスとして送信インタフェースのプライマリ IP アドレスを使用します。

View

ICMP echo operation view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。

説明

source interface コマンドは ICMP エコー要求パケットの送信元 IP アドレスとして指定したインタフェースの IP アドレスを指定します。

undo source interface コマンドはデフォルトに戻します。

source ip コマンドと **source interface** コマンドの両方を設定した場合、最後に行った設定が適用されます。

指定したインタフェースはアップ状態にする必要があります。ダウンしている場合、ICMP エコー要求を送信することができません。

例

ICMP エコー要求パケットの送信元 IP アドレスとして VLAN インタフェース 2 の IP アドレスを設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] source interface vlan-interface 2

関連コマンド

source ip

2.1.33 source ip

Syntax

source ip *ip-address*

undo source ip

デフォルト

プローブパケットの送信元 IP アドレスは設定されていません。

View

FTP/HTTP/SNMP/TCP operation view

ICMP/UDP echo operation view

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

ip-address: プローブパケットの送信元 IPv4 アドレスを指定します。

説明

source ip コマンドはプローブパケットの送信元 IP アドレスを設定します。

undo source ip コマンドは指定された送信元アドレスを削除します。プローブパケットの送信元 IPv4 アドレスは送信インタフェースの IP アドレスです。

ICMP エコーテストで **source ip** コマンドと **source interface** コマンドの両方を設定した場合、最後に行った設定が適用されます。

指定された送信元 IPv4 アドレスはローカルインタフェースの IPv4 アドレスで、インタフェースがアップしている必要があります。そうでない場合、プローブパケットは送信できません。

例

ICMP エコー要求の送信元 IP アドレスを 10.1.1.1 に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] source ip 10.1.1.1

関連コマンド

source interface

2.1.34 source port

Syntax

source port *port-number*

undo source port

デフォルト

設定なし

View

SNMP operation view

UDP echo operation view

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

port-number: 送信元ポート番号を指定します。設定範囲は 1～65535 です。

説明

source port コマンドはプローブパケットの送信元ポート番号を設定します。

undo source port コマンドは設定された送信元ポート番号を削除します。

例

UDP エコーテストのプローブパケットで送信元ポートを 8000 に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type udp-echo

[AC-nqa-admin-test-udp-echo] source port 8000

2.1.35 statistics interval

Syntax

statistics interval *interval*

undo statistics interval

デフォルト

60 分

View

FTP/HTTP/SNMP/TCP operation view

ICMP/UDP echo operation view

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

interval: 統計情報を収集する間隔を指定します。設定範囲は 1～35791394 分です。

説明

statistics interval コマンドは NQA テストで統計情報を収集する間隔を設定します。

undo statistics interval コマンドはデフォルトに戻します。

NQA は指定した間隔で NQA テストを行い、テスト結果の統計情報を計算します。これらの統計情報は統計情報グループを作ります。統計情報グループの情報を表示する場合、**display nqa statistics** コマンドを使用します。

例

ICMP エコーテストで統計情報を収集する間隔を 2 分に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] statistics interval 2

2.1.36 statistics max-group

Syntax

statistics max-group *number*

undo statistics max-group

デフォルト

2

View

FTP/HTTP/SNMP/TCP operation view

ICMP/UDP echo operation view

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

number: 統計情報グループの最大数を指定します。設定範囲は 0～100 です。統計情報の収集を無効にする場合、0 に設定します。

説明

statistics max-group コマンドは保存できる統計情報グループの最大数を設定します。

undo statistics max-group コマンドはデフォルトに戻します。

統計情報グループの数が最大数に到達し、新しいグループが保存されたとき、もっとも古い統計情報が削除されます。

例

ICMP エコーテストで保存できる統計情報グループの最大数を 5 に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] statistics max-group 5

2.1.37 tos

Syntax

tos *value*

undo tos

デフォルト

0

View

すべての operation view

定義済みユーザロール

network-admin

パラメータ

value: ToS 値を指定します。設定範囲は 0～255 です。

説明

tos コマンドはプローブパケットの IP ヘッダの ToS 値を設定します。

undo tos コマンドはデフォルトに戻します。

例

ICMP エコーテストでプローブパケットの IP ヘッダの ToS 値を 1 に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] tos 1

2.1.38 ttl

Syntax

ttl *value*

undo ttl

デフォルト

20

View

FTP/HTTP/SNMP/TCP operation view

ICMP/UDP echo operation view

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

value: プローブパケットの TTL を指定します。設定範囲は 1～255 です。

説明

ttl コマンドはプローブパケットの TTL を指定します。

undo ttl コマンドはデフォルトに戻します。

route-option bypass-route コマンドはプローブパケットの TTL を 1 に設定します。**ttl** コマンドは適用されません。

例

ICMP エコーテストでプローブパケットの TTL を 16 に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type icmp-echo

[AC-nqa-admin-test-icmp-echo] ttl 16

2.1.39 type

Syntax

type { **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** }

デフォルト

設定なし

View

NQA operation view

定義済みユーザロール

network-admin

パラメータ

ftp: FTP テストタイプを指定します。

http: HTTP テストタイプを指定します。

icmp-echo: ICMP エコーテストタイプを指定します。

snmp: SNMP テストタイプを指定します。

tcp: TCP テストタイプを指定します。

udp-echo: UDP エコーテストタイプを指定します。

udp-jitter: UDP ジッタテストタイプを指定します。

説明

type コマンドは NQA テストのテストタイプを設定し、operation type view に移行します。

例

FTP テストのテストタイプを設定し、FTP operation view に移行します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type ftp

[AC-nqa-admin-test-ftp]

2.1.40 url

Syntax

url *url*

undo url

デフォルト

設定なし

View

FTP/HTTP operation view

定義済みユーザロール

network-admin

パラメータ

url: 宛先サーバの URL を指定します。設定範囲は 1～255 文字です。大文字、小文字を区別します。以下の表に異なるテストの URL フォーマットとパラメータを示します。

テスト	URL フォーマット	パラメータの説明
HTTPテスト	*http://host/resource* *http://host:port/resource*	hostパラメータの設定範囲は1～255文字です。ドットで区切られ、大文字、小文字を区別します。英字、数字、ハイフン（-）、アンダーライン（_）を含むことができます。たとえばaabbcc.comです。各部分の設定範囲は1～63文字です。連続してドット（.）を設定することができません。ファイル名のパラメータの詳細は、オペレーションマニュアルのセクション1 *はじめに “ファイルシステム管理”* を参照してください。
FTPテスト	*ftp://host/filename* *ftp://host:port/filename*	

説明

url コマンドは宛先 HTTP サーバあるいは宛先 FTP サーバの URL を指定します。

undo url コマンドは URL を削除します。

例

HTTP テストの URL を **http://www.company.com/index.htm** に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type http

[AC-nqa-admin-test-http] url http://www.company.com/index.html

2.1.41 username

Syntax

username *username*

undo username

デフォルト

設定なし

View

FTP/HTTP operation view

定義済みユーザロール

network-admin

パラメータ

username: ユーザ名を指定します。設定範囲は 1～32 文字で、大文字、小文字を区別します。

説明

username コマンドはユーザ名を指定します。

undo username コマンドはデフォルトに戻します。

例

FTP ログインのユーザ名を **administrator** に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type ftp

[AC-nqa-admin-test-ftp] username administrator

関連コマンド

- **operation**

- **password**

2.1.42 version

Syntax

version { **v1.0** | **v1.1** }

undo version

デフォルト

1.0

View

HTTP operation view

定義済みユーザロール

network-admin

パラメータ

v1.0: HTTP バージョン 1.0 を使用します。

v1.1: HTTP バージョン 1.1 を使用します。

説明

version コマンドは HTTP テストで使用する HTTP バージョンを指定します。

undo version コマンドはデフォルトに戻します。

例

HTTP テストで使用する HTTP バージョンを 1.1 に指定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type http

[AC-nqa-admin-test-http] version v1.1

2.2 NQAサーバ設定コマンド

⚠ **重要：**

UDP ジッタテスト、TCP テスト、UDP エコーテストでのみ NQA サーバを設定します。

2.2.1 display nqa server

Syntax

display nqa server

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nqa server コマンドは NQA サーバの状態を表示します。

例

NQA サーバの状態を表示します。

<AC> display nqa server

```
NQA server status: enabled
TCP connect:
  IP Address         Port     ToS    VPN instance
  2.2.2.2            2000     200    -
UDP echo:
  IP Address         Port     ToS    VPN instance
  3.3.3.3            3000     255    vpn1
```

表 2-6 コマンド出力

フィールド	説明
NQA server status	NQAサーバが有効かどうか
TCP-connect	NQAサーバのTCPリスニングサービスの情報
UDP-echo	NQAサーバのUDPリスニングサービスの情報

フィールド	説明
IP Address	NQAサーバのTCP/UDPリスニングサービスで指定されたIPアドレス
Port	NQAサーバのTCP/UDPリスニングサービスでの指定されたポート番号
Tos	NQAサーバが送信する応答パケットのToS値
VPN instance	NQAサーバがlistenするIPアドレスが属するMPLS L3VPNインスタンスの名前。 このフィールドには、NQAサーバがパブリックIPアドレスでlistenする場合にハイフン（-）が表示されます。 本フィールドは現在のソフトウェアバージョンでサポートしていません。

関連コマンド

- **nqa server enable**
- **nqa server tcp-connect**
- **nqa server udp-echo**

2.2.2 nqa server enable

Syntax

nqa server enable

undo nqa server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

nqa server enable コマンドは NQA サーバを有効にします。

undo nqa server enable コマンドは NQA サーバを無効にします。

例

NQA サーバを有効にします。

<AC> system-view

[AC] nqa server enable

関連コマンド

- **display nqa server**
- **nqa server tcp-connect**
- **nqa server udp-echo**

2.2.3 nqa server tcp-connect

Syntax

nqa server tcp-connect *ip-address port-number* [**tos** *tos*]

undo nqa server tcp-connect *ip-address port-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: TCP リスニングサービスの IP アドレスを指定します。

port-number: TCP リスニングサービスのポート番号を指定します。設定範囲は 1～65535 です。

tos *tos*: 応答パケットの IP ヘッダの ToS を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

説明

nqa server tcp-connect コマンドは NQA サーバが指定された IP アドレスとポート番号をリスニングして応答するため、TCP リスニングサービスを設定します。

undo nqa server tcp-connect コマンドは TCP リスニングサービスを削除します。

本コマンドは NQA サーバ上で TCP テストのみに使用されます。

NQA サーバの TCP リスニングサービスの IP アドレスとポート番号を設定するとき、以下の制限とガイドラインに従ってください。

- IP アドレスとポート番号は NQA サーバで固有に設定し、NQA クライアントの設定に一致するようにしてください。
- IP アドレスは NQA サーバのインタフェースの IP アドレスにする必要があります。

- NQA テストを正常に実行し、既存のサービスへの影響を防ぐため、TCP リスニングサービスで 1～1023 の well-known ポートを設定しないでください。

例

NQA サーバで TCP リスニングサービスを設定します。IP アドレス 169.254.10.2、ポート番号 9000 をリスニングし応答するように設定します。

<AC> system-view

[AC] nqa server tcp-connect 169.254.10.2 9000

関連コマンド

- **display nqa server**
- **nqa server enable**

2.2.4 nqa server udp-echo

Syntax

nqa server udp-echo *ip-address port-number* [**tos** *tos*]

undo nqa server udp-echo *ip-address port-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: UDP リスニングサービスの IP アドレスを指定します。

port-number: UDP リスニングサービスのポート番号を指定します。設定範囲は 1～65535 です。

tos *tos*: 応答パケットの IP ヘッダの ToS を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

説明

nqa server udp-echo コマンドは NQA サーバが指定された IP アドレスとポート番号をリスニングし応答するため、UDP リスニングサービスを設定します。

undo nqa server udp-echo コマンドは UDP リスニングサービスを削除します。

本コマンドは NQA サーバ上で UDP ジッタテスト、UDP エコーテストのみに使用されます。

NQA サーバの UDP リスニングサービスの IP アドレスとポート番号を設定するとき、以下の制限とガイドラインに従ってください。

- IP アドレスとポート番号は NQA サーバで固有に設定し、NQA クライアントの設定に一致するようにしてください。
- IP アドレスは NQA サーバのインタフェースの IP アドレスにする必要があります。
- NQA テストを正常に実行し、既存のサービスへの影響を防ぐため、UDP リスニングサービスで 1～1023 の well-known ポートを設定しないでください。

例

NQA サーバで UDP リスニングサービスを設定します。IP アドレス 169.254.10.2、ポート番号 9000 をリスニングし、応答するように設定します。

<AC> system-view

[AC] nqa server udp-echo 169.254.10.2 9000

関連コマンド

- **display nqa server**
- **nqa server enable**

目次

このセクションのページは **11-x-x** です。

3 章 NTP 3-1
3.1 NTP 設定コマンド 3-1
3.1.1 display ntp-service sessions 3-1
3.1.2 display ntp-service status 3-7
3.1.3 display ntp-service trace 3-9
3.1.4 ntp-service acl 3-11
3.1.5 ntp-service authentication enable 3-13
3.1.6 ntp-service authentication-keyid 3-13
3.1.7 ntp-service broadcast-client 3-15
3.1.8 ntp-service broadcast-server 3-16
3.1.9 ntp-service dscp 3-17
3.1.10 ntp-service enable 3-18
3.1.11 ntp-service inbound enable 3-18
3.1.12 ntp-service max-dynamic-sessions 3-19
3.1.13 ntp-service multicast-client 3-20
3.1.14 ntp-service multicast-server 3-21
3.1.15 ntp-service reliable authentication-keyid 3-22
3.1.16 ntp-service source 3-23
3.1.17 ntp-service unicast-peer 3-25
3.1.18 ntp-service unicast-server 3-26

3章 NTP

3.1 NTP設定コマンド

NTP は、以下のレイヤ 3 インタフェースでサポートされています。

- Layer 3 Ethernet interfaces
- VLAN interfaces
- Tunnel interfaces

3.1.1 display ntp-service sessions

Syntax

display ntp-service sessions [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose: すべての IPv4 NTP アソシエーションの詳細情報を表示します。指定しない場合、NTP アソシエーションの概要情報を表示します。

説明

display ntp-service sessions コマンドはすべての IPv4 NTP アソシエーションの情報を表示します。

装置が NTP ブロードキャストモードあるいはマルチキャストサーバモードで動作しているとき、**display ntp-service sessions** コマンドはブロードキャストサーバあるいはマルチキャストサーバに対応する IPv4 NTP アソシエーションの情報を表示しませんが、アソシエーションの総数がカウントされます。

例

すべての NTP アソシエーションの概要情報を表示します。

<AC> display ntp-service sessions

```
      source         reference      stra reach poll  now offset  delay disper
**************************************************************************
[12345]LOCAL(0)       LOCL             0    1   64    - 0.0000 0.0000 7937.9
```

```
   [5]0.0.0.0        INIT            16    0   64    - 0.0000 0.0000 0.0000
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

表 3-1 コマンド出力

フィールド	説明
source	• 参照クロックがローカルクロックであるとき、**LOCAL**(*number*)と表示されます。ローカルクロックのIPアドレスは127.127.1.*number*です。*number*はNTPプロセス番号です。値の範囲は0～3です。 • 参照クロックが別の装置であるとき、NTPサーバのIPアドレスが表示されます。このフィールドが**0.0.0.0**である場合、NTPサーバのIPアドレスは正常に解決されていません。

reference	NTPサーバの参照クロックIDです。
	• 参照クロックがローカルクロックであるとき、stratフィールドに関連した値が表示されます。
	  • stratフィールドの値が0あるいは1である場合、**LOCL**と表示されます。
	  • stratフィールドが別の値である場合、ローカルクロックのIPアドレスを表示します。
	• 参照クロックがネットワーク上の他の装置のクロックである場合、このフィールドは装置のIPアドレスになります。装置がIPv6をサポートしている場合、装置のIPv6アドレスの最初の32ビットのMD5ダイジェストを表示します。**INIT**と表示される場合、ローカル装置はNTPサーバと接続を確立していません。

stra	クロックソースのstratumレベルです。stratumレベルはクロックの正確さを示します。値の範囲は1～16です。値が大きくなると精度が減少します。クロックの精度は1がもっとも高く、stratumが16は同期化されておらず、参照クロックを使用することができません。
reach	クロックソースの到達可能回数です。0はクロックソースが到達不能であることを示します。
poll	ポーリング間隔です。連続する2つのNTPメッセージ間の最大間隔です。

フィールド	説明
now	最後のNTPメッセージを受信、あるいはローカルクロックが最後に更新されてから現在までの時間です。 デフォルトの時間の単位は秒です。 ● 時間の長さが2048秒を超えると、分で表示されます。 ● 時間の長さが300分を超えると時間で表示されます。 ● 時間の長さが96時間を越えると日の単位で表示されます。 ● 時間の長さが999日を越えると年の単位で表示されます。 最後のNTPメッセージを受信した時間あるいはローカルクロックが最後に更新された時間が、現在時間より遅れている場合、ハイフン（-）が表示されます。
offset	リファレンスクロックに対するシステムクロックのオフセットです。単位はミリ秒です。
delay	ローカル装置からクロックソースまでのラウンドトリップ遅延です。単位はミリ秒です。
disper	リファレンスソースに対するローカルクロックの最大誤差です。単位はミリ秒です。
[12345]	● **1**—システムが選択したクロックソースです（現在のリファレンスソースです）。システムクロックstratumレベルは15以下です。 ● **2**—クロックソースのstratumレベルは15以下です。 ● **3**—クロックソースはクロック選定アルゴリズムに残りしました。 ● **4**—クロックソースはクロックソースの候補です。 ● **5**—クロックソースは設定されたコマンドで作成されました。
Total sessions	アソシエーションの総数です。

すべての IPv4 NTP アソシエーションの詳細情報を表示します。

<AC> display ntp-service sessions verbose

```
Clock source: 192.168.1.40
Session ID: 35888
Clock stratum: 2
Clock status:  configured, master, sane, valid
Reference clock ID: 127.127.1.0
VPN instance: Not specified
Local mode: client, local poll interval: 6
Peer mode: server, peer poll interval: 6
```

```
Offset: 0.2862ms, roundtrip delay: 3.2653ms, dispersion: 4.5166ms
Root roundtrip delay: 0.0000ms, root dispersion: 10.910ms
Reachabilities:31, sync distance: 0.0194
Precision: 2^18, version: 3, source interface: Not specified
Reftime: d17cbba5.1473de1e  Tue, May 17 2011  9:17:25.079
Orgtime: 00000000.00000000  Thu, Feb  7 2036  6:28:16.000
Rcvtime: d17cbbc0.b1959a30  Tue, May 17 2011  9:17:52.693
Xmttime: d17cbbc0.b1959a30  Tue, May 17 2011  9:17:52.693
Roundtrip delay samples: 0.007 0.010 0.006 0.011 0.010 0.005 0.007 0.003
Offset samples: 5629.55 3913.76 5247.27 6526.92 31.99 148.72 38.27 0.29
Filter order: 7    5    2    6    0    4    1    3

Total sessions: 1
```

表 3-2 コマンド出力

フィールド	説明
Clock source	NTPサーバのIPアドレスです。**0.0.0.0**が表示される場合、NTPサーバのIPアドレスは正常に解決されていません。
Clock stratum	NTPサーバのstratumレベルです。stratumレベルはクロックの正確さを示します。値の範囲は1～16です。値が大きくなると精度が減少します。クロックの精度は1がもっとも高く、stratumが16は同期化されておらず、参照クロックを使用することができません。
Clock status	アソシエーションに対応するクロックソースの状態です。 • **configured**—アソシエーションが設定コマンドで作成されました。 • **dynamic**—ダイナミックにアソシエーションが確立されました。 • **master**—クロックソースは現在のシステムのプライマリ参照ソースです。 • **selected**—クロックソースはクロック選定アルゴリズムに残りました。 • **candidate**—クロックソースはクロックソースの候補です • **sane**—クロックソースは認証にパスして、基準クロックとして使用されます。 • **insane**—クロックソースが認証にパスしていないか、または認証にパスしていますが、基準クロックとして使用されません。 • **valid**—クロックソースが有効です。クロックソースは以下の要件に従います。 • クロックソースは認証にパスし、同期しています。

フィールド	説明
	• stratumレベルが有効です。 • ルート遅延とルート拡散が範囲内にあります。 • **invalid**—クロックソースが無効です。 • **unsynced**—クロックソースが同期されていないか、stratumレベルが無効です。
Reference clock ID	NTPサーバの参照クロックのIDです。 • 参照クロックがローカルクロックであるとき、クロックstratumフィールドに関連した値が表示されます。 • クロックstratumフィールドの値が0あるいは1である場合、**LOCL**と表示されます。 • クロックstratumフィールドが別の値である場合、ローカルクロックのIPアドレスを表示します。 参照クロックがネットワーク上の他の装置のクロックである場合、このフィールドは装置のIPアドレスになります。装置がIPv6をサポートしている場合、装置のIPv6アドレスの最初の32ビットのMD5ダイジェストを表示します。**INIT**と表示される場合、ローカル装置はNTPサーバと接続を確立していません。
VPN instance	NTPサーバが属するVPNインスタンスです。NTPサーバがパブリックネットワークにある場合、フィールドには**Not specified**と表示されます。装置は、現在のソフトウェアバージョンではこのフィールドをサポートしていません。
Local mode	ローカル装置の動作モードです。 • **unspec**—このモードは不特定です。 • **active**—アクティブモードです。 • **passive**—パッシブモードです。 • **client**—クライアントモードです。 • **server**—サーバモードです。 • **broadcast**—ブロードキャストあるいはマルチキャストサーバモードです。 • **bclient**—ブロードキャストあるいはマルチキャストクライアントモードです。
local poll interval	ローカル装置のポーリング間隔です。値は2の乗数で表示されます。たとえば、6が表示されている場合、ローカル装置のポーリング間隔は26あるいは64秒です。
Peer mode	ピアの装置の動作モードです。 • **unspec**—このモードは不特定です。 • **active**—アクティブモードです。

フィールド	説明
	• **passive**—パッシブモードです。 • **client**—クライアントモードです。 • **server**—サーバモードです。 • **broadcast**—ブロードキャストあるいはマルチキャストサーバモードです。 • **bclient**—ブロードキャストあるいはマルチキャストクライアントモードです。
peer poll interval	ピアの装置のポーリング間隔です。値は2の乗数で表示されます。たとえば、6が表示されている場合、ローカル装置のポーリング間隔は26あるいは64秒です。
Offset	参照クロックに対するシステムクロックのオフセットです。単位はミリ秒です。
roundtrip delay	ローカル装置からクロックソースまでのラウンドトリップ遅延です。単位はミリ秒です。
dispersion	参照ソースに対するシステムクロックの最大誤差です。
Root roundtrip delay	ローカル装置からプライマリ参照ソースまでのラウンドトリップ遅延です。単位はミリ秒です。
root dispersion	プライマリ参照クロックに対するシステムクロックの最大誤差です。単位はミリ秒です。
Reachabilities	クロックソースの到達可能回数です。0は、このクロックソースが到達不可能であることを示します。
sync distance	上位レベルのクロックに対する同期距離です。単位は秒です。ばらつきとラウンドトリップ遅延の値から計算されます。
Precision	システムクロックの精度です。
version	NTPバージョンです。値の範囲は1～4です。
source interface	送信元インタフェースです。 送信元インタフェースが指定されていない場合、**Not specified**と表示されます。
Reftime	NTPメッセージの参照タイムスタンプです。
Orgtime	NTPメッセージの発生タイムスタンプです。
Rcvtime	NTPメッセージの受信タイムスタンプです。
Xmttime	NTPメッセージの送信タイムスタンプです。
Filter order	情報順序のサンプルです。

フィールド	説明
Reference clock status	ローカルクロックの状態です。このフィールドは参照クロックとしてローカルクロックを設定する**ntp-service refclock-master**コマンドを使用したときに表示されます。ローカルクロックのreachフィールドが255であるとき、**working normally**と表示されます。そうでない場合、**working abnormally**と表示されます。QX-S4100Gシリーズは**ntp-service refclock-master**コマンドをサポートしていません。
Total sessions	アソシエーションの総数です。

3.1.2 display ntp-service status

Syntax

display ntp-service status

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ntp-service status コマンドは NTP サービスの状態を表示します。

例

クロックの同期後の NTP サービスの状態を表示します。

<AC> display ntp-service status

```
Clock status: synchronized
Clock stratum: 2
System peer: LOCAL(0)
Local mode: client
Reference clock ID: 127.127.1.0
Leap indicator: 00
Clock jitter: 0.000977 s
Stability: 0.000 pps
Clock precision: 2^-10
Root delay: 0.00000 ms
Root dispersion: 3.96367 ms
Reference time: d0c5fc32.92c70b1e  Wed, Dec 29 2010 18:28:02.573
```

クロックを同期していないときの NTP サービスの状態を表示します。

<AC> display ntp-service status

```
Clock status: unsynchronized
Clock stratum: 16
Reference clock ID: none
Clock jitter: 0.000000 s
Stability: 0.000 pps
Clock precision: 2^-10
Root delay: 0.00000 ms
Root dispersion: 0.00002 ms
Reference time: d0c5fc32.92c70b1e  Wed, Dec 29 2010 18:28:02.573
```

表 3-3 コマンド出力

フィールド	説明
Clock status	システムクロックの状態です。 ● **synchronized**—システムクロックが同期されています。 ● **unsynchronized**—システムクロックが同期されていません。
Clock stratum	システムクロックのstratumレベルです。
System peer	選択されたNTPサーバのIPアドレスです。
Local mode	ローカル装置の動作モードです。 ● **unspec**—このモードは不特定です。 ● **active**—アクティブモードです。 ● **passive**—パッシブモードです。 ● **client**—クライアントモードです。 ● **server**—サーバモードです。 ● **broadcast**—ブロードキャストあるいはマルチキャストサーバモードです。 ● **bclient**—ブロードキャストあるいはマルチキャストクライアントモードです。
Reference clock ID	IPv4 NTPサーバの場合、以下を示します。 ローカル装置がリモートNTPサーバに同期されているとき、このフィールドはリモートサーバのIPアドレスを表示します。 ローカル装置が参照ソースとしてローカルクロックを使用するとき、このフィールドはローカルクロックを表示します。 ● ローカルクロックのstratumフィールドの値が1である場合、**Local**と表示されます。

フィールド	説明
	• クロックstratumフィールドが別の値である場合、ローカルクロックのIPアドレスを表示します。 IPv6 NTPサーバの場合、以下を示します。 ローカル装置がリモートIPv6 NTPサーバに同期されているとき、このフィールドはリモートサーバのIPv6アドレスの最初の32ビットのMD5ダイジェストを表示します。 ローカル装置が参照ソースとしてローカルクロックを使用するとき、このフィールドはローカルクロックを表示します。 • ローカルクロックのstratumフィールドの値が1である場合、**Local**と表示されます。 • クロックstratumフィールドが別の値である場合、ローカルクロックのIPv6アドレスの最初の32ビットのMD5ダイジェストを表示します。
Leap indicator	アラーム状態です。 • **00**—正常です。 • **01**—leap秒です。一日の最後の分が61秒であることを示します。 • **10**— leap秒です。一日の最後の分が59秒であることを示します。 • **11**—クロックが同期されていません。
Clock jitter	システムクロックと参照クロック間の相違です。単位は秒です。
Stability	クロック周波数の安定性です。値が低い場合、安定性が高いことを示します。
Clock precision	システムクロックの精度です。
Root delay	ローカル装置からプライマリ参照ソースまでのラウンドトリップ遅延です。単位はミリ秒です。
Root dispersion	プライマリ参照クロックに対するシステムクロックの最大誤差です。単位はミリ秒です。
Reference time	参照タイムスタンプです。

3.1.3 display ntp-service trace

Syntax

display ntp-service trace [source interface-type interface-number]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

source *interface-type interface-number*: 各 NTP タイムサーバをローカルデバイスからプライマリタイムサーバに戻すように NTP パケットを送信するための送信元インタフェースを指定します。指定された送信元インタフェースの IP アドレスは、NTP パケットの送信元 IP アドレスです。NTP タイムサーバの IP アドレスがリンクローカルアドレスである場合、指定された送信元インタフェースのリンクローカルアドレスは、NTP パケットの送信元 IP アドレスです。このオプションを指定しないと、トレース NTP パケットを送信するインタフェースが送信元インタフェースとして機能します。

説明

display ntp-service trace コマンドはローカル装置からプライマリタイムサーバ間の NTP タイムサーバの概要情報を表示します。

ローカルデバイスからプライマリタイムサーバまでの各 NTP タイムサーバをトレースするための送信元インタフェースを指定する場合は、送信元インタフェースと NTP タイムサーバが互いに到達可能であることを確認してください。

例

ローカル装置からプライマリタイムサーバ間の NTP タイムサーバの概要情報を表示します。

<AC> display ntp-service trace

```
Server    127.0.0.1
Stratum   3, jitter  0.000, synch distance 0.0000.
Server    3000::32
Stratum   2 , jitter 790.00, synch distance 0.0000.
RefID     127.127.1.0
```

出力は、サーバ 127.0.0.1 がサーバ 3000::32 に同期しており、サーバ 3000::32 がローカルクロックに同期していることを示します。

表 3-4 コマンド出力

フィールド	説明
Server	NTPタイムサーバのIPアドレスです。
Stratum	NTPタイムサーバのstratumレベルです。

フィールド	説明
jitter	上位レベルクロックに対するクロックオフセットのRMS（Root mean square）です。単位は秒です。
synch distance	上位レベルのNTPタイムサーバに対する同期間隔です。単位は秒です。ばらつきとラウンドトリップ遅延の値から計算されます。
RefID	プライマリタイムサーバの識別子です。プライマリタイムサーバのstratumレベルが0であるとき、**Local**と表示されます。そうでなければプライマリタイムサーバのIPアドレスが表示されます。

関連コマンド

- **ntp-service source**
- **ntp-service unicast-peer**
- **ntp-service unicast-server**

3.1.4 ntp-service acl

Syntax

ntp-service { **peer** | **query** | **server** | **synchronization** } **acl** *acl-number*

undo ntp-service { **peer** | **query** | **server** | **synchronization** } [**acl** *acl-number*]

デフォルト

peer

View

System view

定義済みユーザロール

network-admin

パラメータ

peer: タイム要求とピア装置からの NTP 制御クエリ（アラーム、認証状態、タイムサーバ情報など）を許可します。ローカル装置がピアの装置と同期することを許可します。

query: ピア装置からローカル装置の NTP 制御クエリのみ許可します。

server: タイム要求とピア装置からの NTP 制御クエリを許可します。ローカル装置がピアの装置と同期することを許可しません。

synchronization: ACL にパスするアドレスのシステムからのタイム要求のみ許可します。

acl *acl-number*: IPv4 ACL を指定します。ACL に一致するピアの装置は NTP サービスアクセス制御権があります。*acl-number* は ACL 番号を示します。標準 IPv4 ACL の設定範囲は 2000～2999 です。拡張 IPv4 ACL の設定範囲は 3000～3999 です。

説明

ntp-service acl コマンドはローカル装置の IPv4 NTP サービスにアクセスする制御権を設定します。

undo ntp-service コマンドは設定済みの IPv4 NTP サービスのアクセス制御権を削除します。

IPv4 ACL 要求によって NTP アクセスを制御することができます。**peer**、**server**、**synchronization**、**query** の順番でアクセス制御権の制限が高くなります。

装置は以下のルールで IPv4 NTP 要求を処理します。

- IPv4 NTP サービスアクセス制御権が設定されていない場合、**peer** はローカル装置とピアの装置に与えられます。
- ピアの装置の IP アドレスが複数のアクセス制御権のため IPv4 ACL の **permit** 条件に一致する場合、もっとも制限のないアクセス制御権がピアの装置に与えられます。**deny** 条件あるいは IPv4 ACL に一致しない場合、アクセス制御権は与えられません。
- アクセス制御権の IPv4 ACL が作成されていない場合、関連するアクセス制御権は与えられません。
- すべてのアクセス制御権の IPv4 ACL が作成されていない場合、**peer** が与えられます。

ntp-service acl コマンドは NTP が動作するシステムで最低限のセキュリティを提供します。より安全な方法は NTP 認証です。

例

サブネット 10.10.0.0/16 のピアの装置がローカル装置にフルアクセスできるように設定します。

<AC> system-view

[AC] acl basic 2001

[AC-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255

[AC-acl-ipv4-basic-2001] quit

[AC] ntp-service peer acl 2001

関連コマンド

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

3.1.5 ntp-service authentication enable

Syntax

ntp-service authentication enable

undo ntp-service authentication enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ntp-service authentication enable コマンドは NTP 認証を有効にします。

undo ntp-service authentication enable コマンドは NTP 認証を無効にします。

認証された NTP サーバに NTP クライアントが同期できるように、クロック同期のセキュリティが必要なネットワークで NTP 認証を有効にしてください。

NTP サーバを認証するため、認証キーを設定し、トラステッドキーとして指定します。

例

NTP 認証を有効にします。

<AC> system-view

[AC] ntp-service authentication enable

関連コマンド

- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

3.1.6 ntp-service authentication-keyid

Syntax

ntp-service authentication-keyid *keyid* **authentication-mode md5** { **cipher** | **simple** } *value*

undo ntp-service authentication-keyid *keyid*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

keyid: 認証キーID を指定します。設定範囲は 1～4294967295 です。

authentication-mode md5 *value*:キー認証に MD5 アルゴリズムを使用します。

cipher: 暗号化された形式で認証キーを設定します。

simple: プレーンテキストの認証キーを指定します。セキュリティのために、プレーンテキストで指定された認証キーは暗号化された形式で格納されます。

string: 認証キーを指定します。大文字、小文字を区別します。プレーンテキスト認証キーの設定範囲は 1～32 文字です。暗号テキスト認証キーの設定範囲は 1～73 文字です。

説明

ntp-service authentication-keyid コマンドは NTP 認証キーを設定します。

undo ntp-service authentication-keyid コマンドは NTP 認証キーを削除します。

高いセキュリティが要求されるネットワークでは、NTP 認証は NTP が動作するシステムで有効にする必要があります。NTP クライアントが認証された NTP サーバにのみ同期化することを保証するため、システムが稼働している NTP で NTP 認証を有効にする必要があります。

ピアの装置からのメッセージのキーID は認証を行うために使用されます。

このコマンドを使用して最大 128 のキーを設定することができます。

この機能はクライアントーサーバキー認証を使用してネットワークのセキュリティを拡張します。認証に失敗した装置にクライアントが同期することを禁止します。

NTP 認証キーを指定した後、トラステッドキーとして設定するため **ntp-service reliable authentication-keyid** コマンドを使用します。キーを削除した後、キーは自動で非トラステッドキーに変更します。この場合、**undo ntp-service reliable authentication-keyid** コマンドを実行する必要はありません。

例

NTP 認証を有効にします。認証キーID を 10 に設定し、MD5 認証アルゴリズムを指定し、プレーンテキストのキーを BetterKey に設定します。

<AC> system-view

[AC] ntp-service authentication enable

[AC] ntp-service authentication-keyid 10 authentication-mode md5 simple BetterKey

関連コマンド

- **ntp-service authentication enable**
- **ntp-service reliable authentication-keyid**

3.1.7 ntp-service broadcast-client

Syntax

ntp-service broadcast-client

undo ntp-service broadcast-client

デフォルト

装置は NTP アソシエーションモードで動作しません。

View

Interface view

定義済みユーザロール

network-admin

説明

ntp-service broadcast-client コマンドは NTP ブロードキャストクライアントモードで動作するように設定し、現在のインタフェースで NTP ブロードキャストパケットを受信します。

undo ntp-service broadcast-client コマンドは設定を削除します。

コマンドを設定した後、装置は NTP ブロードキャストが送信した NTP メッセージを受信し、受信した NTP メッセージをもとに同期します。

このコマンドによって、装置のインタフェースがブロードキャストクライアントモードで動作するように設定されている場合、アグリゲーショングループにインタフェースを追加することができません。アグリゲーショングループにインタフェースを追加する場合、コマンドの設定を削除してください。

例

NTP ブロードキャストクライアントモードで動作するように設定し、VLAN インタフェース 1 で NTP ブロードキャストパケットを受信します。

<AC> system-view

[AC] interface vlan-interface 1

[AC-Vlan-interface1] ntp-service broadcast-client

関連コマンド

ntp-service broadcast-server

3.1.8 ntp-service broadcast-server

Syntax

ntp-service broadcast-server [**authentication-keyid** *keyid* | **version** *number*] *

undo ntp-service broadcast-server

デフォルト

装置は NTP アソシエーションモードで動作しません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

authentication-keyid *keyid*: ブロードキャストメッセージをクライアントに送信するために使用するキーID を指定します。設定範囲は 1～4294967295 です。指定しない場合、ローカル装置は NTP 認証が有効のブロードキャストクライアントを同期できません。

version *number*: NTP バージョンを指定します。設定範囲は 1～4 です。デフォルトは 4 です。

説明

ntp-service broadcast-server コマンドは NTP ブロードキャストサーバモードで動作するように設定し、現在のインタフェースで NTP ブロードキャストパケットを送信します。

undo ntp-service broadcast-server コマンドは設定を削除します。

コマンドを設定した後、装置は定期的に NTP メッセージをブロードキャストアドレス 255.255.255.255 に送信します。

このコマンドによって、装置のインタフェースがブロードキャストサーバモードで動作するように設定されている場合、アグリゲーショングループにインタフェースを追加することができません。アグリゲーショングループにインタフェースを追加する場合、コマンドの設定を削除してください。

例

NTP ブロードキャストサーバモードで動作するように設定し、VLAN インタフェース 1 で暗号キーID が 4、NTP のバージョンが 4 の NTP ブロードキャストメッセージを送信します。

<AC> system-view

[AC] interface vlan-interface 1

[AC-Vlan-interface1] ntp-service broadcast-server authentication-keyid 4 version 4

関連コマンド

ntp-service broadcast-client

3.1.9 ntp-service dscp

Syntax

ntp-service dscp *dscp-value*

undo ntp-service dscp

デフォルト

48

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: IPv4 NTP パケットの DSCP を設定します。設定範囲は 0〜63 です。

説明

ntp-server dscp コマンドは IPv4 NTP パケットの DSCP を設定します。

undo ntp-server dscp コマンドはデフォルトに戻します。

パケットの優先度を識別するため、DSCP は IPv4 パケットの ToS フィールドに含まれます。

例

IPv4 NTP パケットの DSCP を 30 に設定します。

<AC> system-view

[AC] ntp-service dscp 30

3.1.10 ntp-service enable

Syntax

ntp-service enable

undo ntp-service enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ntp-service enable コマンドは NTP サービスを有効にします。

undo ntp-service enable コマンドは NTP サービスを無効にします。

例

NTP サービスを有効にします。

<AC> system-view

[AC] ntp-service enable

3.1.11 ntp-service inbound enable

Syntax

ntp-service inbound enable

undo ntp-service inbound enable

デフォルト

有効

View

Interface view

定義済みユーザロール

network-admin

説明

ntp-service inbound enable コマンドはインタフェースで NTP メッセージの処理を有効にします。

undo ntp-service inbound enable コマンドはデフォルトに戻します。

以下の場合、インタフェースで **undo ntp-service inbound enable** コマンドを実行してください。

- 装置のインタフェースが対応するサブネットで、ピアの装置と同期しません。
- 装置がインタフェースと一致しているサブネットでピアの装置によって同期しません。

例

VLAN インタフェース 1 で NTP メッセージの処理を無効にします。

<AC> system-view

[AC] interface vlan-interface 1

[AC-Vlan-interface1] undo ntp-service inbound enable

3.1.12 ntp-service max-dynamic-sessions

Syntax

ntp-service max-dynamic-sessions *number*

undo ntp-service max-dynamic-sessions

デフォルト

100

View

System view

定義済みユーザロール

network-admin

パラメータ

number: ダイナミック NTP アソシエーションの最大数を設定します。設定範囲は 0～100 です。

説明

ntp-service max-dynamic-sessions コマンドはダイナミック NTP アソシエーションの最大数を設定します。

undo ntp-service max-dynamic-sessions コマンドはデフォルトに戻します。

装置はスタティックアソシエーションとダイナミックアソシエーションを含めて共通で最大 128 のアソシエーションを設定することができます。スタティックアソシエーションはNTPコマンドを使用して手動で作成されたユーザのアソシエーションを参照します。ダイナミックアソシエーションはシステムの動作中に一時的に作成されたアソシエーションです。

例

ダイナミック NTP アソシエーションの最大数を 50 に設定します。

<AC> system-view

[AC] ntp-service max-dynamic-sessions 50

関連コマンド

display ntp-service sessions

3.1.13 ntp-service multicast-client

Syntax

ntp-service multicast-client [*ip-address*]

undo ntp-service multicast-client [*ip-address*]

デフォルト

装置は NTP アソシエーションモードで動作しません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: マルチキャスト IP アドレスを 224.0.0.0～239.255.255.255 の範囲で指定します。デフォルトは 224.0.1.1 です。マルチキャストサーバとクライアントは同一のマルチキャスト IP アドレスに設定する必要があります。

説明

ntp-service multicast-client コマンドはNTPマルチキャストクライアントモードで動作するように設定し、現在のインタフェースで NTP マルチキャストパケットを受信します。

undo ntp-service multicast-client コマンドは設定を削除します。

コマンドを設定した後、装置は宛先アドレスとして指定したマルチキャストアドレスを使用し NTP メッセージを受信します。

このコマンドによって、装置のインタフェースがマルチキャストクライアントモードで動作するように設定されている場合、アグリゲーショングループにインタフェースを追加することができません。アグリゲーショングループにインタフェースを追加する場合、コマンドの設定を削除してください。

例

NTP マルチキャストクライアントモードで動作するように設定します。VLAN インタフェース 1 で NTP マルチキャストパケットを受信し、マルチキャストアドレスを 224.0.1.1 に設定します。

<AC> system-view

[AC] interface vlan-interface 1

[AC-Vlan-interface1] ntp-service multicast-client 224.0.1.1

関連コマンド

ntp-service multicast-server

3.1.14 ntp-service multicast-server

Syntax

ntp-service multicast-server [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] *

undo ntp-service multicast-server [*ip-address*]

デフォルト

装置は NTP アソシエーションモードで動作しません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: マルチキャスト IP アドレスを 224.0.0.0～239.255.255.255 の範囲で指定します。デフォルトは 224.0.1.1 です。マルチキャストサーバとクライアントは同一のマルチキャスト IP アドレスに設定する必要があります。

authentication-keyid *keyid*: マルチキャストメッセージをクライアントに送信するために使用するキーID を指定します。設定範囲は 1～4294967295 です。指定しない場合、ローカル装置は NTP 認証が有効のマルチキャストクライアントを同期できません。

ttl *ttl-number*: NTP マルチキャストメッセージの TTL を指定します。設定範囲は 1～255 です。デフォルトは 16 です。

version *number*: NTP バージョンを指定します。設定範囲は 1～4 です。デフォルトは 4 です。

説明

ntp-service multicast-server コマンドは NTP マルチキャストサーバモードで動作するように設定し、現在のインタフェースで NTP マルチキャストパケットを送信します。

undo ntp-service multicast-server コマンドは設定を削除します。

コマンドを設定した後、装置は定期的に NTP メッセージをマルチキャストアドレスに送信します。

このコマンドによって、装置のインタフェースがマルチキャストサーバモードで動作するように設定されている場合、アグリゲーショングループにインタフェースを追加することができません。アグリゲーショングループにインタフェースを追加する場合、コマンドの設定を削除してください。

例

NTP マルチキャストサーバモードで動作するように設定し、VLAN インタフェース 1 で暗号キーID が 4､NTP のバージョンが 4 の NTP マルチキャストメッセージをマルチキャストアドレス 224.0.1.1 に送信します。

<AC> system-view

[AC] interface vlan-interface 1

[AC-Vlan-interface1] ntp-service multicast-server 224.0.1.1 version 4 authentication-keyid 4

関連コマンド

ntp-service multicast-client

3.1.15 ntp-service reliable authentication-keyid

Syntax

ntp-service reliable authentication-keyid *keyid*

undo ntp-service reliable authentication-keyid *keyid*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

keyid: 認証キーを指定します。設定範囲は 1～4294967295 です。

説明

ntp-service reliable authentication-keyid コマンドは作成された認証キーをトラステッドキーとして指定します。

undo ntp-service reliable authentication-keyid コマンドは設定を削除します。

NTP 認証が有効であるとき、クライアントは信頼された認証キーを提供するサーバにのみ同期することができます。

このコマンドを使用する前に、NTP 認証が有効で認証キーが設定されていることを確認してください。キーを削除した後、キーは自動で非トラステッドキーに変更します。この場合、**undo ntp-service reliable authentication-keyid** コマンドを実行する必要はありません。

例

NTP 認証を有効にし、キーの ID が 37、キーの値が **BetterKey** の MD5 アルゴリズムの認証キーを設定します。

<AC> system-view

[AC] ntp-service authentication enable

[AC] ntp-service authentication-keyid 37 authentication-mode md5 simple BetterKey

トラステッドキーとして指定します。

[AC] ntp-service reliable authentication-keyid 37

関連コマンド

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**

3.1.16 ntp-service source

Syntax

ntp-service source *interface-type interface-number*

undo ntp-service source

デフォルト

NTP メッセージのインタフェースは指定されていません。装置は以下の処理を行います。

- NTP メッセージの送信インタフェースをルーティングテーブルから検索します。

- NTP メッセージの送信元 IP アドレスとして送信インタフェースのプライマリ IP アドレスを使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。

説明

ntp-service source コマンドは NTP メッセージの送信元インタフェースを指定します。

undo ntp-service source コマンドはデフォルトに戻します。

NTP メッセージの送信元インタフェースを指定する場合、装置は NTP メッセージを送信するとき、指定されたインタフェースのプライマリ IP アドレスとして NTP メッセージの送信元 IP アドレスを設定します。したがって、NTP 応答メッセージの宛先アドレスは送信元インタフェースのプライマリ IP アドレスです。

装置が NTP 要求に応答するとき、NTP 応答の送信元 IP アドレスは常に NTP 要求を受信したインタフェースの IP アドレスです。

応答メッセージの宛先アドレスにローカル装置のインタフェースの IP アドレスを使用しない場合、NTP メッセージの送信元インタフェースとして別のインタフェースを指定するため **ntp-service source** コマンドを使用します。

- NTP クライアント/サーバモードでは、**ntp-service unicast-server** コマンドで、NTP メッセージの送信元インタフェースを指定した場合、**ntp-service unicast-server** コマンドで指定したインタフェースは NTP メッセージの送信元インタフェースとして動作します。
- NTP シンメトリックアクティブ/パッシブモードでは、**ntp-service unicast-peer** コマンドで、NTP メッセージの送信元インタフェースを指定した場合、**ntp-service unicast-peer** コマンドで指定したインタフェースは NTP メッセージの送信元インタフェースとして動作します。
- NTP マルチキャストモードでは、**ntp-service multicast-server** コマンドが設定された場合、マルチキャスト NTP メッセージの送信元インタフェースは、NTP マルチキャストメッセージの送信元インタフェースとして動作します。
- NTP ブロードキャストモードでは、**ntp-service broadcast-server** コマンドが設定された場合、ブロードキャスト NTP メッセージの送信元インタフェースは、NTP ブロードキャストメッセージの送信元インタフェースとして動作します。

指定した送信元インタフェースが down している場合、装置は NTP メッセージを送信しません。

例

NTP メッセージの送信元インタフェースとして VLAN インタフェース 1 を指定します。

<AC> system-view

[AC] ntp-service source vlan-interface 1

3.1.17 ntp-service unicast-peer

Syntax

ntp-service unicast-peer { *peer-name* | *ip-address* } [**authentication-keyid** *keyid* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-peer { *peer-name* | *ip-address* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

peer-name: シンメトリックーパッシブピアのホスト名を指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。

ip-address: シンメトリックーパッシブピアの IP アドレスを指定します。ブロードキャストアドレス、マルチキャストアドレス、ローカルクロックの IP アドレスでなくユニキャストアドレスにする必要があります。

authentication-keyid *keyid*: NTP メッセージをピアに送信するために使用するキーの ID を指定します。設定範囲は 1～4294967295 です。指定しない場合、ローカル装置とピアは互いに認証しません。

priority: 同一条件のもとで最初の選択として、*ip-address* あるいは *peer-name* で指定されたピアを指定します。

source *interface-type interface-number*: NTP メッセージの送信元インタフェースを指定します。ローカル装置がピアに NTP メッセージを送信する場合、送信元 IP アドレスはインタフェースのプライマリ IP アドレスです。*interface-type interface-number* はインタフェースのタイプと番号を示します。

version *number*: NTP バージョンを指定します。設定範囲は 1～4 です。デフォルトは 4 です。

説明

ntp-service unicast-peer コマンドは装置のシンメトリックーパッシブピアを指定します。

undo ntp-service unicast-peer コマンドは装置の指定されたシンメトリックーパッシブピアを削除します。

装置のパッシブピアを指定するとき、装置と装置のパッシブピアは互いに同期することができます。クロックが同期されている場合、高い stratum レベルのクロックは、低い stratum レベルのクロックに同期されます。

例

装置のシンメトリックーパッシブピアとして IP アドレス 10.1.1.1 の装置を指定します。NTP バージョンを 4、NTP メッセージの送信元インタフェースを VLAN インタフェース 1 に設定します。

<AC> system-view

[AC] ntp-service unicast-peer 10.1.1.1 version 4 source-interface vlan-interface 1

関連コマンド

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

3.1.18 ntp-service unicast-server

Syntax

ntp-service unicast-server { *server-name* | *ip-address* } [**authentication-keyid** *keyid* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-server { *server-name* | *ip-address* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

server-name: NTP サーバのホスト名を指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。

ip-address: NTP サーバの IP アドレスを指定します。ブロードキャストアドレス、マルチキャストアドレス、ローカルクロックの IP アドレスでなくユニキャストアドレスにする必要があります。

authentication-keyid *keyid*: NTP メッセージを NTP サーバに送信するために使用するキーの ID を指定します。設定範囲は 1～4294967295 です。指定しない場合、ローカル装置と NTP サーバは互いに認証しません。

priority: 同一条件のもとで最初の選択として、NTP サーバを指定します。

source *interface-type interface-number*: NTP メッセージの送信元インタフェースを指定します。ローカル装置が NTP サーバに NTP メッセージを送信する場合、送信元 IP アドレスはインタフェースのプライマリ IP アドレスです。*interface-type interface-number* はインタフェースのタイプと番号を示します。

version *number*: NTP バージョンを指定します。設定範囲は 1～4 です。デフォルトは 4 です。

説明

ntp-service unicast-server コマンドは装置の NTP サーバを指定します。

undo ntp-service unicast-server コマンドは装置から指定された NTP サーバを削除します。

装置の NTP サーバを指定するとき、装置は NTP サーバに同期されますが、NTP サーバは装置に同期されません。

例

装置の NTP サーバ 10.1.1.1 を指定します。NTP バージョンを 4 で動作するように装置を設定します。

<AC> system-view

[AC] ntp-service unicast-server 10.1.1.1 version 4

関連コマンド

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

目次

このセクションのページは **11-x-x** です。

4 章 SNMP 4-1
4.1 SNMP 設定コマンド 4-1
4.1.1 display snmp-agent community 4-1
4.1.2 display snmp-agent group 4-3
4.1.3 display snmp-agent local-engineid 4-5
4.1.4 display snmp-agent mib-view 4-5
4.1.5 display snmp-agent statistics 4-7
4.1.6 display snmp-agent sys-info 4-9
4.1.7 display snmp-agent trap queue 4-10
4.1.8 display snmp-agent trap-list 4-11
4.1.9 display snmp-agent usm-user 4-12
4.1.10 enable snmp trap updown 4-15
4.1.11 simulate snmp-trap 4-16
4.1.12 snmp-agent 4-18
4.1.13 snmp-agent calculate-password 4-19
4.1.14 snmp-agent community 4-20
4.1.15 snmp-agent group 4-23
4.1.16 snmp-agent local-engineid 4-26
4.1.17 snmp-agent log 4-27
4.1.18 snmp-agent mib-view 4-28
4.1.19 snmp-agent packet max-size 4-30
4.1.20 snmp-agent { inform | trap } source 4-31
4.1.21 snmp-agent sys-info contact 4-32
4.1.22 snmp-agent sys-info location 4-33
4.1.23 snmp-agent sys-info version 4-34
4.1.24 snmp-agent target-host 4-35
4.1.25 snmp-agent trap enable 4-36
4.1.26 snmp-agent trap if-mib link extended 4-38
4.1.27 snmp-agent trap life 4-39
4.1.28 snmp-agent trap log 4-40
4.1.29 snmp-agent trap queue-size 4-40
4.1.30 snmp-agent usm-user { v1 | v2c } 4-41
4.1.31 snmp-agent usm-user v3 4-44

4章 SNMP

SNMP エージェントはリンク状態の変更、ユーザのログイン、ログアウトのような重要なイベントを NMS に知らせるため、notification（トラップと inform）を送信します。特に指定しない限り、コマンドラインの trap キーワードは trap と inform を含みます。

4.1 SNMP設定コマンド

4.1.1 display snmp-agent community

Syntax

display snmp-agent community [**read** | **write**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

read: 読み出し専用コミュニティ情報を表示します。

write: 読み出し、書き込みコミュニティ情報を表示します。

説明

display snmp-agent community コマンドは SNMPv1 あるいは SNMPv2c のコミュニティ情報を表示します。

パラメータを指定しない場合、作成されたすべての SNMPv1 あるいは SNMPv2c のコミュニティ情報を表示します。

このコマンドは以下の方法で作成された SNMPv1、SNMPv2c コミュニティを表示します。

- **snmp-agent community** コマンドで作成されたコミュニティ
- 既存の SNMP グループに割り当てられた SNMPv1 と SNMPv2c のユーザ用に自動で作成されたコミュニティ

例

すべての SNMPv1 あるいは SNMPv2c のコミュニティ情報を表示します。

<AC> display snmp-agent community

```
   Community name: aa
      Group name: aa
      ACL:2001
      Storage-type: nonVolatile
      Context name: con1

   Community name: bb
      Role name: bb
      Storage-type: nonVolatile

   Community name: userv1
      Group name: testv1
      Storage type: nonvolatile
Community name: cc
      Group name: cc
      ACL name: testacl
      Storage type: nonVolatile
```

表 4-1 コマンド出力

フィールド	説明
Community name	**snmp-agent community**コマンドで作成されたコミュニティ名あるいは**snmp-agent usm-user** { **v1** | **v2c** }コマンドで作成されたユーザ名を表示します。
Group name	SNMPグループ名です。 ● **snmp-agent community**コミュニティがコマンドで作成された場合、グループ名はコミュニティ名と同一です。 ● **snmp-agent usm-user** { **v1** | **v2c** }コミュニティがコマンドで作成された場合、ユーザがあるグループ名が表示されます。
Role name	コミュニティのユーザロールです。 コミュニティがRBACモードの**snmp-agent community**コマンドで作成された場合、ユーザロールはコミュニティ名と結合できます。
ACL	ACL番号です。 このフィールドはSNMPv1あるいはSNMPv2cコミュニティで、ACLが指定されたときのみ表示されます。ACL名フィールドと一緒に表示されません。
ACL name	ACL名です。 このフィールドはSNMPv1あるいはSNMPv2cコミュニティで、ACL名が指定されたときのみ表示されます。ACLフィールドと一緒に表示されません。

フィールド	説明
Storage-type	記憶媒体のタイプです。 • **volatile**—システムが再起動したときに設定が失われます。 • **nonVolatile**—システムが再起動しても設定は失われません。 • **permanent**—システムが再起動しても設定は失われません。変更することができますが、削除することができません。 • **readOnly**—システムが再起動しても設定は失われません。変更あるいは削除することができません。 • **other**—他の記憶媒体のタイプです。
Context name	SNMPの内容です。 • SNMPコミュニティとSNMPの内容間のマッピングが設定されている場合、SNMPの内容が表示されます。 • SNMPコミュニティとSNMPの内容間のマッピングが設定されていない場合、表示されません。

関連コマンド

- **snmp-agent community**
- **snmp-agent usm-user { v1 | v2c }**

4.1.2 display snmp-agent group

Syntax

display snmp-agent group [*group-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-name: SNMPv1、SNMPv2c、SNMPv3 グループ名を指定します。設定範囲は 1～32 です。大文字、小文字を区別します。指定しない場合、すべての SNMP グループの情報を表示します。

説明

display snmp-agent group コマンドはグループ名、セキュリティモデル、MIB ビュー、ストレージタイプなどの SNMP グループの情報を表示します。

例

すべての SNMP グループの情報を表示します。

表 4-2 コマンド出力

フィールド	説明
Group name	SNMPグループ名です。
Security model	SNMPグループのセキュリティモデルです。 ● **authPriv**—プライバシーセキュリティありの認証です。 ● **authNoPriv**—プライバシーセキュリティなしの認証です。 ● **noAuthNoPriv**—認証なし、プライバシーセキュリティなしです。 SNMPv1あるいはSNMPv2cグループのセキュリティモデルはnoAuthNoPrivのみです。
Readview	SNMPグループにアクセス可能な読み込み専用のMIB viewです。
Writeview	SNMPグループにアクセス可能な書き込みのMIB viewです。
Notifyview	SNMP viewの通知MIB viewです。グループのSNMPユーザは通知MIB viewのノードの通知を送信できます。
Storage-type	記憶媒体のタイプです。**volatile**、**nonvolatile**、**permanent**、**readOnly**、**other**が含まれます。（表 4-1を参照してください。）
ACL	ACL番号です。 このフィールドはSNMPグループで、ACLが指定されたときのみ表示されます。ACL名フィールドと一緒に表示されません。
ACL name	ACL名です。 このフィールドはSNMPグループで、ACL名が指定されたときのみ表示されます。ACLフィールドと一緒に表示されません。

関連コマンド

snmp-agent group

4.1.3 display snmp-agent local-engineid

Syntax

display snmp-agent local-engineid

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display snmp-agent local-engineid コマンドはローカル SNMP エンジン ID を表示します。

各 SNMP エージェントはメッセージの送受信、メッセージの認証、暗号化、管理されたオブジェクトへのアクセス制御のサービスを提供するため 1 つの SNMP エンジンがあります。

ローカル SNMP エンジン ID は SNMP ドメインの SNMP エージェントの SNMP エンジンを固有に識別します。

例

ローカル SNMP エンジン ID を表示します。

<AC> display snmp-agent local-engineid

```
SNMP local engine ID: 800063A2800084E52BED7900000001
```

関連コマンド

snmp-agent local-engineid

4.1.4 display snmp-agent mib-view

Syntax

display snmp-agent mib-view [**exclude** | **include** | **viewname** *view-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

exclude: MIB view から除外されたサブツリーを表示します。

include: MIB view から含まれるサブツリーを表示します。

viewname *view-name*: 1～32 文字の文字列で MIB ビューを指定します。

説明

display snmp-agent mib-view コマンドは MIB view を表示します。

パラメータを指定しない場合、すべての MIB view を表示します。

例

すべての MIB view を表示します。

<AC> display snmp-agent mib-view

```
View name: ViewDefault
    MIB Subtree: iso
    Subtree mask:
    Storage-type: nonVolatile
    View Type: included
    View status: active

View name: ViewDefault
    MIB Subtree: snmpUsmMIB
    Subtree mask:
    Storage-type: nonVolatile
    View Type: excluded
    View status: active

View name: ViewDefault
    MIB Subtree: snmpVacmMIB
    Subtree mask:
    Storage-type: nonVolatile
    View Type: excluded
    View status: active

View name: ViewDefault
    MIB Subtree: snmpModules.18
    Subtree mask:
    Storage-type: nonVolatile
    View Type: excluded
    View status: active
```

ViewDefault はデフォルトの MIB view です。出力は **snmpUsmMIB**、**snmpVacmMIB**、**snmpModules.18** の MIB オブジェクトを除いて **iso** サブツリーのすべての MIB オブジェクトがアクセス可能です。

表 4-3 コマンド出力

フィールド	説明
View name	MIB view名です。
MIB Subtree	MIB viewで扱われるMIBサブツリーです。
Subtree mask	MIBサブツリーマスクです。
Storage-type	サブツリーが記録される記憶媒体（表 4-1を参照してください）のタイプです。
View Type	MIB viewのMIBサブツリーのアクセス権です。 ● **Included**—MIBサブツリーのすべてのオブジェクトがMIB viewにアクセス可能です。 ● **Excluded**—MIBサブツリーのすべてのオブジェクトがMIB viewにアクセス可能できません。
View status	MIB viewの状態です。 ● **active**—MIB viewが有効です。 ● **inactive**— MIB viewが無効です。 MIB viewは、CLIで作成されるとactiveになります。 MIB viewを削除せずに一時的に無効にするには、SNMPセット操作を実行してステータスをinactiveに設定します。

関連コマンド

snmp-agent mib-view

4.1.5 display snmp-agent statistics

Syntax

display snmp-agent statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display snmp-agent statistics コマンドは SNMP メッセージの統計情報を表示します。

例

SNMP メッセージの統計情報を表示します。

<AC> display snmp-agent statistics

```
1684 messages delivered to the SNMP entity.
5 messages were for an unsupported version.
0 messages used an unknown SNMP community name.
0 messages represented an illegal operation for the community supplied.
0 ASN.1 or BER errors in the process of decoding.
1679 messages passed from the SNMP entity.
0 SNMP PDUs had badValue error-status.
0 SNMP PDUs had genErr error-status.
0 SNMP PDUs had noSuchName error-status.
0 SNMP PDUs had tooBig error-status (Maximum packet size 1500).
16544 MIB objects retrieved successfully.
2 MIB objects altered successfully.
7 GetRequest-PDU accepted and processed.
7 GetNextRequest-PDU accepted and processed.
1653 GetBulkRequest-PDU accepted and processed.
1669 GetResponse-PDU accepted and processed.
2 SetRequest-PDU accepted and processed.
0 Trap PDUs accepted and processed.
0 alternate Response Class PDUs dropped silently.
0 forwarded Confirmed Class PDUs dropped silently.
```

表 4-4 コマンド出力

フィールド	説明
messages delivered to the SNMP entity	SNMPエージェントが受信したメッセージ数です。
messages were for an unsupported version	SNMPエージェントのバージョンでサポートされていないメッセージ数です。
messages used an unknown SNMP community name	不明なSNMPコミュニティ名が使用されたメッセージ数です。
messages represented an illegal operation for the community supplied	コミュニティを実行する権限がないオペレーションが運ばれたメッセージ数です。
ASN.1 or BER errors in the process of decoding	復号化の間にASN.1あるいはBERエラーがあるメッセージ数です。

フィールド	説明
messages passed from the SNMP entity	SNMPエージェントによって送信されたメッセージ数です。
SNMP PDUs had badValue error-status	BadValueエラーのPDU数です。
SNMP PDUs had genErr error-status	genErrエラーのPDU数です。
SNMP PDUs had noSuchName error-status	NoSuchNameエラーのPDU数です。
SNMP PDUs had tooBig error-status	TooBigエラーのPDU数です。（最大パケットサイズが1500バイトです）
MIB objects retrieved successfully	正常に読み込まれたMIBオブジェクト数です。
MIB objects altered successfully	正常に書き込まれたMIBオブジェクト数です。
GetRequest-PDU accepted and processed	読み込み、処理されたGetRequest要求の数です。
GetNextRequest-PDU accepted and processed	読み込み、処理されたgetNext要求の数です。
GetBulkRequest-PDU accepted and processed	読み込み、処理されたgetBulk要求の数です。
GetResponse-PDU accepted and processed	読み込み、処理されたget応答の数です。
SetRequest-PDU accepted and processed	読み込み、処理されたset要求の数です。
Trap PDUs accepted and processed	読み込み、処理された通知の数です。
alternate Response Class PDUs dropped silently	廃棄された応答パケットの数です。
forwarded Confirmed Class PDUs dropped silently	廃棄された転送パケットの数です。

4.1.6 display snmp-agent sys-info

Syntax

display snmp-agent sys-info [**contact** | **location** | **version**] *

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

contact: システム連絡先を表示します。

location: 装置の所在地を表示します。

version: SNMP エージェントのバージョンを表示します。

説明

display snmp-agent sys-info コマンドは SNMP エージェントシステムの情報を表示します。

パラメータを指定しない場合、すべての SNMP エージェントシステムの情報を表示します。

例

すべての SNMP エージェントシステムの情報を表示します。

<AC> display snmp-agent sys-info

```
The contact information of the agent:

The location information of the agent:

The SNMP version of the agent:
  SNMPv3
```

関連コマンド

snmp-agent sys-info

4.1.7 display snmp-agent trap queue

Syntax

display snmp-agent trap queue

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display snmp-agent trap queue コマンドは trap キューの基本情報を表示します。

例

trap キューの設定と使用状態を表示します。

<AC> display snmp-agent trap queue

```
Queue size: 100
Message number: 6
```

関連コマンド

- **snmp-agent trap life**
- **snmp-agent trap queue-size**

4.1.8 display snmp-agent trap-list

Syntax

display snmp-agent trap-list

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display snmp-agent trap-list コマンドはモジュールのステータスを有効にする SNMP 通知を表示します。

モジュールに複数のサブモジュールがあり、そのサブモジュールの 1 つに対して SNMP 通知が有効になっている場合、コマンド出力はそのモジュールが SNMP 通知を有効にしていることを示します。

モジュールが SNMP 通知をサポートしているかどうかを判断するには、**snmp-agent trap enable ?**コマンドを実行します。

display snmp-agent trap-list コマンドの出力は、**snmp-agent trap enable** コマンド設定およびモジュール設定によって異なります。

例

モジュールのステータスを有効にする SNMP 通知を表示します。

<AC> display snmp-agent trap-list

```
arp notification is enabled.
configuration notification is enabled.
ike notification is disabled.
ipsec notification is disabled.
mac-address notification is enabled.
policy-based-route notification is enabled.
port-security notification is enabled.
radius notification is disabled.
standard notification is enabled.
stp notification is disabled.
syslog notification is disabled.
system notification is enabled.
wlan ap notification is disabled.
wlan capwap notification is disabled.
wlan client notification is enabled.
wlan load-balance notification is disabled.
wlan mobility notification is disabled.
wlan usersec notification is enabled.

Enabled notifications: 9; Disabled notifications: 9
```

関連コマンド

snmp-agent trap enable

4.1.9 display snmp-agent usm-user

Syntax

display snmp-agent usm-user [**engineid** *engineid* | **group** *group-name* | **username** *user-name*] *

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

engineid *engineid*: SNMP エンジン ID の SNMPv3 ユーザ情報を表示します。SNMP エンジン ID は *engineid* で識別されます。SNMPv3 ユーザが作成されているとき、システムはローカル SNMP エンティティのエンジン ID を記録します。エンジン ID が変更され

るとユーザは無効になり、記録されたエンジン ID が復元されるとユーザが有効になります。

group *group-name*: 指定した SNMP グループ名の SNMPv3 ユーザ情報を表示します。グループ名は大文字、小文字を区別します。

username *user-name*: 指定した SNMPv3 ユーザの情報を表示します。ユーザ名は大文字、小文字を区別します。

説明

display snmp-agent usm-user コマンドは SNMPv3 ユーザ情報を表示します。

このコマンドは **snmp-agent usm-user v3** コマンドを使用して作成された SNMPv3 ユーザのみ表示します。**snmp-agent usm-user** { **v1** | **v2c** }コマンドを使用して作成された SNMPv1 あるいは SNMPv2c ユーザを表示する場合、**display snmp-agent community** コマンドを使用します。

例

すべての SNMPv3 ユーザ情報を表示します。

<AC> display snmp-agent usm-user

```
Username: userv3
Group name: mygroupv3
    Engine ID: 800063A203000FE240A1A6
    Storage type: nonVolatile
    User status: active
    ACL: 2000

Username: userv3
Group name: mygroupv3
    Engine ID: 8000259503000BB3100A508
    Storage type: nonVolatile
    User status: active
    ACL name: testacl

Username: userv3code
Role name: groupv3code
          network-operator
    Engine ID: 800063A203000FE240A1A6
    Storage type: nonVolatile
    User status: active

Username: userv3code
Role name: snmprole
          network-operator
    Engine ID: 800063A280000002BB0001
```

```
Storage type: nonVolatile
User status: active
```

表 4-5 コマンド出力

フィールド	説明
Username	SNMPユーザ名です。
Group name	SNMPグループ名です。
Role name	SNMPユーザロール名です。
Engine ID	SNMPユーザが作成されたとき、SNMPエージェントが使用したエンジンIDです。
Storage-type	記憶媒体のタイプです。 ● **volatile** ● **nonVolatile** ● **permanent** ● **readOnly** ● **other** 記憶媒体の詳細は表 4-1を参照してください。
UserStatus	SNMPユーザの状態です。 ● **active**—SNMPユーザは動作しています。 ● **notInService**—SNMPユーザは正常に設定されていますが、動作していません。 ● **notReady**—SNMPユーザの設定が不完全です。 ● **other**—他の状態です。 SNMPユーザは、作成時にactiveになります。SNMPユーザを削除せずに一時的に無効にするには、SNMPセット操作を実行してステータスを変更します。
ACL	ACL番号です。 装置にアクセスするには、ACLでNMSのIPアドレスを許可する必要があります。 このフィールドはSNMPv3ユーザで、ACLが指定されたときのみ表示されます。ACL名フィールドと一緒に表示されません。
ACL name	ACL名です。 装置にアクセスするには、ACLでNMSのIPアドレスを許可する必要があります。 このフィールドはSNMPv3ユーザで、ACL名が指定されたときのみ表示されます。ACLフィールドと一緒に表示されません。

関連コマンド

snmp-agent usm-user v3

4.1.10 enable snmp trap updown

Syntax

enable snmp trap updown

undo enable snmp trap updown

デフォルト

有効

View

Interface view

定義済みユーザロール

network-admin

説明

enable snmp trap updown コマンドはインタフェースのリンク状態の通知を有効にします。

undo enable snmp trap updown コマンドはインタフェースのリンク状態の通知を無効にします。

状態が変更したとき、インタフェースで linkUp/linkDown の通知を作成する場合、**snmp-agent trap enable standard** [**linkdown** | **linkup**] *コマンドを使用してグローバルに linkUp/linkDown 通知機能を有効にする必要があります。

例

GigabitEthernet 1/0/1 で linkUp/linkDown の SNMP trap を 10.1.1.1 に送信することを有効にします。コミュニティ名は **public** を使用します。

<AC> system-view

[AC] snmp-agent trap enable

[AC] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] enable snmp trap updown

関連コマンド

- **snmp-agent target-host**

- **snmp-agent trap enable**

4.1.11 simulate snmp-trap

🕮 **メモ**:

simulate snmp-trap コマンドはソフトウェアバージョン7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

simulate snmp-trap all [**ifindex** *ifindex*]

simulate snmp-trap trap-node *name-string* [**context** *context-name*] [**variable-binding** { *variable-binding-name* { **hex** *hex-value* | **null-string** | *variable-binding-value* } } &<1-n>]

View

System view

定義済みユーザロール

network-admin

パラメータ

all：すべての SNMP 通知を指定します。

ifindex *ifindex*: SNMP 通知で送信される ifindex バインド（ノードとも呼ばれます）の値を指定します。値は、装置に存在する任意のインタフェースのインデックスにすることができます。このパラメータを指定しない場合、既存のインタフェースのインデックスを自動的に選択します。

trap-node *name-string*: SNMP 通知ノードを名称もしくは OID で指定します。このパラメータは大文字と小文字を区別しません。1～255 文字で既存のノードを指定してください。

context *context-name*: SNMP コンテキストを指定します。大文字と小文字を区別します。1～32 文字で指定してください。いくつかの通知ノードは異なるシナリオで使用できます。このパラメータは通知が引き起こされる特定のシナリオを示すために使用されます。

variable-binding { *variable-binding-name* { **hex** *hex-value* | **null-string** | *variable-binding-value* } } &<1-n> : SNMP 通知で送信される多様なバインドを指定します。

- *variable-binding-name*: 変数名もしくは OID を指定します。大文字と小文字は区別せず、通知ノードにサポートされる必要があります。
- **hex** *hex-value*: 16 進数形式で指定します。大文字と小文字は区別しません。1～255 の 16 進数で指定します。値は偶数にする必要があります。ベストプラクティスとして、16 進数以外の文字列として変数の値を設定します。ただし、変数値に文字列と

して直接表現できない特殊文字が含まれている場合は、値を 16 進数形式で設定します。変数バインド値を 16 進数形式で設定する場合は、最初に文字を ASCII コードに変換してから、ASCII コードを 16 進値に変換してください。

- **null-string**: 変数のバインドがヌル文字列であることを示します。
- *variable-binding-value*: 変数を 16 進数ではない形式で指定します。大文字と小文字を区別しません。1 から 255 の 16 進数文字ではない文字列です。
- &<1-n>: 最大 n 個の変数バインドを指定できることを示します。n の値は、通知ノードによって異なります。

説明

simulate snmp-trap コマンドは SNMP 通知送信をシミュレートします。

1) アプリケーションシナリオ
この機能は SNMP 通知機能が正常かどうか、通知設定が正しいか、NMS が通知を受信し正常に解析できるかどうかをテストできます。NMS が SNMP 通知を受信できない場合、問題を特定し、解決するためのトラブルシューティングを実施します。
2) 動作メカニズム
この機能を設定すると、装置は各ノードのメッセージを含む SNMP 通知を生成し、生成した通知を SNMP モジュールから送信します。
生成された SNMP 通知で送信されるノードは、以下のような値が割り当てられます。

- **数字タイプノード**—ノードの範囲の最小値を指定します。値の範囲がないノードには、0 が割り当てられます。
- **文字タイプノード**—値は Test です。文字数の指定要件がある場合、要件を満たすまで“Test”を切り捨てるか、繰り返します。
- **タイムスタンプタイプノード**—現在のシステム時刻を指定します。
- **IPv4 アドレスタイプノード**—“127.0.0.1”を指定します。
- **ビットタイプノード**—ノードのデフォルト値を使用します。デフォルト値がないノードの場合、ノードの設定範囲の最小値を使用します。
- **パスワードタイプノード**—値は“******”です。
- **オブジェクト識別子ノード**—値は通知の OID です。

同じイベントの通知とリカバリ通知は順番に送信されます。
通知ノードに同じ名前の変数が複数含まれている場合、同一の変数と値を順番に指定してください。変数に値を指定しない場合、上記の規則に基づいて値が割り当てられます。

この機能を有効にする前に、SNMP を有効にする必要があります。また、通知が送信されるようにするために、**snmp-agent target-host** コマンドを実行し、SNMP 通知のターゲットホストを指定してください。必要に応じて別の SNMP パラメータを設定してください。

このコマンドを設定するためのヘルプ情報を取得するには、コマンドの特定のパラメーター位置に「?」を入力します。たとえば、デバイスでサポートされているトラップ通知を取得するには、simulate snmp-trap trap-node ? のようにコマンドに「?」と入力します。

例

サポートされているすべての SNMP 通知の送信をシミュレートします。

<AC> system-view

[AC] simulate snmp-trap all

```
This operation will take long time and is resources-intensive. Continue?[Y/N]:y
```

linkUP SNMP 通知の送信をシミュレートします。

<AC> system-view

[AC] simulate snmp-trap trap-node linkUP

OID 1.3.6.1.6.3.1.1.5.4 (linkUp) を使用した SNMP 通知の送信をシミュレートします。OID 1.3.6.1.2.1.2.2.1.1 (ifIndex) の変数と OID 1.3.6.1.2.1.2.2.1.7 の変数 (ifAdminStatus) を送信するように通知を設定し、両方の変数の値を 1 に設定します。

<AC> system-view

[AC] simulate snmp-trap trap-node 1.3.6.1.6.3.1.1.5.4 variable-binding 1.3.6.1.2.1.2.2.1.1 1 1.3.6.1.2.1.2.2.1.7 1

関連コマンド

- **snmp-agent**
- **snmp-agent target-host**

4.1.12 snmp-agent

🕮 **メモ**:

- デフォルトコンフィグが設定された装置で **snmp-agent** コマンドを設定すると、**snmp-agent local-engineid** コマンドと **snmp-agent sys-info version v3** コマンドが自動的に追加されます。
- snmp の設定を変更した装置を **undo snmp-agent** コマンドによって無効した後、再度 snmp を有効にすると **undo** コマンド実行前の設定状態に戻ります。

Syntax

snmp-agent

undo snmp-agent

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent コマンドは SNMP エージェントを有効にします。

undo snmp-agent コマンドは SNMP エージェントを無効にします。

snmp-agent calculate-password を除く **snmp-agent** で始まるコマンドを実行するとき、SNMP エージェントは自動で有効になります。

例

SNMP エージェントを有効にします。

<AC> system-view

[AC] snmp-agent

4.1.13 snmp-agent calculate-password

Syntax

snmp-agent calculate-password *plain-password* **mode** { **3desmd5** | **3dessha** | **md5** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }

View

System view

定義済みユーザロール

network-admin

パラメータ

plain-password: プレーンテキスト形式のキーを指定します。大文字と小文字を区別する 1～64 文字の文字列です。

mode: **snmp-agent usm-user v3** コマンドで設定したのと同じ認証アルゴリズムと暗号化アルゴリズムを指定します。HMAC-MD5 は HMAC-SHA1 よりも計算が早いですが、HMAC-SHA1 は HMAC-MD5 よりもセキュリティ強度が高いです。

暗号化アルゴリズムは AES、3DES、DES の順番でセキュリティ強度が弱くなります。セキュリティ強度が強いアルゴリズムは計算が遅くなります。DES は一般的なセキュリティの要件を満たすのに十分です。

- **3desmd5**: HMAC-MD5 認証アルゴリズムと連携して使用される 3DES 認証キーのため、プライバシーキーをプレーンテキストから暗号テキストに変換します。
- **3dessha**: HMAC-SHA1 認証アルゴリズムと連携して使用される 3DES 認証キーのため、プライバシーキーをプレーンテキストから暗号テキストに変換します。

- **md5**: MD5 認証アルゴリズムと AES あるいは DES 暗号化アルゴリズムを使用して認証キーあるいは暗号化キーをプレーンテキストから暗号テキストに変換します。
- **sha**: SHA1 認証アルゴリズムと AES あるいは DES 暗号化アルゴリズムを使用して認証キーあるいは暗号化キーをプレーンテキストから暗号テキストに変換します。

local-engineid: キーの暗号化された形式を計算するためローカルエンジン ID を使用します。**snmp-agent local-engineid** コマンドでローカルエンジン ID を設定することができます。

specified-engineid *engineid*: キーの暗号化された形式を計算するためユーザ定義のエンジン ID を使用します。*engineid* は 16 進数の文字列で SNMP エンジン ID を指定します。文字列の長さは偶数で構成する必要があります。設定範囲は 10～64 です。すべて 0 あるいはすべて F の文字列は無効です。

説明

snmp-agent calculate-password コマンドを使用して、鍵の暗号化された形式を平文形式で計算します。

snmp-agent calculate-password コマンドを実行する前に SNMP エージェントが有効であることを確認してください。

セキュリティのため、**snmp-agent usm-user v3** コマンドで cipher キーワードを指定して SNMPv3 ユーザを作成するとき、**snmp-agent calculate-password** コマンドで生成された暗号化キーを使用します。

変換されたキーは変換のため、指定されたエンジン ID でのみ有効です。

例

プレーンテキスト authkey から変換された暗号テキストのダイジェストを計算するため、ローカルエンジンと HMAC-SHA1 アルゴリズムを使用します。

<AC> system-view

[AC] snmp-agent calculate-password authkey mode sha local-engineid

```
The encrypted key is: 09659EC5A9AE91BA189E5845E1DDE0CC
```

関連コマンド

- **snmp-agent local-engineid**
- **snmp-agent usm-user v3**

4.1.14 snmp-agent community

Syntax

snmp-agent community { **read** | **write** } [**simple** | **cipher**] *community-name* [**mib-view** *view-name*] [**acl** { *acl-number* | **name** *acl-name* }] *

undo snmp-agent community [**cipher**] *community-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

read: 指定されたコミュニティを MIB オブジェクトへの読み出し専用のアクセス権限に割り当てます。読み出し専用コミュニティは MIB 情報を問い合わせることのみ可能です。

write: 指定されたコミュニティを MIB オブジェクトへの読み出し、書き込みのアクセス権限に割り当てます。読み出し専用コミュニティは MIB 情報を設定することができます。

simple: プレーンテキストのコミュニティを設定します。セキュリティのため、コミュニティは暗号テキストで保存されます。

cipher: 暗号テキストのコミュニティを設定し、暗号テキストで保存します。

community-name: コミュニティを設定します。大文字、小文字を区別します。プレーンテキストの設定範囲は 1～32 文字です。暗号テキストの設定範囲は 33～73 文字です。バックスラッシュの後にエスケープ文字として文字列を入力します。

mib-view *view-name*: コミュニティで有効な MIB view を指定します。*view-name* は MIB view の名前を示します。設定範囲は 1～32 文字です。MIB view はアクセス可能な MIB オブジェクトの一式を示します。MIB view を指定しない場合、コミュニティはデフォルト MIB view の **ViewDefault** の MIB オブジェクトにアクセスできます。

acl *ipv4-acl-number*: 標準 IPv4 ACL 番号を指定します。設定範囲は 2000～2999 です。

name *ipv4-acl-name*: 標準 IPv4 ACL 名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

acl ipv6 *ipv6-acl-number*: 標準 IPv6 ACL 番号を指定します。設定範囲は 2000～2999 です。

name *ipv6-acl-name*: 標準 IPv6 ACL 名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

説明

snmp-agent community コマンドは SNMPv1 あるいは SNMPv2c コミュニティを設定します。

undo snmp-agent community コマンドは SNMPv1 あるいは SNMPv2c コミュニティを削除します。

SNMP コミュニティは NMS と SNMP エージェントの一式を構成し、コミュニティによって識別します。NMS と SNMP エージェントは互いにに称するため、同じコミュニティを使用する必要があります。

通常、**public** は読み込み専用のコミュニティとして使用され、**private** は読み込み、書き込みコミュニティとして使用します。セキュリティを改善するため、SNMP コミュニティに **public** と **private** 以外の名前を割り当てます。

SNMP コミュニティで MIB オブジェクトにアクセスを制御するため、以下のモードを使用することができます。

- **VACM（View ベースアクセス制御モデル）**—VACM モードは MIB view を SNMP コミュニティに割り当てることで MIB オブジェクトへのアクセスを制御します。

VACM モードは NMS から MIB オブジェクトのアクセス権のみを必要とします。

snmp-agent community コマンドを使用して 10 個の SNMP コミュニティを作成することができます。コミュニティ名が同一で、ほかのパラメータが異なる設定を指定するため、コマンドを複数回実行する場合、最後に実行した設定が適用されます。

プレーンテキストでコミュニティを設定し、保存する場合、**simple** あるいは **cipher** を指定しないでください。

ACL は不正な NMS をフィルタするために使用します。

- ACL を指定しない、指定した ACL が存在しない、ACL にルールがない場合、すべての NMS は SNMP エージェントにアクセスすることができます。
- ACL を指定し､ACL にルールが存在する場合､ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

ACL の詳細はオペレーションマニュアルのセクション 8 *ACL and QoS “ACL”* を参照してください。

snmp-agent usm-user { v1 | v2c }コマンド、**snmp-agent group { v1 | v2c }**コマンドを使用して SNMP コミュニティを作成することができます。2 つのコマンドは SNMPv1 あるいは SNMPv2c ユーザ、ユーザが割り当てられるグループを作成します。システムは自動で SNMPv1 あるいは SNMPv2c ユーザ名を使用して SNMP コミュニティを制御します。

例

プレーンテキストで読み込み専用のコミュニティ readaccess を作成します。SNMPv1 あるいは SNMPv2c の NMS はデフォルト view の ViewDefault の MIB オブジェクトを読むため、コミュニティ readaccess を使用します。

<AC> system-view

[AC] snmp-agent sys-info version v1 v2c

[AC] snmp-agent community read simple readaccess

プレーンテキストで読み込み、書き込みコミュニティ writeaccess を作成します。SNMPv2c の IP アドレスが 1.1.1.1 の NMS はデフォルト view の ViewDefault の MIB オブジェクトを読み書きするため、コミュニティ writeaccess を使用します。

<AC> system-view

[AC] acl basic 2001

[AC-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0.0.0.0

[AC-acl-ipv4-basic-2001] rule deny source any

[AC-acl-ipv4-basic-2001] quit

[AC] snmp-agent sys-info version v2c

[AC] snmp-agent community write simple writeaccess acl 2001

プレーンテキストで読み込み、書き込みコミュニティ writeaccess を作成します。SNMPv2c の IP アドレスが 1.1.1.2 の NMS はデフォルト view の ViewDefault の MIB オブジェクトを読み書きするため、コミュニティ writeaccess を使用します。

<AC> system-view

[AC] acl basic name testacl

[AC-acl-ipv4-basic-testacl] rule permit source 1.1.1.2 0.0.0.0

[AC-acl-ipv4-basic-testacl] rule deny source any

[AC-acl-ipv4-basic-testacl] quit

[AC] snmp-agent sys-info version v2c

[AC] snmp-agent community write simple writeaccess acl name testacl

プレーンテキストで読み込み、書き込みコミュニティ wr-sys-acc を作成します。SNMPv1 あるいは SNMPv2c の NMS はシステムサブツリー（OID 1.3.6.1.2.1.1）の MIB オブジェクトを読み書きするため、コミュニティ wr-sys-acc を使用します。

<AC> system-view

[AC] snmp-agent sys-info version v1 v2c

[AC] undo snmp-agent mib-view ViewDefault

[AC] snmp-agent mib-view included test system

[AC] snmp-agent community write simple wr-sys-acc mib-view test

関連コマンド

- **display snmp-agent community**
- **snmp-agent mib-view**

4.1.15 snmp-agent group

Syntax

SNMPv1、SNMPv2c：

snmp-agent group { **v1** | **v2c** } *group-name* [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] *

undo snmp-agent group { **v1** | **v2c** } *group-name*

SNMPv3：

snmp-agent group v3 *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] *

undo snmp-agent group v3 *group-name* [**authentication** | **privacy**]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

v1: SNMPv1 を指定します。

v2c: SNMPv2c を指定します。

v3: SNMPv3 を指定します。

group-name: SNMP グループ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

authentication: SNMPv3 グループでプライバシーなしのモデルを指定します。

privacy: SNMPv3 グループでプライバシーセキュリティのモデルを指定します。

read-view *view-name*: 読み込み専用の MIB view を指定します。*view-name* は MIB view の名前を示します。設定範囲は 1～32 文字です。読み込み専用の MIB view を指定しない場合、SNMP グループはデフォルト MIB view の **ViewDefault** の MIB オブジェクトに問い合わせることができます。

write-view *view-name*: 読み込み、書き込みの MIB view を指定します。*view-name* は MIB view の名前を示します。設定範囲は 1～32 文字です。読み込み、書き込みの MIB view を指定しない場合、SNMP グループは SNMP エージェントの MIB オブジェクトを設定することができません。

notify-view *view-name*: notify の MIB view を指定します。*view-name* は MIB view の名前を示します。設定範囲は 1～32 文字です。SNMP エージェントは notify view に含まれる MIB オブジェクトのため、指定されたグループのみのユーザに通知を送信します。notify の MIB view を指定しない場合、SNMP グループは指定されたグループのユーザに通知を送信しません。

acl *ipv4-acl-number*: 標準 ACL 番号を指定します。設定範囲は 2000～2999 です。

name *ipv4-acl-name*: 標準 ACL 名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

説明

snmp-agent group コマンドは SNMP グループを作成します。

undo snmp-agent group コマンドは SNMP グループを削除します。

このコマンドを実行できるのは、ネットワーク管理者またはレベル 15 のユーザロールを持つユーザだけです。これらのロールにこのコマンドまたは SNMP 機能のコマンドへのアクセスが許可されていても、他のユーザロールを持つユーザはこのコマンドを実行できません。

SNMP グループのすべてのユーザはグループのセキュリティモデルとアクセス権限を共有します。

SNMP グループのすべてのユーザはセキュリティモデルとグループのアクセス権限を共有します。

SNMPv1 グループ、SNMPv2c グループ、SNMPv3 グループを含んで 20 個の SNMP グループを作成することができます。

グループのすべての SNMPv3 ユーザは同じセキュリティモデルを共有しますが、異なる認証と暗号化キーの設定を使用することができます。ユーザのセキュリティモデルを実装し、SNMP 通信の失敗を防ぐため、グループのセキュリティモデルの設定とユーザのセキュリティのキーの設定が、表 4-6 に従い、NMS の設定に一致していることを確認してください。

表 4-6 異なるセキュリティモデルの標準セキュリティの設定要件

セキュリティモデル	グループのセキュリティモデルのキーワード	ユーザのセキュリティのキーの設定	補足
プライバシーセキュリティあり、認証	**privacy**	認証キー、暗号化キー	認証キーあるいは暗号化キーが設定されていない場合、SNMP の通信は失敗します。
プライバシーセキュリティなし、認証	**authentication**	認証キー	認証キーが設定されていない場合、SNMP の通信は失敗します。ユーザの暗号化キー（ある場合）は影響しません。
プライバシーセキュリティなし、認証なし	**authentication**、**privacy** のどちらもありません。	なし	認証キーと暗号化キーが設定されても影響ありません。

ユーザ、グループのため、ACL は不正な NMS をフィルタするために使用します。ユーザ、グループの両方で ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

- ACL を指定しない、指定した ACL が存在しない、ACL にルールがない場合、すべての NMS は SNMP エージェントにアクセスすることができます。
- ACL を指定し、ACL にルールが存在する場合、ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

ACL の詳細はオペレーションマニュアルのセクション 8 *ACL and QoS "ACL"* を参照してください。

例

SNMPv3 グループ **group1** を作成します。

<Switch> system-view

[Switch] snmp-agent group v3 group1

関連コマンド

- **display snmp-agent group**
- **snmp-agent mib-view**
- **snmp-agent usm-user**

4.1.16 snmp-agent local-engineid

🕮 **メモ**:

デフォルトコンフィグが設定された装置で snmp を有効にすると、**snmp-agent local-engineid** コマンドが自動的に追加されます。

Syntax

snmp-agent local-engineid *engineid*

undo snmp-agent local-engineid

デフォルト

ローカルエンジン ID は company ID と device ID の組み合わせです。Device ID は製品によって異なり、IP アドレス、MAC アドレス、ユーザ定義の 16 進数の文字列などです。

View

System view

定義済みユーザロール

network-admin

パラメータ

engineid: 16 進数の文字列で SNMP エンジン ID を指定します。文字列の長さは偶数で構成する必要があります。設定範囲は 10～64 です。すべて 0 あるいはすべて F の文字列は無効です。

説明

snmp-agent local-engineid コマンドはローカル SNMP エージェントの SNMP エンジン ID を変更します。

undo snmp-agent local-engineid コマンドはデフォルトに戻します。

SNMP エンジン ID は SNMP が管理するネットワークで SNMP エンティティを固有に識別します。ローカル SNMP エンジン ID は通信の問題を防ぐため、SNMP が管理するネットワーク内で一意であることを確認してください。

SNMPv3 ユーザが設定されている場合、必要に応じてローカル SNMP エンジン ID を変更してください。変更すると設定した SNMPv3 ユーザ名と暗号化したキーを無効にすることができます。

例

ローカルエンジン ID を 123456789A に変更します。

<AC> system-view

[AC] snmp-agent local-engineid 123456789A

関連コマンド

- **display snmp-agent local-engineid**
- **snmp-agent usm-user**

4.1.17 snmp-agent log

Syntax

snmp-agent log { **all** | **authfail** | **get-operation** | **set-operation** }

undo snmp-agent log { **all** | **authfail** | **get-operation** | **set-operation** }

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

all: SNMP 認証失敗、Get オペレーション、Set オペレーションのロギングを有効にします。

authfail: SNMP 認証の失敗のロギングを有効にします。

get-operation: SNMP Get オペレーションのロギングを有効にします。

set-operation: SNMP Set オペレーションのロギングを有効にします。

説明

snmp-agent log コマンドは SNMP オペレーションのロギングを有効にします。

undo snmp-agent log コマンドは SNMP オペレーションのロギングを無効にします。

NMS のふるまいを検査するため、SNMP エージェントで実行された SNMP オペレーションを記録することができます。SNMP エージェントはログデータを information center に送信します。必要に応じて宛先にデータを出力するように Information Center を設定することができます。

例

SNMP Get オペレーションのロギングを有効にします。

<AC> system-view

[AC] snmp-agent local-engineid 123456789A

SNMP Set オペレーションのロギングを有効にします。

<AC> system-view

[AC] snmp-agent log set-operation

SNMP 認証失敗のロギングを有効にします。

<AC> system-view

[AC] snmp-agent log authfail

4.1.18 snmp-agent mib-view

Syntax

snmp-agent mib-view { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]

undo snmp-agent mib-view *view-name*

デフォルト

SNMP エージェントが有効なとき、システムは **ViewDefault** view を作成します。デフォルト MIB view では **iso** サブツリーのすべての MIB オブジェクトは **snmpUsmMIB**、**snmpVacmMIB**、**snmpModules.18** サブツリーを除いてアクセス可能です。

View

System view

定義済みユーザロール

network-admin

パラメータ

excluded: 指定した MIB サブツリーのすべてのノードへのアクセスを拒否します。

included: 指定した MIB サブツリーのすべてのノードへのアクセスを許可します。
view-name: view 名を指定します。設定範囲は 1～32 文字です。

oid-tree: ルートノードの OID（たとえば、**1.3.6.1.2.1.1**）あるいはオブジェクト名（たとえば、**system**）によって MIB サブツリーを指定します。oid-tree 引数は、1～255 文字の文字列です。OID は MIB ツリーのオブジェクトを固有に識別するドットで区切られた 10 進数の数字です。

mask *mask-value*: MIB サブツリーのマスクを指定します。16 進数です。マスク長は 1～32 の偶数にする必要があります。

説明

snmp-agent mib-view コマンドは MIB view を作成あるいはアップデートします。

undo snmp-agent mib-view コマンドは MIB view を削除します。

MIB view は、アクセス制限のある MIB オブジェクトの集合（あるいは MIB オブジェクト階層）を示し、view 名によって識別されます。MIB view に含まれる MIB オブジェクトはアクセス可能ですが、MIB view から除外されている MIB オブジェクトはアクセスできません。

各 *view-name oid-tree* は view のレコードを示します。異なる MIB サブツリーのマスクで複数回、同一のレコードを指定する場合、最後に行った設定が適用されます。

システムは、最大 20 個の MIB view のレコードを格納できます。4 つのデフォルト MIB view レコードに加えて、最大 16 個の MIB view レコードを作成できます。**undo snmp-agent mib-view** コマンドを使用してデフォルトビューを削除すると、最大 20 個の MIB view レコードを作成できます。

デフォルト MIB view を削除する場合には注意してください。デフォルト view を使用する NMS から装置の MIB オブジェクトにアクセスできなくなります。

例

mibtest view に mib-2（OID 1.3.6.1.2.1）サブツリーを含め、この view から **system** サブツリーを除外します。

<AC> system-view

[AC] snmp-agent sys-info version v1

[AC] snmp-agent mib-view included mibtest 1.3.6.1.2.1

[AC] snmp-agent mib-view excluded mibtest system

[AC] snmp-agent community read public mib-view mibtest

コミュニティ **public** の SNMPv1 の NMS は **mib-2** サブツリーのオブジェクトに問い合わせすることができますが、**system** サブツリーの他のオブジェクト（たとえば、**sysDescr** あるいは **sysObjectID** ノード）は問い合わせすることができません。

関連コマンド

- **display snmp-agent mib-view**
- **snmp-agent group**

4.1.19 snmp-agent packet max-size

Syntax

snmp-agent packet max-size *byte-count*

undo snmp-agent packet max-size

デフォルト

1500 バイト

View

System view

定義済みユーザロール

network-admin

パラメータ

byte-count: SNMP エージェントが送受信できる SNMP パケットの最大サイズを指定します。設定範囲は 484～17940 バイトです。

説明

snmp-agent packet max-size コマンドは SNMP エージェントが送受信できる SNMP パケットの最大サイズを設定します。

undo snmp-agent packet max-size コマンドはデフォルトに戻します。

NMS へのパス上の装置がパケットのフラグメンテーションをサポートしていない場合、大きいサイズのパケットが廃棄されないようにするため、SNMP パケットサイズを制限します。通常のネットワークではデフォルトの設定で十分です。

例

SNMP パケットの最大サイズを 1024 バイトに設定します。

<AC> system-view

[AC] snmp-agent packet max-size 1024

4.1.20 snmp-agent { inform | trap } source

Syntax

snmp-agent { **inform** | **trap** } **source** *interface-type interface-number*

undo snmp-agent { **inform** | **trap** } **source**

デフォルト

SNMP エージェントはルートの送信インタフェースの IP アドレスを使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

inform: inform を指定します。

trap: trap を指定します。

interface-type interface-number: インタフェースのタイプと番号を指定します。*interface-number* 引数は、メインインタフェース番号を指定します。

説明

snmp-agent { **inform** | **trap** } **source** コマンドは SNMP エージェントによって送信される inform あるいは trap の送信元 IP アドレスを指定します。

undo snmp-agent { **inform** | **trap** } **source** コマンドはデフォルトに戻します。

snmp-agent source コマンドは、送信インタフェースに関わらず、SNMP エージェントがすべての SNMP の inform あるいは trap の送信元 IP アドレスとして、インタフェースまたはサブインタフェースのプライマリ IP アドレスを使用することを有効にします。NMS は SNMP エージェントによって送信されたすべての inform あるいは trap をフィルタするため、この IP アドレスを使用します。

指定されたインタフェースが作成され、有効な IP アドレスが割り当てられていることを確認してください。インタフェースが作成されていない場合、設定は適用されません。指定したインタフェースに有効な IP アドレスが割り当てられたのち、設定が適用されます。

例

SNMP trap の送信元アドレスとして、GigabitEthernet 1/0/1 のプライマリ IP アドレスを設定します。

<AC> system-view

[AC] snmp-agent trap source gigabitethernet 1/0/1

SNMP inform の送信元アドレスとして、GigabitEthernet 1/0/2 のプライマリ IP アドレスを設定します。

<AC> system-view

[AC] snmp-agent inform source gigabitethernet 1/0/2

関連コマンド

- **snmp-agent target-host**
- **snmp-agent trap enable**

4.1.21 snmp-agent sys-info contact

Syntax

snmp-agent sys-info contact *sys-contact*

undo snmp-agent sys-info contact

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

sys-contact: システム連絡先を指定します。設定範囲は 1～255 文字です。

説明

snmp-agent sys-info contact コマンドはシステム連絡先を設定します。

undo snmp-agent sys-info contact コマンドはデフォルトに戻します。

システム管理の連絡先と管理者を設定します。

例

システム連絡先を **Dial System Operator # 27345** に指定します。

<AC> system-view

[AC] snmp-agent sys-info contact Dial System Operator # 27345

関連コマンド

display snmp-agent sys-info

4.1.22 snmp-agent sys-info location

Syntax

snmp-agent sys-info location *sys-location*

undo snmp-agent sys-info location

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

sys-location: システム所在地を指定します。設定範囲は 1～255 文字です。

説明

snmp-agent sys-info location コマンドはシステム所在地を設定します。

undo snmp-agent sys-info location コマンドはデフォルトに戻します。

システム管理の装置と管理者の所在地を設定します。

例

システム所在地を **Room524-row1-3** に設定します。

<AC> system-view

[AC] snmp-agent sys-info location Room524-row1-3

関連コマンド

display snmp-agent sys-info

4.1.23 snmp-agent sys-info version

🕮 **メモ**:

SNMP 機能を有効にすると、自動的に **snmp-agent sys-info version v3** が設定されます。SNMPv3 が必要ない場合、**undo snmp-agent sys-info version v3** コマンドを実行してください。

Syntax

snmp-agent sys-info version { **all** | { **v1** | **v2c** | **v3** } * }

undo snmp-agent sys-info version { **all** | { **v1** | **v2c** | **v3** } * }

デフォルト

SNMPv3

View

System view

定義済みユーザロール

network-admin

パラメータ

all: SNMPv1、SNMPv2c、SNMPv3 を指定します。

v1: SNMPv1 を指定します。

v2c: SNMPv2c を指定します。

v3: SNMPv3 を指定します。

説明

snmp-agent sys-info version コマンドは SNMP のバージョンを有効にします。

undo snmp-agent sys-info version コマンドは SNMP のバージョンを無効にします。

NMS が SNMP エージェントと正常に通信するため、SNMP エージェントは NMS と同じ SNMP のバージョンを設定します。

例

SNMPv3 を有効にします。

<AC> system-view

[AC] snmp-agent sys-info version v3

関連コマンド

display snmp-agent sys-info

4.1.24 snmp-agent target-host

Syntax

snmp-agent target-host inform address udp-domain { *ip-address* } [**udp-port** *port-number*] **params securityname** *security-string* { **v2c** | **v3** [**authentication** | **privacy**] }

snmp-agent target-host trap address udp-domain { *ip-address* } [**udp-port** *port-number*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

undo snmp-agent target-host { **trap** | **inform** } **address udp-domain** { *ip-address* } **params securityname** *security-string*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

inform: inform として通知を送信します。

trap: trap として通知を送信します。

address: SNMP 通知の宛先アドレスを指定します。

udp-domain: トランスポートプロトコルとして UDP を指定します。

ip-address: SNMP 通知の宛先として、ターゲットホストの IPv4 アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1～253 文字です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含むことができます。ホスト名を指定する場合、ターゲットホストの IPv4 アドレスは、取得することができます。

udp-port *port-number*: SNMP 通知の UDP ポートを指定します。指定しない場合、UDP ポート 162 が使用されます。

params securityname *security-string*: 認証パラメータを指定します。*security-string* は SNMPv1 コミュニティ、SNMPv2c コミュニティ、あるいは SNMPv3 ユーザ名を指定します。設定範囲は 1～32 文字です。

v1: SNMPv1 を指定します。

v2c: SNMPv2c を指定します。

v3: SNMPv3 を指定します。

- **authentication**: プライバシーセキュリティなしで認証するようにセキュリティモデルを指定します。SNMPv3 ユーザを作成したとき認証キーを指定する必要があります。
- **privacy**: プライバシーセキュリティありで認証するようにセキュリティモデルを指定します。SNMPv3 ユーザを作成したとき認証キーと暗号化キーを指定する必要があります。

説明

snmp-agent target-host コマンドは SNMP 通知（inform あるいは trap）をホストに送信するため、SNMP エージェントを設定します。

undo snmp-agent target-host コマンドは SNMP 通知のターゲットホストを削除します。

複数の SNMP 通知のターゲットホストを指定することができます。

SNMP エージェントは SNMP 通知のため、ターゲットホストの UDP ポートと同一のポートを使用する必要があります。通常、MIB ブラウザのような NMS は SNMP 通知のために、SNMP プロトコルで定義された UDP ポート 162 を使用します。

v1、**v2c**、**v3** を指定しない場合、SNMPv1 が使用されます。ホストが通知を受信できるように、SNMP エージェントは、ターゲットホストの SNMP のバージョンと同一のバージョンを使用することを確認してください。

authentication あるいは **privacy** の両方を指定しない場合、セキュリティモデルはプライバシーセキュリティなし、認証なしです。

例

ユーザ **public** の 10.1.1.1 に SNMPv3 の trap を送信するため、SNMP エージェントを設定します。

<AC> system-view

[AC] snmp-agent trap enable standard

[AC] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public v3

関連コマンド

- **snmp-agent { inform | trap } source**
- **snmp-agent trap enable**
- **snmp-agent trap life**

4.1.25 snmp-agent trap enable

Syntax

snmp-agent trap enable [**configuration** | *protocol* | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] * | **system**]

undo snmp-agent trap enable [**configuration** | *protocol* | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] * | **system**]

デフォルト

SNMP configuration 通知、standard 通知、system 通知は有効です。他の SNMP 通知はモジュールによって変わります。

View

System view

定義済みユーザロール

network-admin

パラメータ

configuration: configuration 通知を指定します。configuration 通知が有効である場合、システムはカレントコンフィグレーションとスタートアップコンフィグレーションを 10 分毎に変更点を確認し、最新の変更の通知を作成します。

protocol: SNMP 通知が有効なモジュールを指定します。このパラメータの詳細は各モジュールのコマンドマニュアルを参照してください。

standard: standard 通知を指定します。

表 4-7 Standard SNMP 通知

キーワード	定義
authentication	NMSがSNMPエージェントへの認証に失敗したとき、認証失敗通知を送信します。
coldstart	装置が再起動したときに通知を送信します。
linkdown	ポートのリンクがダウンしたときに通知を送信します。
linkup	ポートのリンクがアップしたときに通知を送信します。
warmstart	SNMPエージェントが再起動したときに通知を送信します。

system: システム時間が変更された、システムが再起動した、あるいはメインのシステムソフトウェアイメージが有効でないときに system 通知を指定します。

説明

snmp-agent trap enable コマンドはグローバルで SNMP 通知を有効にします。

undo snmp-agent trap enable コマンドはグローバルで SNMP 通知を無効にします。

snmp-agent trap enable コマンドを使用する場合、**trap** キーワードが使用されていても、inform と trap のそれぞれを生成します。

snmp-agent target-host コマンドを使用すると、装置が通知を inform または trap としてホストに送信できるようになります。

パラメータを指定しない場合、**snmp-agent trap enable** コマンドあるいは **undo** コマンドは装置でサポートされるすべての SNMP 通知を有効あるいは無効にします。

例

SNMP 認証の失敗の Notification をコミュニティ **public** で 10.1.1.1 に送信するように SNMP エージェントを有効にします。

<AC> system-view

[AC] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public

[AC] snmp-agent trap enable standard authentication

関連コマンド

snmp-agent target-host

4.1.26 snmp-agent trap if-mib link extended

Syntax

snmp-agent trap if-mib link extended

undo snmp-agent trap if-mib link extended

デフォルト

SNMP エージェントは標準 linkUp/linkDown 通知を送信します。

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap if-mib link extended コマンドは拡張 linkUp/linkDown 通知を送信するように SNMP エージェントを設定します。

undo snmp-agent trap if-mib link extended コマンドはデフォルトに戻します。

拡張 linkUp/linkDown 通知は、早急に故障個所を識別するため、標準 linkUp/linkDown 通知にインタフェースの説明とインタフェースのタイプを追加します。

このコマンドを使用するとき、NMS が拡張 linkUp/linkDown 通知をサポートしていることを確認してください。

例

拡張 linkUp/linkDown 通知を送信するように SNMP エージェントを設定します。

<AC> system-view

[AC] snmp-agent trap if-mib link extended

4.1.27 snmp-agent trap life

Syntax

snmp-agent trap life *seconds*

undo snmp-agent trap life

デフォルト

120 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

seconds: ライフタイムを指定します。設定範囲は 1～2592000 秒です。

説明

snmp-agent trap life コマンドは SNMP 通知キューの通知のライフタイムを設定します。

undo snmp-agent trap life コマンドはデフォルトの通知のライフタイムに戻します。

衝突が発生すると、SNMP エージェントはキューに通知をバッファします。通知のライフタイムはキューに保持しておく期間を設定します。ライフタイムが終了したとき notification は削除されます。

例

SNMP 通知のライフタイムを 60 秒に設定します。

<AC> system-view

[AC] snmp-agent trap life 60

関連コマンド

- **snmp-agent target-host**
- **snmp-agent trap enable**
- **snmp-agent trap queue-size**

4.1.28 snmp-agent trap log

Syntax

snmp-agent trap log

undo snmp-agent trap log

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap log コマンドは SNMP 通知のロギングを有効にします。

undo snmp-agent trap log コマンドは SNMP 通知のロギングを無効にします。

通知のトラッキングを行うため、SNMP エージェントによって送信された SNMP 通知を記録するため、SNMP 通知のロギングを使用します。SNMP エージェントは Information Center にログを送信します。必要に応じて宛先にログを出力するように Information Center を設定することができます。

例

SNMP 通知のロギングを有効にします。

<AC> system-view

[AC] snmp-agent trap log

4.1.29 snmp-agent trap queue-size

Syntax

snmp-agent trap queue-size *size*

undo snmp-agent trap queue-size

デフォルト

100

View

System view

定義済みユーザロール

network-admin

パラメータ

size: SNMP 通知のキューが保持できる通知の最大数を指定します。設定範囲は 1～1000 です。

説明

snmp-agent trap queue-size コマンドは SNMP 通知のキューのサイズを設定します。

undo snmp-agent trap queue-size コマンドはデフォルトのキューのサイズに戻します。

衝突が発生したとき、SNMP エージェントはキューに通知をバッファします。SNMP 通知のキューのサイズは SNMP 通知のキューが保持できる通知の最大数を設定します。キューのサイズが上限に到達したとき、新しい通知のために、古い通知が廃棄されます。

例

SNMP 通知のキューのサイズを 200 に設定します。

<AC> system-view

[AC] snmp-agent trap queue-size 200

関連コマンド

- **snmp-agent target-host**
- **snmp-agent trap enable**
- **snmp-agent trap life**

4.1.30 snmp-agent usm-user { v1 | v2c }

Syntax

snmp-agent usm-user { **v1** | **v2c** } *user-name group-name* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] *

undo snmp-agent usm-user { **v1** | **v2c** } *user-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

v1: SNMPv1 を指定します。

v2c: SNMPv2c を指定します。

user-name: SNMP ユーザ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

group-name: SNMPv1 あるいは SNMPv2c のグループ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。グループは、すでに作成されたものでも指定できます。グループが作成されていない場合、グループを作成した後、適用されます。

acl *ipv4-acl-number*: 標準 ACL 番号を指定します。設定範囲は 2000～2999 です。

name *ipv4-acl-name*: 標準 ACL 名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

説明

snmp-agent usm-user { **v1** | **v2c** }コマンドは SNMPv1 あるいは SNMPv2c グループにユーザを追加します。

undo snmp-agent usm-user { **v1** | **v2c** }コマンドは SNMPv1 あるいは SNMPv2c グループからユーザを削除します。

コマンドはユーザロールが network-admin あるいは level-15 のみ実行することができます。これらのロールがほかのユーザロールでは SNMP 機能やコマンドの使用を許可されたとしても実行することができません。

SNMPv1 あるいは SNMPv2c では NMS エージェントはコミュニティ名を使用して互いに認証します。SNMPv3 ではユーザ名を使用して互いに認証します。

以下のどちらかの方法を使用して SNMPv1 あるいは SNMPv2c コミュニティを作成することができます。

- **snmp-agent community** コマンドを実行します。
- SNMPv1 あるいは SNMPv2c ユーザ、ユーザに割り当てられるグループを作成するため、**snmp-agent usm-user { v1 | v2c }**コマンド、**snmp-agent group { v1 | v2c }** コマンドを実行します。システムは SNMPv1 あるいは SNMPv2c のユーザ名を使用して自動で SNMP コミュニティを作成します。

ユーザ、グループのために ACL は不正な NMS をフィルタするために使用します。ユーザ、グループの両方で ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

- ACL を指定しない、指定した ACL が存在しない、ACL にルールがない場合、すべての NMS は SNMP エージェントにアクセスすることができます。
- ACL を指定し､ACL にルールが存在する場合､ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

ACL の詳細はオペレーションマニュアルのセクション 8 *ACL and QoS "ACL"* を参照してください。

例

NMS が SNMPv2c を使用するため、SNMPv2c グループ **readCom** にユーザ **userv2c** を追加します。読み込み専用のコミュニティ **userv2c** を使用して装置にアクセスします。

<AC> system-view

[AC] snmp-agent sys-info version v2c

[AC] snmp-agent group v2c readCom

[AC] snmp-agent usm-user v2c userv2c readCom

IP アドレス 1.1.1.1 の NMS が SNMPv2c を使用するため、SNMPv2c グループ **readCom** にユーザ **userv2c** を追加します。読み込み専用のコミュニティ **userv2c** を使用して装置にアクセスします。

<AC> system-view

[AC] acl basic 2001

[AC-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0.0.0.0

[AC-acl-ipv4-basic-2001] rule deny source any

[AC-acl-ipv4-basic-2001] quit

[AC] snmp-agent sys-info version v2c

[AC] snmp-agent group v2c readCom

[AC] snmp-agent usm-user v2c userv2c readCom acl 2001

IP アドレス 1.1.1.2 の NMS が SNMPv2c を使用するため、SNMPv2c グループ **readCom** にユーザ **userv2c** を追加します。読み込み専用のコミュニティ **userv2c** を使用して装置にアクセスします。

[AC] acl basic name testacl

[AC-acl-ipv4-basic-testacl] rule permit source 1.1.1.2 0.0.0.0

[AC-acl-ipv4-basic-testacl] rule deny source any

[AC-acl-ipv4-basic-testacl] quit

[AC] snmp-agent sys-info version v2c

[AC] snmp-agent group v2c readCom

[AC] snmp-agent usm-user v2c userv2c readCom acl name testacl

関連コマンド

- **display snmp-agent community**
- **snmp-agent community**
- **snmp-agent group**

4.1.31 snmp-agent usm-user v3

Syntax

snmp-agent usm-user v3 *user-name group-name* [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **aes128 | 3des** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] *

undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

user-name: SNMPv3 ユーザ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

group-name: SNMPv3 のグループ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

cipher: 暗号化された形式で認証キーと暗号化キーを指定します。キーは暗号化された形式のダイジェストに変換され、デバイスに保存されます。

simple: 認証キーと平文の暗号化キーを指定します。キーは暗号化された形式のダイジェストに変換され、デバイスに保存されます。

authentication-mode: 認証アルゴリズムを指定します。キーワードを指定しないと、システムは認証を実行しません。認証アルゴリズムの詳細については、オペレーションマニュアルのセクション 9 *セキュリティ "IPSec"* を参照してください。

- **md5**: HMAC-MD5 認証アルゴリズムを指定します。
- **sha**: HMAC-SHA1 認証アルゴリズムを指定します。

auth-password: プレーンテキストまたは認証キーを指定します。大文字、小文字を区別します。

- プレーンテキストの設定範囲は 1～64 文字です。数字、大文字、小文字、記号を含む必要があります。
- キーの暗号テキストは **snmp-agent calculate-password** コマンドで計算されます。

privacy-mode: 暗号アルゴリズムを指定します。指定しない場合、暗号を行いません。

- **aes128**: 168 ビットのキーを使用して AES アルゴリズムを指定します。
- **3des**: 128 ビットのキーを使用して 3DES アルゴリズムを指定します。
- **des56:** 56 ビットのキーを使用して DES アルゴリズムを指定します。

priv-password: プレーンテキストまたは暗号キーを指定します。大文字、小文字を区別します。

- プレーンテキストの設定範囲は 1～64 文字です。数字、大文字、小文字、記号を含む必要があります。
- キーの暗号テキストは **snmp-agent calculate-password** コマンドで計算されます。

acl *ipv4-acl-number*: 標準 ACL 番号を指定します。設定範囲は 2000～2999 です。

name *ipv4-acl-name*: 標準 ACL 名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

local: ローカル SNMP エンジンを指定します。デフォルトでは、SNMPv3 ユーザはローカル SNMP エンジンに関連付けられています。

engineid *engineid-string*: 16 進数の文字列で SNMP エンジン ID を指定します。文字列の長さは偶数で構成する必要があります。設定範囲は 10～64 です。すべて 0 あるいはすべて F の文字列は無効です。ローカルエンジンの ID を変更した後、既存の SNMPv3 ユーザと暗号化されたキーは無効になります。無効なユーザ名を削除する場合、**undo snmp-agent usm-user v3** コマンドでユーザ名にエンジン ID を指定してください。

再度設定を行う必要があります。

説明

snmp-agent usm-user v3 コマンドは SNMPv3 ユーザを作成します。

undo snmp-agent usm-user v3 コマンドは SNMPv3 グループからユーザを削除します。

コマンドはユーザロールが network-admin あるいは level-15 のみ実行することができます。これらのロールがほかのユーザロールでは SNMP 機能やコマンドの使用を許可されたとしても実行することができません。

SNMPv3 ユーザで MIB オブジェクトにアクセスを制御するため、以下のモードを使用することができます。

- **VACM（View ベースアクセス制御モデル）**—VACM モードはグループに SNMPv3 ユーザを割り当てる前に SNMPv3 グループを作成する必要があります。そうでない場合、グループが作成されたのち、ユーザが適用されません。SNMP グループは複数のユーザを含むことができます。SNMP グループはユーザのグループの MIB view とセキュリティモデルを指定します。各ユーザの認証と暗号化アルゴリズムは作成されたときに指定されます。

異なる SNMPv3 ユーザを作成するため **snmp-agent usm-user v3** コマンドを複数設定することができます。ユーザ名が同一である場合、最後に行った設定が適用されます。

NMS でエージェントにアクセスする場合、以下のことが必要です。

ユーザ、グループのために ACL は不正な NMS をフィルタするために使用します。ユーザ、グループの両方で ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

- ACL を指定しない、指定した ACL が存在しない、ACL にルールがない場合、すべての NMS は SNMP エージェントにアクセスすることができます。

- ACL を指定し、ACL にルールが存在する場合、ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

ACL の詳細はオペレーションマニュアルのセクション 8 *ACL and QoS "ACL"* を参照してください。

例

SNMPv3 グループ **testGroup** にユーザ **testUser** を追加します。グループでプライバシーセキュリティモデルなしで認証を有効にします。ユーザの認証アルゴリズムを HMAC-SHA11、プレーンテキストで認証キーを **123456TESTplat&!**に設定します。

<AC> system-view

[AC] snmp-agent group v3 testGroup authentication

[AC] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha 123456TESTplat&!

デフォルト view が **ViewDefault** の MIB オブジェクトに NMS がアクセスするため、SNMP エージェントの設定と同様に以下の NMS の設定を行います。

- SNMPv3 ユーザ名
- SNMP プロトコルバージョン
- 認証アルゴリズムとキー

SNMPv3 グループ **testGroup** にユーザ **testUser** を追加します。グループで認証とプライバシーセキュリティモデルを有効にします。ユーザの認証アルゴリズムを HMAC-SHA1、プライバシーアルゴリズムを AES、プレーンテキストで認証キーを **123456TESTauth&!**に設定します。プレーンテキストでユーザのプライバシーキーを **123456TESTencr&!**に設定します。

<AC> system-view

[AC] snmp-agent group v3 testGroup privacy

[AC] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha 123456TESTauth&! privacy-mode aes128 123456TESTencr&!

デフォルト view が **ViewDefault** の MIB オブジェクトに NMS がアクセスするため、SNMP エージェントの設定と同様に以下の NMS の設定を行います。

- SNMPv3 ユーザ名
- SNMP プロトコルバージョン
- 認証アルゴリズム
- プライバシーアルゴリズム
- プレーンテキストの認証とプライバシーキー

関連コマンド

- **display snmp-agent usm-user**
- **snmp-agent calculate-password**
- **snmp-agent group**

目次

このセクションのページは **11-x-x** です。

5 章 RMON 5-1
5.1 RMON 設定コマンド 5-1
5.1.1 display rmon alarm 5-1
5.1.2 display rmon event 5-3
5.1.3 display rmon eventlog 5-4
5.1.4 display rmon history 5-6
5.1.5 display rmon prialarm 5-10
5.1.6 display rmon statistics 5-12
5.1.7 rmon alarm 5-14
5.1.8 rmon event 5-17
5.1.9 rmon history 5-18
5.1.10 rmon prialarm 5-20
5.1.11 rmon statistics 5-22

5章 RMON

5.1 RMON設定コマンド

5.1.1 display rmon alarm

Syntax

display rmon alarm [*entry-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

entry-number: RMON アラームエントリのインデックスを指定します。設定範囲は 1～65535 です。指定しない場合、RMON アラームテーブルのすべてのエントリを表示します。

説明

display rmon alarm コマンドは RMON アラームテーブルのエントリを表示します。

例

RMON アラームテーブルのすべてのエントリを表示します。

<AC> display rmon alarm

```
AlarmEntry 1 owned by user1 is VALID.
  Sample type         : absolute
  Sampled variable    : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
  Sampling interval (in seconds)    : 10
  Rising threshold     : 50(associated with event 1)
  Falling threshold    : 5(associated with event 2)
  Alarm sent upon entry startup  : risingOrFallingAlarm
  Latest value         : 0
```

表 5-1 コマンド出力

フィールド	説明

AlarmEntry *entry-number* owned by *owner* is status.	アラームエントリのオーナと状態です。
	• *entry-number*—アラームエントリのインデックスです。
	• *owner*—エントリオーナです。
	• *status*—エントリ状態です。
	  • **VALID**—エントリが有効です。
	  • **UNDERCREATION**—エントリが無効です。
	*status*フィールドはCLIで設定できません。CLIから作成されたすべてのアラームエントリはデフォルトで有効です。**display rmon alarm**コマンドは無効のエントリを表示することができますが、**display current-configuration**コマンドと**display this**コマンドは設定を表示しません。

Sample type	サンプルタイプです。 • **absolute** • **delta**
Sampled variable	モニタされる変数です。
Sampling interval	サンプルされるデータの間隔（単位は秒）です。
Rising threshold	アラームの増加方向のしきい値です。
associated with event	アラームに関連したイベントインデックスです。
Falling threshold	アラームの減少方向のしきい値です。
Alarm sent upon entry startup	最初のサンプリングで生成できるアラーム • **risingAlarm** • **fallingAlarm** • **risingOrFallingAlarm** 最初のサンプリングにアラームタイプを指定しないと、**risingOrFallingAlarm**が有効になります。
Latest value	最後に取得したサンプル値です。

関連コマンド

rmon alarm

5.1.2 display rmon event

Syntax

display rmon event [*entry-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

entry-number: イベントエントリのインデックスを指定します。設定範囲は 1～65535 です。指定しない場合、すべてのイベントエントリを表示します。

説明

display rmon event コマンドは RMON イベントエントリを表示します。

イベントエントリは、以下の情報が含まれます。

- イベントインデックス
- イベントオーナ
- イベント説明
- イベントによって発生するアクション（たとえば、イベントをロギングします、あるいは SNMP 通知を送信します）
- イベントが発生した最後の時間（システムが起動してからの経過時間です。単位は秒です）

例

すべてのイベントエントリを表示します。

<AC> display rmon event

```
EventEntry 1 owned by user1 is VALID.
  Description: N/A
  Community: Security
  Take the action log-trap when triggered, last triggered at 0days 00h:02m:27s
uptime.
```

表 5-2 コマンド出力

フィールド	説明
EventEntry *entry-number* owned by *owner* is *status*.	イベントエントリのオーナと状態です。 • *entry-number*—イベントエントリのインデックスです。 • *owner*—エントリオーナです。 • *status*—エントリ状態です。 • **VALID**—エントリが有効です。 • **UNDERCREATION**—エントリが無効です。 *status*フィールドはCLIで設定できません。CLIから作成されたすべてのイベントエントリはデフォルトで有効です。**display rmon event**コマンドは無効のエントリを表示することができますが、**display current-configuration**コマンドと**display this**コマンドは設定を表示しません。
Description	イベント説明です。
Community	RMONイベントのSNMPコミュニティ名です。
Take the action action when triggered	イベントが発生したときのアクションです。 • **none**—アクションを行いません。 • **log**—イベントをロギングします。 • **trap**—SNMP通知を送信します。 • **log-trap**—イベントをロギングし、SNMP通知を送信します。
last triggered at time uptime	イベントが発生したときの最後の時間です。システムが起動してからの経過時間として表示されます。

関連コマンド

rmon event

5.1.3 display rmon eventlog

Syntax

display rmon eventlog [*entry-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

entry-number: イベントエントリのインデックスを指定します。設定範囲は 1～65535 です。指定しない場合、すべてのイベントエントリを表示します。

説明

display rmon eventlog コマンドはイベントログのエントリを表示します。

イベントのログのアクションが指定されている場合、イベントが発生する毎に、イベントログテーブルにレコードを追加します。各レコードはログエントリインデックス、イベントがログされた時間（システムが起動してからの経過時間）、イベント説明を含みます。

システムはイベントに 10 個のレコードを追加することができます。レコードが 10 になったとき、古いレコードを最新のレコードに置き換えます。

例

イベントエントリ 99 の RMON ログを表示します。

<AC> display rmon eventlog 99

```
EventEntry 99 owned by ww is VALID.
  LogEntry 99.1 created at 50days 08h:54m:44s uptime.
  Description: The 1.3.6.1.2.1.16.1.1.1.4.5 defined in alarmEntry 77,
    uprise 16760000 with alarm value 16776314. Alarm sample type is absolute.
  LogEntry 99.2 created at 50days 09h:11m:13s uptime.
  Description: The 1.3.6.1.2.1.16.1.1.1.4.5 defined in alarmEntry 77,
    less than(or =) 20000000 with alarm value 16951648. Alarm sample type is
absolute.
  LogEntry 99.3 created at 50days 09h:18m:43s uptime.
  Description: The alarm formula defined in prialarmEntry 777,
    less than(or =) 15000000 with alarm value 14026493. Alarm sample type is
absolute.
  LogEntry 99.4 created at 50days 09h:23m:28s uptime.
  Description: The alarm formula defined in prialarmEntry 777,
    uprise 17000000 with alarm value 17077846. Alarm sample type is absolute.
```

この例では、イベントログテーブルはイベント 99 で 4 つのレコードがあることを示します。

- イベント 99 がアラームエントリ 77 によって発生したとき 2 つのレコードが作成されました。
- イベント 99 がアラームエントリ 777 によって発生したとき 2 つのレコードが作成されました。

表 5-3 コマンド出力

フィールド	説明
EventEntry *entry-number* owned by *owner* is *status*.	イベントログエントリのオーナと状態です。 • *entry-number*—イベントログエントリのインデックスです。ログエントリが作成されたイベントエントリのインデックスと同一です。 • *owner*—エントリオーナです。 • *status*—エントリ状態です。 • **VALID**—エントリが有効です。（デフォルトです） • **UNDERCREATION**—エントリが無効です。 *status*フィールドはCLIで設定できません。CLIから作成されたすべてのイベントログエントリはデフォルトで有効です。 **display rmon eventlog**コマンドは無効のエントリを表示することができますが、**display current-configuration**コマンドと**display this**コマンドは設定を表示しません。
LogEntry *entry-number* created at *created-time* uptime.	イベントレコードが作成された時間です。 • **entry-number**—イベントレコードインデックスです。logEventIndex.logIndexとして示されます。logEventIndexとlogIndexはMIBオブジェクトです。イベントのすべてのレコードのなかでレコードを一意に識別します。 • **created-time**—イベントエントリが作成された時間です。
Description	レコードの説明です。

関連コマンド

rmon event

5.1.4 display rmon history

Syntax

display rmon history [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。インタフェースを指定しない場合、RMON 履歴管理エントリがあるすべてのインタフェースの履歴サンプルを表示します。

説明

display rmon history コマンドは Ethernet インタフェースの RMON 履歴管理エントリと Ethernet 履歴のサンプルの統計情報を表示します。

RMON は Ethernet インタフェースの Ethernet 履歴のサンプルを記録するため、etherHistoryTable オブジェクトを使用します。

Ethernet インタフェースの履歴サンプルを収集するため、最初にインタフェースで履歴管理エントリを作成する必要があります。

表示できる履歴サンプルの数とサンプリング間隔を設定する場合、**rmon history** コマンドを使用します。

例

GigabitEthernet 1/0/1 の RMON 履歴管理エントリと履歴のサンプルの情報を表示します。

<AC> display rmon history gigabitethernet 1/0/1

```
HistoryControlEntry 6 owned by user1 is VALID.
  Sampled interface    : GigabitEthernet 1/0/1 <ifIndex.117>
  Sampling interval    : 8(sec) with 3 buckets max
  Sampling record 1 :
    dropevents       : 0        , octets             : 5869
    packets          : 54       , broadcast packets    : 9
    multicast packets : 23        , CRC alignment errors : 0
    undersize packets : 0         , oversize packets     : 0
    fragments        : 0        , jabbers            : 0
    collisions       : 0        , utilization         : 0
  Sampling record 2 :
    dropevents       : 0        , octets             : 5367
    packets          : 55       , broadcast packets    : 1
    multicast packets : 7         , CRC alignment errors : 0
    undersize packets : 0         , oversize packets     : 0
    fragments        : 0        , jabbers            : 0
    collisions       : 0        , utilization         : 0
  Sampling record 3 :
    dropevents       : 0        , octets             : 936
    packets          : 10       , broadcast packets    : 0
    multicast packets : 6         , CRC alignment errors : 0
```

```
    undersize packets : 0        , oversize packets    : 0
    fragments        : 0        , jabbers            : 0
    collisions       : 0        , utilization         : 0
HistoryControlEntry 7 owned by user1 is VALID.
  Sampled interface    : GigabitEthernet 1/0/1 <ifIndex.117>
  Sampling interval    : 9(sec) with 1 buckets max
  Sampling record 1 :
    dropevents       : 0        , octets             : 1150
    packets          : 12       , broadcast packets   : 0
    multicast packets : 8        , CRC alignment errors : 0
    undersize packets : 0        , oversize packets    : 0
    fragments        : 0        , jabbers            : 0
    collisions       : 0        , utilization         : 0
```

表 5-4 コマンド出力

フィールド	説明

HistoryControlEntry *entry-number* owned by *owner* is *status*.	ヒストリ制御エントリのオーナと状態です。
	• *entry-number*—ヒストリ制御エントリのインデックスです。
	• *owner*—エントリオーナです。
	• *status*—エントリ状態です。
	  • **VALID**—エントリが有効です。
	  • **UNDERCREATION**—エントリが無効です。
	*status*フィールドはCLIで設定できません。CLIから作成されたすべてのヒストリ制御エントリはデフォルトで有効です。
	The **display rmon history**コマンドは無効のエントリを表示することができますが、**display current-configuration**コマンドと**display this**コマンドは設定を表示しません。

Sampled Interface	サンプルされるインタフェースです。
Sampling interval	サンプルされるデータの間隔です。単位は秒です。
buckets max	履歴管理エントリで保存できるサンプルの最大数です。 **rmon history**コマンドで設定した、予期したバケットサイズが有効な履歴テーブルサイズを超過した場合、RMONはバケットサイズをできるだけ、予期したバケットサイズに近づけます。 バケットサイズが一杯になったとき、RMONは新しいサンプルを古いサンプルに上書きします。
Sampling record	履歴サンプルインデックスです。

フィールド	説明
dropevents	サンプリング間隔中にパケットが廃棄されたイベントの総数です。 🕮 メモ： 統計情報は、廃棄が発生した回数です。廃棄したパケットの総数になるわけではありません。
octets	サンプリング間隔中に受信したオクテット数です。
packets	サンプリング間隔中に受信したパケットの総数（不良パケットを含みます）です。
broadcast packets	サンプリング間隔中に受信したブロードキャストパケットの総数です。
multicast packets	サンプリング間隔中に受信したマルチキャストパケットの総数です。
CRC alignment errors	サンプリング間隔中に受信したCRCエラーパケットの数です。
undersize packets	サンプリング間隔中に受信した過小サイズのエラーパケットの数です。 過小サイズエラーパケットはパケット長が64オクテット未満のパケットです。（フレームビットを除き、FCSオクテットを含みます）
oversize packets	サンプリング間隔中に受信した過大サイズのエラーパケットの数です。 過大サイズエラーパケットはパケット長が1518オクテットより長いパケットです。（フレームビットを除き、FCSオクテットを含みます）
fragments	サンプリング間隔中に受信した過小サイズのCRCエラーパケットの数です。
jabbers	サンプリング間隔中に受信した過大サイズのCRCエラーパケットの数です。
collisions	サンプリング間隔中に受信したコリジョンパケットの数です。
utilization	サンプリング間隔中の帯域幅の使用率です。（単位は%です）

関連コマンド

rmon history

5.1.5 display rmon prialarm

Syntax

display rmon prialarm [*entry-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

entry-number: アラームエントリのインデックスを指定します。設定範囲は 1～65535 です。指定しない場合、すべてのプライベートアラームエントリを表示します。

説明

display rmon prialarm コマンドはプライベート RMON アラームテーブルのエントリを表示します。

例

すべてのプライベートアラームエントリを表示します。

<AC> display rmon prialarm

```
PrialarmEntry 1 owned by user1 is VALID.
  Sample type                : absolute
  Variable    formula                                                 :
(.1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1)
  Description                : ifUtilization.GigabitEthernet1/0/1
  Sampling interval (in seconds) : 10
  Rising threshold            : 80(associated with event 1)
  Falling threshold           : 5(associated with event 2)
  Alarm sent upon entry startup  : risingOrFallingAlarm
  Entry lifetime              : forever
  Latest value               : 85
```

表 5-5 コマンド出力

フィールド	説明

PrialarmEntry *entry-number* owned by *owner* is *status*.	プライベートアラームエントリのオーナと状態です。
	• *entry-number*—プライベートアラームエントリのインデックスです。
	• *owner*—エントリオーナです。
	• *status*—エントリ状態です。
	  • **VALID**—エントリが有効です。
	  • **UNDERCREATION**—エントリが無効です。
	*status*フィールドはCLIで設定できません。CLIから作成されたすべてのプライベートアラームエントリはデフォルトで有効です。
	display rmon prialarmコマンドは無効のエントリを表示することができますが、**display current-configuration**コマンドと**display this**コマンドは設定を表示しません。

Sample type	サンプルタイプです。 • **absolute** • **delta**
Variable formula	変数の式です。
Description	アラームエントリの説明です。
Sampling interval	サンプルされるデータの間隔です。単位は秒です。
Rising threshold	アラームの増加方向のしきい値です。
Falling threshold	アラームの減少方向のしきい値です。
associated with event	アラームに関連したイベントインデックスです。
Alarm sent upon entry startup	最初のサンプリングで生成できるアラーム • **risingAlarm** • **fallingAlarm** • **risingOrFallingAlarm** 最初のサンプリングにアラームタイプを指定しないと、**risingOrFallingAlarm**が有効になります。
Entry lifetime	エントリの有効期限です。 • 有効期限がforeverに設定されている場合、エントリは削除されません。 • 有効期限に時間が設定されている場合、時間が終了したときエントリが削除されます。

フィールド	説明
Latest value	最後に取得したサンプル値です。

関連コマンド

rmon prialarm

5.1.6 display rmon statistics

Syntax

display rmon statistics [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。インタフェースを指定しない場合、すべてのインタフェースの RMON の統計情報を表示します。

説明

display rmon statistics コマンドは RMON の統計情報を表示します。

このコマンドは、統計情報エントリが作成された時間からコマンドが実行された時間までの期間のインタフェース統計情報を表示します。装置が再起動するとその統計情報は削除されます。

例

GigabitEthernet 1/0/1 の RMON の統計情報を表示します。

<AC> display rmon statistics gigabitethernet 1/0/1

```
EtherStatsEntry 1 owned by user1 is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets        : 43393306  , etherStatsPkts         : 619825
  etherStatsBroadcastPkts  : 503581    , etherStatsMulticastPkts : 44013
  etherStatsUndersizePkts  : 0         , etherStatsOversizePkts  : 0
  etherStatsFragments      : 0         , etherStatsJabbers       : 0
  etherStatsCRCAlignErrors : 0         , etherStatsCollisions    : 0
```

```
etherStatsDropEvents (insufficient resources): 0
Incoming packets by size:
64     : 0        ,  65-127  : 0        ,  128-255  : 0
256-511: 0        ,  512-1023: 0        ,  1024-1518: 0
```

表 5-6 コマンド出力

フィールド	説明

EtherStatsEntry *entry-number* owned by *owner* is *status*.	統計情報エントリのオーナと状態です。
	• *entry-number*—統計情報エントリのインデックスです。
	• *owner*—エントリオーナです。
	• *status*—エントリ状態です。
	  • **VALID**—エントリが有効です。
	  • **UNDERCREATION**—エントリが無効です。
	*status*フィールドはCLIで設定できません。CLIから作成されたすべての統計情報エントリはデフォルトで有効です。**display rmon statistics**コマンドは無効のエントリを表示することができますが、**display current-configuration**コマンドと**display this**コマンドは設定を表示しません。

Interface	統計情報が収集されたインタフェースです。
etherStatsOctets	インタフェースで受信したオクテットの総数です。
etherStatsPkts	インタフェースで受信したパケットの総数です。
etherStatsBroadcastPkts	インタフェースで受信したブロードキャストパケットの総数です。
etherStatsMulticastPkts	インタフェースで受信したマルチキャストパケットの総数です。
etherStatsUndersizePkts	インタフェースで受信した過小サイズのエラーパケットの総数です。
etherStatsOversizePkts	インタフェースで受信した過大サイズのエラーパケットの総数です。
etherStatsFragments	インタフェースで受信したCRCエラーパケットの総数です。
etherStatsJabbers	インタフェースで受信した過大サイズのCRCエラーパケットの総数です。
etherStatsCRCAlignErrors	インタフェースで受信したCRCエラーパケットの総数です。
etherStatsCollisions	インタフェースで受信したコリジョンパケットの総数です。

フィールド	説明
etherStatsDropEvents	廃棄されたパケットのイベント総数です。 🕮 **メモ：** 統計情報は、廃棄が発生した回数です。廃棄したパケットの総数になるわけではありません。
Incoming packets by size:	パケット長毎の入力パケットです。 ● **64**—長さが64バイト以下のパケット数。 ● **65-127**—65～127バイト長のパケット数です。 ● **128-255**—128～255バイト長のパケット数です。 ● **256-511**—256～511バイト長のパケット数です。 ● **512-1023**—512～1023バイト長のパケット数です。 ● **1024-1518**—1024～1518バイト長のパケット数です。

関連コマンド

rmon statistics

5.1.7 rmon alarm

Syntax

rmon alarm *entry-number alarm-variable sampling-interval* { **absolute** | **delta** } [**startup-alarm** { **falling** | **rising** | **rising-falling** }] **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *text*]

undo rmon alarm *entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

entry-number: アラームエントリのインデックスを指定します。設定範囲は 1～65535 です。

alarm-variable: アラーム変数を指定します。設定範囲は 1～255 です。変数は ASN.1 INTEGER（INTEGER、NTEGER32、Unsigned32、Counter32、Counter64、Gauge、TimeTicks）のみを使用できます。アラーム変数は表 5-7 の 1 つを使用します。

表 5-7 アラーム変数

フォーマット	例
ドットで区切られたOID形式： エントリ.整数,インスタンス	1.3.6.1.2.1.2.1.10.1
オブジェクト名.インスタンス	etherStatsOctets.1 etherStatsPkts.1 etherStatsBroadcastPkts.1 ifInOctets.1 ifInUcastPkts.1 ifInNUcastPkts.1

sampling-interval: サンプリング間隔を指定します。設定範囲は 5～65535 秒です。

absolute: 絶対値のサンプリングを指定します。RMON はサンプリング間隔の両端で増加方向のしきい値と減少方向のしきい値を比較します。

delta: 相対値のサンプリングを指定します。RMON は現在の値から前に取得したサンプル値を引き、増加方向と減少方向のしきい値の差異を比較します。

startup-alarm: アラームエントリが有効なときに作成されるアラームを指定します。アラームを指定しない場合、RMON は最初のサンプルに依存して増加方向のアラームあるいは減少方向のアラームを作成します。

rising: エントリが有効になったのち、最初にサンプルが増加方向のしきい値以上になった場合に、増加方向のアラームを作成します。

falling: エントリが有効になったのち、最初にサンプルが減少方向のしきい値以下になった場合に、減少方向のアラームを作成します。

rising-falling: 最初のサンプルが増加方向のしきい値と交差した場合、増加方向のアラームを作成します。あるいは最初のサンプルが減少方向のしきい値と交差した場合、減少方向のアラームを作成します。

rising-threshold *threshold-value1 event-entry1*: 増加方向のしきい値を指定します。*threshold-value1* の設定範囲は–2147483648 ～ +2147483647 です。*event-entry1* は増加方向のしきい値が交差したとき発生するイベントのインデックスを示します。*event-entry1* の設定範囲は 0～65535 です。0 が指定された場合、イベントでアラームが発生しません。

falling-threshold *threshold-value2 event-entry2*: 減少方向のしきい値を指定します。*threshold-value2* の設定範囲は–2147483648 ～ +2147483647 です。*event-entry2* は減少方向のしきい値が交差したとき発生するイベントのインデックスを示します。*event-entry2* の設定範囲は 0～65535 です。0 が指定された場合、イベントでアラームが発生しません。

owner *text*: エントリオーナを指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

rmon alarm コマンドは RMON アラームテーブルのエントリを作成します。

undo rmon alarm コマンドは RMON アラームテーブルからエントリを削除します。

RMON アラームテーブルに最大 60 のエントリを作成することができます。

アラームエントリは固有のアラーム変数、サンプリング間隔、サンプリングタイプ、増加方向のしきい値あるいは減少方向のしきい値がある必要があります。エントリのすべてのパラメータが既存のエントリと同一である場合、アラームエントリを作成することができません。

アラーム状況に関連したイベントを発生させるため、**rmon event** コマンドでイベントを作成する必要があります。

RMON は指定されたサンプリング間隔でモニタ対象のアラーム変数をサンプリングします。予期されたしきい値とサンプリングされた値と比較し、以下の 1 つの処理を行います。

- サンプリングした値が増加方向のしきい値以上である場合、増加方向のアラームに関連したイベントを発生します。
- サンプリングした値が減少方向のしきい値以下である場合、減少方向のアラームに関連したイベントを発生します。

例

GigabitEthernet 1/0/1 でアラームテーブルにエントリ 1 を作成します。サンプリングタイプを absolute （絶対値）にし、オブジェクト ID 1.3.6.1.2.1.16.1.1.1.4.1 を 10 秒間隔でサンプリングします。サンプリングした値が上昇しきい値 5000 以上になった場合、増加方向のアラームイベントをロギングします。サンプリングした値が 5 以下である場合、アクションは発生しません。

<AC> system-view

[AC] rmon event 1 log

[AC] rmon event 2 none

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] rmon statistics 1

[AC-GigabitEthernet1/0/1] quit

[AC] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 absolute rising-threshold 5000 1 falling-threshold 5 2 owner user1

この例では、1.3.6.1.2.1.16.1.1.1.4.1 を etherStatsOctets に置き換えることができます。ここで 1 はインタフェースのエントリインデックスの統計情報です。**rmon statistics 5** コマンドを実行した場合、1.3.6.1.2.1.16.1.1.1.4.5 を置き換えるために etherStatsOctets を使用します。

関連コマンド

- **display rmon alarm**
- **rmon event**

5.1.8 rmon event

Syntax

rmon event *entry-number* [**description** *string*] { **log** | **log-trap** *security-string* | **none** | **trap** *security-string* } [**owner** *text*]

undo rmon event *entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

entry-number: アラームエントリのインデックスを指定します。設定範囲は 1～65535 です。

description *string*: イベントの説明を設定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

log: イベントが発生したとき、ログを取得します。

log-trap: イベントが発生したとき、ログを取得し、SNMP 通知を送信します。

security-string: SNMP コミュニティを指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。SNMP の設定に依存します。このパラメータは現在のソフトウェアバージョンでサポートしていません。

none: イベントが発生したとき、アクションを行いません。

trap: イベントが発生したとき、SNMP 通知を送信します。

owner *text*: エントリオーナを指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

🕮 **メモ：**

security-string の SNMP コミュニティの設定は、コマンドで設定することができますが適用されません。システムは RMON の SNMP 通知を送信するとき、SNMP の設定を使用します。SNMP 通知の詳細は、オペレーションマニュアルのセクション 11 *システム管理 “SNMP”* を参照してください。

説明

rmon event コマンドは RMON イベントテーブルのエントリを作成します。

undo rmon event コマンドは RMON イベントテーブルからエントリを削除します。

最大 60 のイベントエントリを作成することができます。

アラーム状況が発生したとき、アクションを指定するため、イベントエントリを標準あるいはプライベートアラームエントリに関連づけることができます。設定に依存して、イベントのログを取得し、SNMP 通知を送信することができます。

1 つのイベントを複数のアラームエントリに関連づけることができます。

例

RMON イベントエントリを作成します。イベント 10、エントリオーナ user1 を指定します。

<AC> system-view

[AC] rmon event 10 log owner user1

関連コマンド

- **display rmon event**
- **rmon alarm**
- **rmon prialarm**

5.1.9 rmon history

Syntax

rmon history *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text*]

undo rmon history *entry-number*

デフォルト

設定なし

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

entry-number: 履歴管理エントリのインデックスを指定します。設定範囲は 1～65535 です。

buckets *number*: エントリのために記録されるサンプルの予期する最大数を指定します。設定範囲は 1～65535 です。RMON は各履歴管理エントリで 50 のサンプルを記録することができます。予期したバケットサイズが有効な履歴テーブルサイズを超過した場合、RMON はバケットサイズをできるだけ、予期したバケットサイズに近づけます。しかし 50 を超過することはできません。たとえば、予期したバケットサイズを 55 に設定し、有効なバケットサイズが 30 である場合、履歴管理エントリのバケットサイズは 30 となります。

interval *sampling-interval*: サンプリング間隔を指定します。設定範囲は 5～3600 秒です。

owner *text*: エントリオーナを指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

rmon history コマンドは RMON 履歴管理テーブルのエントリを作成します。

undo rmon history コマンドは RMON 履歴管理テーブルからエントリを削除します。

レイヤ 2 Ethernet インタフェースあるいはレイヤ 3 Ethernet インタフェースでのみ RMON 履歴管理エントリを作成することができます。

システムで最大 100 の履歴管理エントリを作成することができます。

Ethernet インタフェースで履歴管理エントリがある場合、RMON はインタフェースで定期的にパケットの統計情報をサンプリングし、履歴テーブルにサンプルを記録します。履歴管理エントリのバケットサイズが最大になったとき、RMON は古いサンプルを新しいサンプルに上書きします。

1 つのインタフェースで複数の履歴管理エントリを設定することができますが、エントリ数とサンプリング間隔を変更する必要があります。

例

GigabitEthernet 1/0/1 で RMON 履歴管理テーブルのエントリ 1 を作成します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] rmon history 1 buckets 10 interval 5 owner user1

関連コマンド

display rmon history

5.1.10 rmon prialarm

Syntax

rmon prialarm *entry-number prialarm-formula prialarm-des sampling-interval* { **absolute** | **delta** } [**startup-alarm** { **falling** | **rising** | **rising-falling** }] **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **entrytype** { **forever** | **cycle** *cycle-period* } [**owner** *text*]

undo rmon prialarm *entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

entry-number: アラームエントリのインデックスを指定します。設定範囲は 1～65535 です。

prialarm-formula: プライベートアラーム変数を指定します。設定範囲は 1～255 文字です。変数の式はドット（.）始まる OID で示されます。たとえば、(.1.3.6.1.2.1.2.1.10.1) *8 です。この変数は、加減乗除の四則演算を行うことができます。演算の結果は長整数になります。エラーを防ぐため、演算の各段階の結果が、以下の値になるようにしてください。

- 式の変数の値が整数
- 設定範囲各計算のステップが long 整数

prialarm-des: エントリの説明を設定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

sampling-interval: サンプリング間隔を指定します。設定範囲は 10～65535 秒です。

absolute: 絶対値のサンプリングを指定します。RMON はサンプリング間隔の両端で増加方向のしきい値と減少方向のしきい値を比較します。

delta: 相対値のサンプリングを指定します。RMON は現在の値から前に取得したサンプル値を引き、増加方向と減少方向のしきい値の差異を比較します。

startup-alarm: アラームエントリが有効なときに作成されるアラームを指定します。アラームを指定しない場合、RMON は以下を行います。

- 最初のサンプルが増加方向のしきい値を交差したとき、増加方向のアラームを作成します。

- 最初のサンプルが減少方向のしきい値を交差したとき、減少方向のアラームを作成します。

rising: エントリが有効になったのち、最初にサンプルが増加方向のしきい値以上になった場合に、増加方向のアラームを作成します。

falling: エントリが有効になったのち、最初にサンプルが減少方向のしきい値以下になった場合に、減少方向のアラームを作成します。

rising-falling: 最初のサンプルが増加方向のしきい値と交差した場合、増加方向のアラームを作成します。あるいは最初のサンプルが減少方向のしきい値と交差した場合、減少方向のアラームを作成します。

rising-threshold *threshold-value1 event-entry1*: 増加方向のしきい値を指定します。*threshold-value1* の設定範囲は–2147483648 ～ +2147483647 です。*event-entry1* は増加方向のしきい値が交差したとき発生するイベントのインデックスを示します。*event-entry1* の設定範囲は 0～65535 です。0 が指定された場合、イベントでアラームが発生しません。

falling-threshold *threshold-value2 event-entry2*: 減少方向のしきい値を指定します。*threshold-value2* の設定範囲は–2147483648 ～ +2147483647 です。*event-entry2* は減少方向のしきい値が交差したとき発生するイベントのインデックスを示します。*event-entry2* の設定範囲は 0～65535 です。0 が指定された場合、イベントでアラームが発生しません。

forever: 無期限のエントリを指定します。RMON は手動で削除するまで無期限のプライベートアラームエントリを保持します。

cycle *cycle-period*: エントリの有効期限を指定します。設定範囲は 0～4294967 秒です。RMON は有効期限が終了したとき、エントリを削除します。

owner *text*: エントリオーナを指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

rmon prialarm コマンドはプライベートアラームテーブルのエントリを作成します。

undo rmon prialarm コマンドはプライベートアラームテーブルからエントリを削除します。

最大 50 のプライベートアラームエントリを作成することができます。

アラームエントリは固有のアラーム変数、サンプリング間隔、サンプリングタイプ、増加方向のしきい値あるいは減少方向のしきい値がある必要があります。エントリのすべてのパラメータが既存のエントリと同一である場合、アラームエントリを作成することができません。

アラーム状況に関連したイベントを発生させるため、**rmon event** コマンドでイベントを作成する必要があります。

RMON エージェントは変数をサンプリングし、プライベートアラームエントリをもとにしてアラームのアクションを行います。

1) プライベートアラームの式で指定された変数を定期的にサンプリングします。

2) 式でサンプリングした値を処理します。
3) 計算結果と予期されたしきい値を比較し、以下のアクションの 1 つを行います。
   - □ 結果が増加方向のしきい値以上である場合、増加方向のアラームに関連したイベントを発生します。
   - □ 結果が減少方向のしきい値以下である場合、減少方向のアラームに関連したイベントを発生します。

例

GigabitEthernet 1/0/1 で入力パケットの総数と入力ブロードキャストの割合をモニタするため、無期限のプライベートアラームエントリを追加します。割合が 80%を超過したとき、増加方向のアラームイベントのログを取得し、割合が 5%以下になったとき、アクションを行いません。式は（1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1）です。ここで 1.3.6.1.2.1.16.1.1.1.6.1 はオブジェクトインスタンス etherStatsBroadcastPkts.1 の OID です。1.3.6.1.2.1.16.1.1.1.5.1 はオブジェクトインスタンス etherStatsPkts.1 の OID です。

<AC> system-view

[AC] rmon event 1 log

[AC] rmon event 2 none

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] rmon statistics 1

[AC-GigabitEthernet1/0/1] quit

[AC] rmon prialarm 1 (.1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1) BroadcastPktsRatioOfEth1/1 10 absolute rising-threshold 80 1 falling-threshold 5 2 entrytype forever owner user1

変数の OID の最後の数はインタフェースのエントリインデックスの統計情報と同一にする必要があります。たとえば、**rmon statistics 5** コマンドを実行するとき、それぞれ 1.3.6.1.2.1.16.1.1.1.6.1 、 1.3.6.1.2.1.16.1.1.1.5.1 を 1.3.6.1.2.1.16.1.1.1.6.5 、1.3.6.1.2.1.16.1.1.1.5.5 に置き換えます。

関連コマンド

- **display rmon prialarm**
- **rmon event**

5.1.11 rmon statistics

Syntax

rmon statistics *entry-number* [**owner** *text*]

undo rmon statistics *entry-number*

デフォルト

設定なし

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

entry-number: アラームエントリのインデックスを指定します。設定範囲は 1～65535 です。

owner *text*: エントリオーナを指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

rmon statistics コマンドは RMON 統計情報テーブルのエントリを作成します。

undo rmon statistics コマンドは RMON 統計情報テーブルからエントリを削除します。

レイヤ 2 Ethernet インタフェースあるいはレイヤ 3 Ethernet インタフェースでのみ RMON 統計情報エントリを作成することができます。

各インタフェースで 1 つの統計情報のエントリを作成することができます。

装置で最大 100 の統計情報エントリを作成することができます。

各 RMON 統計情報テーブルエントリは、インタフェースで収集したトラフィックを現在の時間まで累積した統計情報の合計です。統計情報はコリジョン、過大サイズの CRC エラーパケットの数、過大サイズのパケット数、過小サイズのパケット数、ブロードキャストパケット数、マルチキャストパケット数、受信したバイト数、受信したパケット数を含みます。統計情報は、再起動で削除されます。

RMON 統計情報のテーブルを表示する場合、**display rmon statistics** コマンドを使用します。

例

GigabitEthernet 1/0/1 でインデックス 20、オーナ **user1** の RMON 統計情報エントリを作成します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] rmon statistics 20 owner user1

関連コマンド

display rmon statistics

目次

このセクションのページは **11-x-x** です。

6 章 NETCONF 6-1
6.1 NETCONF 設定コマンド 6-1
6.1.1 netconf log 6-1
6.1.2 netconf soap http enable 6-2
6.1.3 netconf soap https enable 6-3
6.1.4 xml 6-3

6章 NETCONF

6.1 NETCONF設定コマンド

6.1.1 netconf log

Syntax

netconf log source { { **soap** | **web** } * } { { **protocol-operation** { **all** | { **action** | **config** | **get** | **set** | **session** | **syntax** | **others** } * } } | **verbose** }

undo netconf log source { { **soap** | **web** } * } { { **protocol-operation** { **all** | { **action** | **config** | **get** | **set** | **session** | **syntax** | **others** } * } } | **verbose** }

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

source: NETCONF オペレーションを実行するクライアントプロトコルを指定します。

- **soap**: SOAP over HTTP 、あるいは SOAP over HTTPS を使用しているクライアントを指定します。
- **web**: Web を使用しているクライアントを指定します。

protocol-operation: NETCONF オペレーションタイプを指定します。

- **all**: 全ての NETCONF オペレーションを指定します。
- **action**: action オペレーションを指定します。
- **config**: NETCONF のコンフィグオペレーションを指定します。CLI、save、load、rollback、lock、unlock と save-point オペレーションを含みます。
- **get**: 情報取得に関する NETCONF オペレーションを指定します。get、get-config、get-bulk、get-bulk-config と get-sessions オペレーションを含みます。
- **set**: 全ての edit-config オペレーションを指定します。
- **session**: セッションに関する NETCONF オペレーションを指定します。kill-session、close-session と hello メッセージの capability 交換を含みます。
- **syntax**: XML と schema のエラーを指定します。
- **others**: action、config、get、set、session、syntax 以外の NETCONF オペレーションを指定します。

verbose: NETCONF 操作の要求および応答に関する詳細情報を記録します。書式が正しい要求のパケット内容と、失敗した<edit-config>操作に関するエラー情報が含まれます。

説明

netconf log コマンドは、NETCONF ロギングを有効にします。

undo netconf log コマンドは、NETCONF ロギングを無効にします。

NETCONF で作成されたログを Information Center に正しく送信するため、Information Center の設定を行う必要があります。詳細はオペレーションマニュアルのセクション 11 *システム管理 "Information Center"* を参照してください。

例

クライアントからの edit-config 情報について、NETCONF のログを出力するように設定します。

<AC> system-view

[AC] netconf log source web protocol-operation set

6.1.2 netconf soap http enable

Syntax

netconf soap http enable

undo netconf soap http enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

netconf soap http enable コマンドは NETCONF over SOAP over HTTP を有効にします。

undo netconf soap http enable コマンドは NETCONF over SOAP over HTTP を無効にします。

本コマンドにより、HTTP パケット中の SOAP（Simple Object Access Protocol）でカプセル化された NETCONF メッセージを解釈するようになります。

例

NETCONF over SOAP over HTTP を有効にします。

<AC> system-view

[AC] netconf soap http enable

6.1.3 netconf soap https enable

Syntax

netconf soap https enable

undo netconf soap https enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

netconf soap https enable コマンドは、NETCONF over SOAP over HTTPS を有効にします。

undo netconf soap https enable コマンドは、NETCONF over SOAP over HTTPS を無効にします。

本コマンドにより、HTTPS パケット中の SOAP でカプセル化された NETCONF メッセージを解釈するようになります。

例

NETCONF over SOAP over HTTPS を有効にします。

<AC> system-view

[AC] netconf soap https enable

6.1.4 xml

Syntax

xml

View

User view

定義済みユーザロール

network-admin

network-operator

説明

xml コマンドは XML view に移行します。

XML view では装置の設定や装置からの情報取得を行う NETCONF メッセージを使用することができます。操作可能な NETCONF オペレーションはユーザロールに依存し、表 6-1 のとおりです。

表 6-1 操作可能な NETCONF オペレーションとユーザロール

フィールド	説明
network-admin	すべてのNETCONFオペレーション
network-operator	• Get • Get-bulk • Get-bulk-config • Get-config • Get-sessions • Close-session

XML view に移行した後、装置は自動でクライアントに NETCONF の機能をアドバタイズします。NETCONF 機能をサポートしている装置に通知するため、クライアントを設定してください。機能の交換を行った後、クライアントを使用して装置を設定することができます。

NETCONF メッセージは、XML フォーマット要求および、装置の NETCONF XML API レファレンスにおける意味および構文の要求に合致している必要があります。設定が正しく行われるようにするためには、NETCONF メッセージを生成する他社製ソフトウェアを使用することを推奨します。

XML view を終了するには、**quit** コマンドのかわりに NETCONF メッセージを使用してください。

user line/user line class view でエスケープキーを用いたショートカットキーを設定している場合、NETCONF メッセージはっそのショートカットキー文字列を含むことができません。

NETCONF メッセージにショートカットキーが含まれる場合、XML view で関連する設定が影響を受ける可能性があります。たとえば、user line view で **escape-key a** コマンドを使用してショートカットキー“a”を設定した場合、NETCONF メッセージには文字“a”が含まれます。メッセージの最後の“a”のあとの内容のみを処理することができます。

例

XML view に移行します。

<AC> xml

```
<?xml version="1.0" encoding="UTF-8"?><hello
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"><capabilities><capability>urn
:ietf:params:netconf:base:1.0</capability><capability>urn:ietf:params:netconf
:capability:writable-running:1.0</capability><capability>urn:ietf:params:netc
onf:capability:notification:1.0</capability><capability>urn:ietf:params:netco
nf:capability:validate:1.0</capability><capability>urn:ietf:params:netconf:ca
pability:interleave:1.0</capability><capability>urn:ietf:params:netconf:capab
ility:rollback-on-error:1.0</capability><capability>urn:nec:params:netconf:ca
pability:nec-netconf-ext:1.0</capability><capability>urn:nec:params:netconf:c
apability:nec-save-point:1.0</capability></capabilities><session-id>1</sessio
n-id></hello>]]>]]>
```

クライアントでサポートされる NETCONF 機能を装置にアドバタイズします。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
          urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>]]>]]>
```

XML view を終了します。

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <close-session>
  </close-session>
</rpc>]]>]]>
```

<AC>

目次

このセクションのページは **11-x-x** です。

7 章 プロセスモニタリングとメンテナンス 7-1
7.1 プロセスモニタリングとメンテナンス設定コマンド 7-1
7.1.1 display exception context 7-1
7.1.2 display exception filepath 7-6
7.1.3 exception filepath 7-7
7.1.4 process core 7-8
7.1.5 reset exception context 7-9

7章 プロセスモニタリングとメンテナンス

7.1 プロセスモニタリングとメンテナンス設定コマンド

7.1.1 display exception context

Syntax

display exception context [**count** *value*]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

count *value*: コンテキスト情報のエントリ番号を指定します。設定範囲は 1～20 です。デフォルトは 1 です。

説明

display exception context コマンドはプロセス例外に関するコンテキスト情報を表示します。

システムは、各プロセス例外のコンテキスト情報エントリを作成します。コンテキスト情報エントリは、プロセス ID、クラッシュ時間、コアファイルのディレクトリ、スタック情報、レジスタ情報が含まれます。

例

x86 ベースの 32 ビット装置のプロセス例外に関するコンテキスト情報を表示します。

<AC> display exception context

```
Index 1 of 1
------------------------------
Crashed PID: 120 (routed)
Crash signal: SIGBUS
Crash time: Tue Apr  9 17:14:30 2013
Core file path:
cfa0:/core/node0_routed_120_7_20130409-171430_1365527670.core
#0  0xb7caba4a
#1  0x0804cb79
#2  0xb7cd77c4
#3  0x08049f45
```

```
Backtrace stopped.
                    Registers' content
  eax:0xfffffffc   ebx:0x00000003   ecx:0xbfe244ec   edx:0x0000000a
  esp:0xbfe244b8   ebp:0xbfe244c8   esi:0xffffffff   edi:0xbfe24674
  eip:0xb7caba4a eflag:0x00000292    cs:0x00000073    ss:0x0000007b
   ds:0x0000007b    es:0x0000007b    fs:0x00000000    gs:0x00000033
```

x86 ベースの 64 ビット端末のプロセス例外に関するコンテキスト情報を表示します。

<AC> display exception context

```
Index 1 of 1
------------------------------
Crashed PID: 121 (routed)
Crash signal: SIGBUS
Crash time: Sun Mar 31 11:12:21 2013
Core file path:
cfa0:/core/node0_routed_121_7_20130331-111221_1364728341.core
#0  0x00007fae7dbad20c
#1  0x00000000004059fa
#2  0x00007fae7dbd96c0
#3  0x0000000000402b29
Backtrace stopped.
                    Registers' content
      rax:0xfffffffffffffffc      rbx:0x00007fff88a5dd10
      rcx:0xffffffffffffffff      rdx:0x000000000000000a
      rsi:0x00007fff88a5dd10      rdi:0x0000000000000003
      rbp:0x00007fff88a5dcf0      rsp:0x00007fff88a5dcf0
       r8:0x00007fae7ea587e0       r9:0x0000000000000079
      r10:0xffffffffffffffff      r11:0x0000000000000246
      r12:0x0000000000405b18      r13:0x00007fff88a5ff7a
      r14:0x00007fff88a5de30      r15:0x0000000000000000
      rip:0x00007fae7dbad20c     flag:0x0000000000000246
       cs:0x0000000000000033       ss:0x000000000000002b
       ds:0x0000000000000000       es:0x0000000000000000
       fs:0x0000000000000000       gs:0x0000000000000000
   fs_base:0x00007fae80a5d6a0   gs_base:0x0000000000000000
   orig_ax:0x00000000000000e8
```

Power PC ベースの 32 ビット端末のプロセス例外に関するコンテキスト情報を表示します。

<AC> display exception context

```
Index 1 of 1
------------------------------
Crashed PID: 133 (routed)
Crash signal: SIGBUS
```

```
Crash time: Wed Apr 10 15:47:49 2013
Core file path:
cfa0:/core/node0_routed_133_7_20130410-154749_1365608869.core
#0  0x184720bc
#1  0x10006b4c
Backtrace stopped.
                    Registers' content
grp00: 0x000000ee 0x7ffd6ad0 0x1800f440 0x00000004
grp04: 0x7ffd6af8 0x0000000a 0xffffffff 0x184720bc
grp08: 0x0002d200 0x00000003 0x00000001 0x1847209c
grp12: 0x10006b4c 0x10020534 0xd6744100 0x00000000
grp16: 0x00000000 0xa0203ff0 0xa028b12c 0xa028b13c
grp20: 0xa028b148 0xa028b168 0xa028b178 0xa028b190
grp24: 0xa028b1a8 0xa028b1b8 0x00000000 0x7ffd6c08
grp28: 0x10006cac 0x7ffd6f92 0x184c1b84 0x7ffd6ae0

  nip:0x184720bc   lr:0x10006b4c   cr:0x38000022   ctr:0x1847209c
  msr:0x0002db00  xer:0x00000000  ret:0xfffffffc dsisr:0x08000000
  gr3:0x00000003   mq:0x00000000 trap:0x00000c00  dar:0x1833114c
```

Power PC ベースの 64 ビット端末のプロセス例外に関するコンテキスト情報を表示します。

<AC> display exception context

```
Index 1 of 1
------------------------------
Crashed PID: 172 (routed)
Crash signal: SIGBUS
Crash time: Sat Sep 15 16:53:16 2007
Core file path:
cfa0:/core/node1_routed_172_7_20070915-165316_1189875196.core
#0  0x00000fff803c66b4
#1  0x0000000010009b94
#2  0x00000fff80401814
Backtrace stopped.
                    Registers' content
    grp00: 0x00000000000000ee 0x00000fffffd04840
    grp02: 0x00000fff80425c28 0x0000000000000004
    grp04: 0x00000fffffd048c0 0x000000000000000a
    grp06: 0xffffffffffffffff 0x00000fff803c66b4
    grp08: 0x000000008002d000 0x0000000000000000
    grp10: 0x0000000000000000 0x0000000000000000
    grp12: 0x0000000000000000 0x00000fff80a096b0
    grp14: 0x000000007b964c00 0x000000007b7d0000
```

```
    grp16: 0x0000000000000001 0x000000000000000b
    grp18: 0x0000000000000031 0x0000000000a205b8
    grp20: 0x0000000000a20677 0x0000000000000000
    grp22: 0x000000007bb91014 0x0000000000000000
    grp24: 0xc0000000005ae1c8 0x0000000000000000
    grp26: 0xc0000001f00bff20 0xc0000001f00b0000
    grp28: 0x00000fffffd04a30 0x000000001001aed8
    grp30: 0x00000fffffd04fae 0x00000fffffd04840

     nip:0x00000fff803c66b4       lr:0x0000000010009b94
      cr:0x0000000058000482      ctr:0x00000fff803c66ac
     msr:0x000000008002d000      xer:0x0000000000000000
     ret:0xfffffffffffffffc    dsisr:0x0000000000000000
     gr3:0x0000000000000003    softe:0x0000000000000001
    trap:0x0000000000000c00      dar:0x00000fff8059d14c
```

MIPS ベースの 32 ビット端末のプロセス例外に関するコンテキスト情報を表示します。

<AC> display exception context

```
Index 1 of 1
------------------------------
Crashed PID: 182 (routed)
Crash signal: SIGBUS
Crash time: Sun Jan  2 08:11:38 2013
Core file path:
cfa0:/core/node4_routed_182_10_20130102-081138_1293955898.core
#0  0x2af2faf4
#1  0x00406d8c
Backtrace stopped.
                    Registers' content
 zero:0x00000000   at:0x1000dc00   v0:0x00000004   v1:0x00000003
   a0:0x00000003   a1:0x7fd267e8   a2:0x0000000a   a3:0x00000001
   t0:0x00000000   t1:0xcf08fa14   t2:0x80230510   t3:0xffffff8
   t4:0x69766520   t5:0x00000000   t6:0x63cc6000   t7:0x44617461
   s0:0x7fd26f81   s1:0x00401948   s2:0x7fd268f8   s3:0x803e1db0
   s4:0x803e1da0   s5:0x803e1d88   s6:0x803e1d70   s7:0x803e1d60
   t8:0x00000008   t9:0x2af2fae0   k0:0x00000000   k1:0x00000000
   gp:0x2af9a3a0   sp:0x7fd267c0   s8:0x7fd267c0   ra:0x00406d8c
   sr:0x0000dc13   lo:0xef9db265   hi:0x0000003f  bad:0x2add2010
cause:0x00800020   pc:0x2af2faf4
```

MIPS ベースの 64 ビット端末のプロセス例外に関するコンテキスト情報を表示します。

<AC> display exception context

```
Index 1 of 1
------------------------------
```

```
Crashed PID: 270 (routed)
Crash signal: SIGBUS
Crash time: Wed Mar 27 12:39:12 2013
Core file path:
cfa0:/core/node16_routed_270_10_20130327-123912_1364387952.core
#0  0x0000005555a3bcb4
#1  0x0000000120006c1c
Backtrace stopped.
                    Registers' content
     zero:0x0000000000000000       at:0x0000000000000014
       v0:0x0000000000000004       v1:0x0000000000000003
       a0:0x0000000000000003       a1:0x000000ffff899d90
       a2:0x000000000000000a       a3:0x0000000000000001
       a4:0x0000005555a9b4e0       a5:0x0000000000000000
       a6:0xffffffff8021349c       a7:0x20696e206368616e
       t0:0x0000000000000000       t1:0xffffffff80105068
       t2:0xffffffff80213890       t3:0x0000000000000008
       s0:0x0000005555a99c40       s1:0x000000ffff89af5f
       s2:0x0000000120007320       s3:0x0000005555a5f470
       s4:0x000000ffff899f80       s5:0xffffffff803cc6c0
       s6:0xffffffff803cc6a8       s7:0xffffffff803cc690
       t8:0x0000000000000002       t9:0x0000005555a3bc98
       k0:0x0000000000000000       k1:0x0000000000000000
       gp:0x0000000120020460       sp:0x000000ffff899d70
       s8:0x000000ffff899d80       ra:0x0000000120006c1c
       sr:0x000000000400fff3       lo:0xdf3b645a1cac08c9
       hi:0x000000000000007f      bad:0x000000555589ba84
    cause:0x0000000000800020       pc:0x0000005555a3bcb4
```

表 7-1 コマンド出力

フィールド	説明
Crashed PID	クラッシュしたプロセスのID

フィールド	説明
Crash signal	クラッシュを引き起こしたシグナル • **SIGABRT**—中断 • **SIGBUS**—バスエラー • **SIGFPE**—間違った四則演算 • **SIGILL**—不正なハードウェア指令 • **SIGQUIT**—コントロール端末によってquit信号が送信されました。 • **SIGSEGV**—不正なメモリアクセス • **SIGSYS**—不正なシステムコール • **SIGTRAP**—トラップメッセージ • **SIGXCPU**—CPU使用率上限を超過しました。 • **SIGXFSZ**—ファイルサイズ上限を超過しました。 • **SIGUNKNOW**—不明な理由
Crash time	クラッシュ発生時間
Core file path	コアファイルが保存されているディレクトリ
Backtrace stopped	すべてのスタック情報が表示されています。

関連コマンド

reset exception context

7.1.2 display exception filepath

Syntax

display exception filepath

View

すべての view

定義済みユーザロール

network-admin

説明

display exception filepath コマンドはコアファイルのディレクトリを表示します。

例

装置のコアファイルのディレクトリを表示します。

<AC> display exception filepath

```
The exception filepath is cfa0:.
```

7.1.3 exception filepath

Syntax

exception filepath *directory*

undo exception filepath *directory*

デフォルト

コアファイルはストレージメディアのルートディレクトリに保存されます。

View

User view

定義済みユーザロール

network-admin

パラメータ

directory: コアファイルを保存するディレクトリを指定します。ルートディレクトのみ可能です。

説明

exception filepath コマンドはコアファイルを保存するディレクトリを設定します。

undo exception filepath コマンドは指定されたディレクトリを削除します。

ルートディレクトリにディレクトリがない場合、以下の動作を行います。

1) コアファイル保存ディレクトリを作成します。
2) ディレクトリにコアファイルを保存します。

本コマンドでディレクトリを変更することができます。

ディレクトリが指定されていない、あるいは指定されたディレクトリがアクセス不能である場合、コアファイルを保存することができません。

例

コアファイルを保存するディレクトリを指定します。

<AC> exception filepath cfa0:/

関連コマンド

- **display exception filepath**
- **process core**

7.1.4 process core

Syntax

process core { **maxcore** *value* | **off** } { **job** *job-id* | **name** *process-name* }

View

User view

デフォルト

プロセスは最初の例外のコアファイルを作成し、後続の例外についてはコアファイルを作成しません。

定義済みユーザロール

network-admin

パラメータ

off: コアファイルの作成を無効にします。

maxcore *value*: コアファイルの作成を有効にし、コアファイルの最大数を設定します。設定範囲は 1～10 です。

name *process-name*: プロセス名を指定します。設定範囲は 1～15 文字です。大文字、小文字を区別しません。

job *job-id*: job ID でプロセスを指定します。設定範囲は 1～2147483647 です。プロセスを再起動しても、job ID は変わりません。

説明

process core コマンドは例外のコアファイルを作成するプロセスを有効あるいは無効にし、コアファイルの最大数を設定します。

本コマンドはプロセスのすべてのインスタンスに適用します。

本コマンドにより、コアファイルが最大数になるまで指定されたプロセスがクラッシュするたびにコアファイルを作成します。コアファイルは例外情報を記録します。

コアファイルがシステムのストレージのリソースを消費するため、例外情報を調査する必要がないプロセスはコアファイルの生成を無効にすることができます。

例

プロセス **routed** のコアファイルの作成を無効にします。

<AC> process core off name routed

プロセス **routed** のコアファイルの作成を有効にし、コアファイルの最大数を 5 に設定します。

<AC> process core maxcore 5 name routed

関連コマンド

- **display exception context**
- **exception filepath**

7.1.5 reset exception context

Syntax

reset exception context

View

User view

定義済みユーザロール

network-admin

説明

reset exception context コマンドはプロセス例外のコンテキスト情報を削除します。

例

プロセス例外のコンテキスト情報を削除します。

<AC> reset exception context

関連コマンド

display exception context

目次

このセクションのページは **11-x-x** です。

8 章 パケットキャプチャ.....8-1
8.1 パケットキャプチャ設定コマンド.....8-1
8.1.1 display packet-capture status.....8-1
8.1.2 packet-capture local ap.....8-2
8.1.3 packet-capture remote ap.....8-4
8.1.4 packet-capture stop.....8-5

8章 パケットキャプチャ

8.1 パケットキャプチャ設定コマンド

8.1.1 display packet-capture status

Syntax

display packet-capture status

View

すべての view

定義済みユーザロール

network-admin

説明

display packet-capture status コマンドを使用して、パケットキャプチャステータス情報を表示します。

例

AP1 の無線 1 のパケットキャプチャステータス情報を表示します。

<AC> display packet-capture status

```
AP name       : ap1
Radio ID      : 1
Radio mode    : 802.11n(2.4GHz)
Channel       : 1
Status        : Capturing
File name     : database.dhcp
Username      : 1
Password      : ******
```

表 8-1 コマンド出力

フィールド	説明
Status	パケットキャプチャステータスです。現在のソフトウェアバージョンでは**Capturing**テータスのみがサポートされています。
Username	リモートFTPサーバにログインするためのユーザ名です。

フィールド	説明
Password	リモートFTPサーバにログインするためのパスワードです。暗号文と平文のそれぞれのパスワードは******として表示されます。パスワードが必要でないか設定されていない場合、このフィールドにはN/Aが表示されます。

関連コマンド

- **packet-capture local ap**
- **packet-capture remote ap**

8.1.2 packet-capture local ap

Syntax

packet-capture local ap *ap-name* **radio** *radio-id* [**capture-filter** *capt-expression* | **limit-frame-size** *bytes* | **autostop filesize** *kilobytes* | **autostop duration** *seconds*] * **write url** *url* [**username** *username* [**password** { **cipher** | **simple** } *key*]]

View

User view

定義済みユーザロール

network-admin

パラメータ

ap-name : AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

radio *radio-id* : ID でラジオを指定します。

capture-filter *capt-expression* ： キャプチャするパケットに一致する条件式を指定します。キャプチャフィルタ条件式を指定しない場合、装置はインタフェース上のすべての受信パケットをキャプチャします。

limit-frame-size *bytes*： パケットをキャプチャする最大バイト数を設定します。値の範囲は 64～8000 バイトで、デフォルト値は 8000 バイトです。

autostop filesize *kilobytes*： ファイルローテーションが無効になっているときに最大パケットファイルサイズを超えた場合、パケットのキャプチャを停止します。*kilobytes* 引

数は、ファイルの最大サイズを設定します。値の範囲は 1～65536 キロバイトです。制限を設定しない場合、ファイルのサイズは無制限です。

autostop duration *seconds*：キャプチャ時間が終了したときにパケットのキャプチャを停止します。*seconds* 引数はキャプチャ時間を設定します。値の範囲は 1～2147483647 秒です。制限を設定しない場合、キャプチャ時間は無制限です。

write url *url*：キャプチャされたパケットデータを格納する FTP サーバ上のファイルの URL を指定します。URL は 1～255 文字の大文字小文字を区別する文字列である必要があります。URL 文字列には、アットマーク（@）、および指定されたユーザ名とパスワードを使用できません。URL を指定しないと、キャプチャされたパケットデータは保存されません。

username *username* : FTP サーバにログインするためのユーザ名を指定します。ユーザ名は、大文字と小文字を区別する 1～32 文字です。

password : FTP サーバにログインするためのパスワードを指定します。

cipher：暗号文のパスワードを指定します。

simple：平文のパスワードを指定します。

key：パスワードを指定します。この引数は大文字と小文字を区別します。**simple** を指定する場合は、1～32 文字の文字列でなければなりません。**cipher** を指定する場合は、1～73 文字の暗号文字列でなければなりません。

説明

packet-capture local ap コマンドを使用して、AP 無線で受信したパケットをキャプチャし、キャプチャしたパケットを FTP サーバ上のファイルに保存します。

パケットのキャプチャ中にキャプチャを停止するには、**packet-capture stop** コマンドを使用します。

autostop filesize オプションと **autostop duration** オプションのそれぞれを設定した場合、停止オプションの制限のいずれかに達すると、パケットキャプチャが停止します。

URL、ユーザ名、パスワードを指定するには、次の制限事項とガイドラインに従ってください。

- FTP サーバの IP アドレスが IPv4 アドレスの場合は、*ftp://FTP server IPv4 address[:port number]/file name* の形式で URL を入力します。
- サーバアドレスフィールドの DNS ドメイン名を指定することもできます。URL の形式は *ftp:///DNS domain name/file name* です。
- ユーザ名とパスワードは、FTP サーバで設定されているものと同じである必要があります。サーバがユーザ名のみを認証する場合、パスワードは省略できます。

autostop duration *seconds* オプションで短いキャプチャ時間を設定しないでください。時間が短すぎると、FTP サーバにログインしていないときにキャプチャが停止することがあります。その場合キャプチャされたパケットは、パケットファイルが作成されていないため保存できません。

例

AP1 の無線 1 で受信パケットをキャプチャします。

<AC> packet-capture local ap ap1 radio 1 write url ftp://10.1.1.1/database.pcap username 1 password simple 1

関連コマンド

- **display packet-capture status**
- **packet-capture stop**

8.1.3 packet-capture remote ap

Syntax

packet-capture remote ap *ap-name* **radio** *radio-id* [**port** *port*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ap-name : AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。

ソフトウェアバージョン 7.2.13 を含む以前のソフトウェアでは大文字と小文字を区別しません。

ソフトウェアバージョン 7.2.18 を含む以降のソフトウェアでは大文字と小文字を区別します。

radio *radio-id* : ID で無線を指定します。

port *port* : AP の RPCAP サービスポートをポート番号で指定します。RPCAP サービスポートを指定しない場合は、RPCAP サービスポート 2002 が使用されます。

説明

packet-capture remote ap コマンドを使用して、AP 無線で受信パケットをキャプチャします。

このコマンドが実行されると、AP の RPCAP サービスポートに接続されたクライアント（Wireshark など）は、AP 無線でキャプチャされたパケットを取得できます。

パケットのキャプチャ中にキャプチャを停止するには、**packet-capture stop** コマンドを使用します。

例

AP1 の無線 2 で受信パケットをキャプチャし、RPCAP サービスポート番号を 2014 として指定します。

<AC> packet-capture remote ap ap1 radio 2 port 2014

関連コマンド

- **display packet-capture status**
- **packet-capture stop**

8.1.4 packet-capture stop

Syntax

packet-capture stop

View

ユーザ view

定義済みユーザロール

network-admin

説明

packet-capture stop コマンドを使用して、パケットキャプチャを停止します。

階層型ネットワーク上のローカル AC がオフラインになると、センターAC は、ローカル AC に接続された AP のパケットキャプチャ管理プロセスを停止します。ただし、AP でのパケットキャプチャは継続されます。パケットキャプチャを停止するには、AP のセンターAC 上でパケットキャプチャを再度有効にして、このコマンドを実行する必要があります。

例

パケットキャプチャを停止します。

<AC> packet-capture stop

関連コマンド

- **packet-capture local ap**
- **packet-capture remote ap**

目次

このセクションのページは **11-x-x** です。

9 章 Information Center 9-1
9.1 Information Center 設定コマンド 9-1
9.1.1 display info-center 9-1
9.1.2 display logbuffer 9-2
9.1.3 display logbuffer summary 9-3
9.1.4 display logfile summary 9-5
9.1.5 enable log updown 9-5
9.1.6 info-center enable 9-6
9.1.7 info-center logbuffer 9-7
9.1.8 info-center logbuffer size 9-7
9.1.9 info-center logfile directory 9-8
9.1.10 info-center logfile enable 9-9
9.1.11 info-center logfile frequency 9-10
9.1.12 info-center logfile size-quota 9-11
9.1.13 info-center loghost 9-12
9.1.14 info-center loghost keep-alive custom-info 9-14
9.1.15 info-center loghost keep-alive enable 9-15
9.1.16 info-center loghost keep-alive interval 9-16
9.1.17 info-center loghost keep-alive level 9-17
9.1.18 info-center loghost source 9-18
9.1.19 info-center source 9-19
9.1.20 info-center synchronous 9-21
9.1.21 info-center syslog min-age 9-22
9.1.22 info-center timestamp 9-23
9.1.23 info-center timestamp loghost 9-24
9.1.24 logfile save 9-25
9.1.25 reset logbuffer 9-25
9.1.26 snmp-agent trap enable syslog 9-26
9.1.27 terminal debugging 9-27
9.1.28 terminal logging level 9-28
9.1.29 terminal monitor 9-29

9章 Information Center

9.1 Information Center設定コマンド

9.1.1 display info-center

Syntax

display info-center

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display info-center コマンドは Information Center の情報を表示します。

例

Information Center の情報を表示します。

<AC> display info-center

```
Information Center: Enabled
Console: Enabled
Monitor: Enabled
Log host: Enabled
   IP address: 192.168.0.1, port number: 5000, host facility: local7
   IP address: 192.168.0.2, port number: 5001, host facility: local5
Log buffer: Enabled
   Max buffer size 1024, current buffer size 512,
   Current messages 0, dropped messages 0, overwritten messages 0
Log file: Enabled
Security log file: Enabled
Information timestamp format:
   Loghost: Date
   Other output destination: Date
```

9.1.2 display logbuffer

Syntax

display logbuffer [**reverse**] [**level** *severity* | **size** *buffersize*] *

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

reverse: 最新のログエントリを年代順で上から表示します。指定しない場合、もっとも古いログエントリを上から表示します。

level *severity*: severity レベルを指定します。設定範囲は 0～7 です。指定しない場合、すべてのレベルのログ情報を表示します。

表 9-1 ログレベル

Severity	レベル	説明	コマンドに対応するキーワード
0	Emergency	システムが使用できません。たとえば、システムの許可が終了しました。	emergency
1	Alert	即急に対応が必要です。たとえば、インタフェースのトラフィックが上限を超えました。	alert
2	Critical	深刻な状態です。たとえば、装置の温度が上限を超えました、電源モジュールが故障しました、FANトレイが故障しました。	critical
3	Error	エラー状態です。たとえば、リンク状態が変更しました。	error
4	Warning	警告状態です。たとえば、インタフェースが切断されました、あるいはメモリリソースが上限まで使われました。	warning
5	Notification	通常通りですが、注意状態です。たとえば、装置にログインしました、あるいは装置が再起動しました。	notification
6	Informational	情報メッセージです。たとえば、コマンドあるいは**ping**コマンドが実行されました。	informational
7	Debugging	デバッグメッセージです。	debugging

説明

display logbuffer コマンドはログバッファの状態とログバッファのログ情報を表示します。

例

ログバッファの状態とログ情報を表示します。

<AC> display logbuffer

```
Log buffer: Enabled
Max buffer size: 1024
Actual buffer size: 512
Dropped messages: 0
Overwritten messages: 0
Current messages: 127
%Jun 19 18:03:24:55 2006 AC SYSLOG /7/SYS_RESTART:System restarted
...
```

表 9-2 コマンド出力

フィールド	説明
Log buffer	• **Enabled**—ログバッファにログを出力できます。 • **Disabled**—ログバッファにログを出力できません。
Max buffer size	装置でサポートしている最大バッファサイズです。
Actual buffer size	**info-center logbuffer size**コマンドで設定された最大バッファサイズです。
Dropped messages	廃棄されたメッセージ数です。
Overwritten messages	上書きされたメッセージ数です。
Current messages	現在のメッセージ数です。

関連コマンド

- **info-center logbuffer**
- **reset logbuffer**

9.1.3 display logbuffer summary

Syntax

display logbuffer summary [**level** *severity*] *

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

level *severity*: severity レベルを指定します。設定範囲は 0～7 です。指定しない場合、すべてのレベルのログ情報を表示します。ログレベルの詳細は表 9-1 を参照してください。

説明

display logbuffer summary コマンドはログバッファの概要を表示します。

例

ログバッファの概要を表示します。

<AC> display logbuffer summary

```
Slot EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
   1     0     0     1    11     4    20    24     0
```

表 9-3 コマンド出力

フィールド	説明
Slot	スロット番号は1に固定されており、意味はありません。
EMERG	emergencyを示します。詳細は表 9-1を参照してください。
ALERT	alertを示します。詳細は表 9-1を参照してください。
CRIT	criticalを示します。詳細は表 9-1を参照してください。
ERROR	errorを示します。詳細は表 9-1を参照してください。
WARN	warningを示します。詳細は表 9-1を参照してください。
NOTIF	notificationを示します。詳細は表 9-1を参照してください。
INFO	informationalを示します。詳細は表 9-1を参照してください。
DEBUG	debugを示します。詳細は表 9-1を参照してください。

9.1.4 display logfile summary

Syntax

display logfile summary

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display logfile summary コマンドはログファイルの設定を表示します。

例

ログファイルの設定を表示します。

<AC> display logfile summary

```
Log file: Enabled.
Log file size quota: 10 MB
Log file directory: cfa0:/logfile
Writing frequency: 0 hour 1 min 10 sec
```

表 9-4 コマンド出力

フィールド	説明
Log file	• **Enabled**—ログをファイルに出力できます。 • **Disabled**—ログをファイルに出力できません。
Log file size quota	ログファイルで予約された最大記憶容量です。単位はMBです。
Log file directory	ログファイルのディレクトリです。
Writing frequency	ログファイルを書き込む間隔です。

9.1.5 enable log updown

Syntax

enable log updown

undo enable log updown

デフォルト

有効

View

Interface view

定義済みユーザロール

network-admin

説明

enable log updown コマンドはインタフェースの状態が変化したとき、インタフェースでリンクアップあるいはリンクダウンのログを作成することを有効にします。

undo enable log updown コマンドはインタフェースの状態が変化したとき、インタフェースでリンクアップあるいはリンクダウンのログを作成することを無効にします。

例

GigabitEthernet1/0/1 でリンクアップあるいはリンクダウンのログを作成することを無効にします。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] undo enable log updown

9.1.6 info-center enable

Syntax

info-center enable

undo info-center enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

info-center enable コマンドは Information Center を有効にします。

undo info-center enable コマンドは Information Center を無効にします。

例

Information Center を有効にします。

<AC> system-view

[AC] info-center enable

```
Information center is enabled.
```

9.1.7 info-center logbuffer

Syntax

info-center logbuffer

undo info-center logbuffer

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

info-center logbuffer コマンドはログバッファにログの出力を有効にします。

undo info-center logbuffer コマンドはログバッファにログの出力を無効にします。

例

ログバッファにログ情報を出力するように設定します。

<AC> system-view

[AC] info-center logbuffer

関連コマンド

- **display logbuffer**
- **info-center enable**

9.1.8 info-center logbuffer size

Syntax

info-center logbuffer size *buffersize*

undo info-center logbuffer size

デフォルト

512

View

System view

定義済みユーザロール

network-admin

パラメータ

buffersize: ログバッファに記憶できるログの最大数を指定します。設定範囲は 0～1024 です。デフォルトは 512 です。

説明

info-center logbuffer size コマンドはログバッファに記憶できるログの最大数を設定します。

undo info-center logbuffer size コマンドはデフォルトに戻します。

例

ログバッファに記憶できるログの最大数を 50 に設定します。

<AC> system-view

[AC] info-center logbuffer size 50

ログのバッファサイズをデフォルトに戻します。

<AC> system-view

[AC] undo info-center logbuffer size

関連コマンド

- **display logbuffer**
- **info-center enable**

9.1.9 info-center logfile directory

Syntax

info-center logfile directory *dir-name*

デフォルト

ログファイルは、ストレージ装置のルートディレクトリ下の **logfile** ディレクトリに保存されます。

View

System view

定義済みユーザロール

network-admin

パラメータ

dir-name: ディレクトリ名を指定します。設定範囲は 1～64 文字です。

説明

info-center logfile directory コマンドはログファイルが保存されるディレクトリを設定します。

指定されたディレクトリは作成されている必要があります。

ログファイルの拡張子は“.log”です。ファイルを記録するためにデフォルトディレクトリに十分な容量がない場合、ログファイルに新しいディレクトリを指定することができます。

このコマンドの設定は、再起動で削除されます。

例

ディレクトリ名 **test** を cfa0 のルートディレクトリの下に作成します。

<AC> mkdir test

```
Creating directory cfa0:/test... Done.
```

ログファイルディレクトリを **cfa0:/test** に設定します。

<AC> system-view

[AC] info-center logfile directory cfa0:/test

```
The directory is in primary partition.
```

関連コマンド

info-center logfile enable

9.1.10 info-center logfile enable

Syntax

info-center logfile enable

undo info-center logfile enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

info-center logfile enable コマンドはログファイル機能を有効にします。

undo info-center logfile enable コマンドはログファイル機能を無効にします。

例

ログファイルにログを出力することを有効にします。

<AC> system-view

[AC] info-center logfile enable

9.1.11 info-center logfile frequency

Syntax

info-center logfile frequency *freq-sec*

undo info-center logfile frequency

デフォルト

86400 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

freq-sec: ログファイルにシステムがログを保存する間隔を指定します。設定範囲は 1～86400 秒です。

説明

info-center logfile frequency コマンドはログバッファからログファイルにログを保存する間隔を設定します。

undo info-center logfile frequency コマンドはデフォルトに戻します。

このコマンドを実行することで、指定した間隔でログファイルに、ログファイルのバッファのログを自動で保存します。

例

ログファイルにログを保存する間隔を 60000 秒に設定します。

<AC> system-view

[AC] info-center logfile frequency 60000

関連コマンド

info-center logfile enable

9.1.12 info-center logfile size-quota

Syntax

info-center logfile size-quota *size*

undo info-center logfile size-quota

デフォルト

ログファイルの最大サイズは 10 MB です。

View

System view

定義済みユーザロール

network-admin

パラメータ

size: ログファイルの最大サイズを指定します。設定範囲は 1～10MB です。

説明

info-center logfile size-quota コマンドはログファイルの最大サイズを設定します。

undo info-center logfile size-quota コマンドはデフォルトに戻します。

例

ログファイルの最大サイズを 6MB に設定します。

<AC> system-view

[AC] info-center logfile size-quota 6

関連コマンド

info-center logfile enable

9.1.13 info-center loghost

🕮 メモ：

下記のパラメータは、ソフトウェアバージョン 7.2.73 を含む以降のソフトウェアからサポートしています。

- **format rfc5424-json-v1**
- **end-with-length**
- **tcp**
- **ssl-client-policy** *policy-name*
- **directory** *dir-name* **size-quota** *size*

Syntax

info-center loghost { *hostname* | *ipv4-address* } [**port** *port-number*] [**facility** *local-number*] | [**format rfc5424-json-v1 tcp** [**end-with-length**] **ssl-client-policy** *ssl-client-policy-name* **directory** *dir-name* **size-quota** *size*] | **tcp** [**ssl-client-policy** *policy-name*]]

undo info-center loghost { *hostname* | *ipv4-address* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

hostname: ログホスト名を指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含むことができます。

ipv4-address: ログホストの IPv4 アドレスを指定します。

port *port-number*: ログホストのポート番号を指定します。設定範囲は 1～65535 です。デフォルトは 514 です。設定された値はログホストで設定された値と同じにする必要があります。そうでない場合、ログホストはシステム情報を受信できません。

facility *local-number*: ログホストのロギング facility を指定します。設定範囲は local0～local7 です。デフォルトは local7 です。ロギング facility は異なるロギングの送信元、query、ログのフィルタリングを識別するために使用します。

format rfc5424-json-v1 :ログホストに送信されるログの形式として RFC5424-JSON-v1 を指定します。この形式では、ログのコンテンツフィールドは JSON 形式を使用し、ログの他のフィールドは RFC5424 形式を使用します。このキーワードを指定しない場合、info-center format コマンドで指定された形式が使用されます。

end-with-length：ログの末尾を示す Length フィールドを保持します。このキーワードを指定しない場合、ログの末尾を示すために改行文字 (¥n) が使用されます。

tcp: TCP を使用してログを送信します。デフォルトは、UDP を使用してログを送信します。

ssl-client-policy *policy-name*: TCP 経由で送信されるログを SSL によって暗号化します。*policy-name* 引数は、SSL クライアントポリシーの名前を大文字と小文字を区別しない 1 から 31 文字の文字列です。このオプションを指定しない場合、ログは暗号化されていない形式でログホストに送信されます。

SSL を使用して TCP 経由で送信されるログを暗号化するには、事前に SSL クライアントポリシーを設定する必要があります。SSL クライアントポリシーを設定していない場合、SSL 接続を確立できずログの送信に発生します。SSL クライアントポリシーの詳細については、オペレーションマニュアルのセクション 9 *セキュリティ*“*SSL*”を参照してください。

directory *dir-name* **size-quota** *size*：装置とログホスト間の TCP 接続が切断されたときに、ログホストにファイル形式で送信する必要があるログをローカルに保存するディレクトリを指定します。*dir-name* 引数は、ディレクトリの絶対パスを表す 1 から 64 文字の文字列です。ログファイル名は、このコマンドで指定したログホストの IP アドレスまたは名前に基づいて自動的に生成されます。*size* 引数は、ログファイルのサイズを 1 から 70 MB の範囲で表します。指定したサイズに達すると、デバイスは最も古いログを削除して新しいログを保存します。

説明

info-center loghost コマンドはログホストを指定し、出力パラメータを設定します。

undo info-center loghost コマンドはデフォルトに戻します。

info-center enable コマンドで有効にしたのち、**info-center loghost** コマンドは適用されます。

装置は最大 4 のログホストをサポートします。

例

ログホスト 1.1.1.1 にログを出力します。

<AC> system-view

[AC] info-center loghost 1.1.1.1

#ログホスト 1.1.1.1 に TCP 経由で送信されるログを SSL を用いて暗号化して送信します。SSL クライアントポリシーとして tls-test を指定します。

<AP> system-view

[AP] info-center loghost 1.1.1.1 tcp ssl-client-policy tls-test

9.1.14 info-center loghost keep-alive custom-info

🕮 **メモ**:

このコマンドは、ソフトウェアバージョン 7.2.85a を含む以降のソフトウェアからサポートしています。

Syntax

info-center loghost keep-alive custom-info *text*

undo info-center loghost keep-alive custom-info

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

text: カスタム情報を 1 から 255 文字の文字列で指定します。

説明

info-center loghost keep-alive custom-info コマンドはキープアライブログに含めるカスタム情報を設定します。

undo info-center loghost keep-alive custom-info コマンドはデフォルトに戻します。

キープアライブログにカスタム情報を含めることで、ログ解析やトラブルシューティングを容易にします。

カスタム情報には、デバイスの設置位置、デバイス ID、その他備考の情報を含めることができます。

カスタム情報には ASCII 文字のみ設定できます。特殊文字は使用できません。

例

キープアライブログにカスタム情報として No.123 を設定します。

<AC> system-view

[AC] info-center loghost keep-alive custom-info No.123

関連コマンド

- **info-center loghost keep-alive enable**
- **info-center loghost keep-alive interval**

- **info-center loghost keep-alive level**

9.1.15 info-center loghost keep-alive enable

🕮 **メモ**:

このコマンドは、ソフトウェアバージョン 7.2.85a を含む以降のソフトウェアからサポートしています。

Syntax

info-center loghost keep-alive enable

undo info-center loghost keep-alive enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

info-center loghost keep-alive enable コマンドはキープアライブログ送信を有効にします。

undo info-center loghost keep-alive enable コマンドはデフォルトに戻します。

この機能を有効にすると、装置は設定された全てのログホストに対して定期的にキープアライブログを送信します。

キープアライブログを定期的に受信することにより、装置の運用状態を確認できるようにします。

例

キープアライブログの送信を有効にします。

<AC> system-view

[AC] info-center loghost keep-alive enable

関連コマンド

- **info-center loghost**
- **info-center loghost keep-alive interval**
- **info-center loghost keep-alive level**

- **info-center loghost keep-alive message**

9.1.16 info-center loghost keep-alive interval

> 🕮 **メモ**:
> このコマンドは、ソフトウェアバージョン 7.2.85a を含む以降のソフトウェアからサポートしています。

Syntax

info-center loghost keep-alive interval *seconds*

undo info-center loghost keep-alive interval

デフォルト

60 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

seconds: キープアライブログを送信する間隔を 60 から 3600 秒の範囲で指定します。

説明

info-center loghost keep-alive interval コマンドはキープアライブログ送信間隔を設定します。

undo info-center loghost keep-alive interval コマンドはデフォルトに戻します。

例

キープアライブログの送信間隔を 180 秒に設定します

<AC> system-view

[AC] info-center loghost keep-alive interval 180

9.1.17 info-center loghost keep-alive level

> 🕮 **メモ：**
>
> このコマンドは、ソフトウェアバージョン 7.2.85a を含む以降のソフトウェアからサポートしています。

Syntax

info-center loghost keep-alive level *severity*

undo info-center loghost keep-alive level

デフォルト

Informational

View

System view

定義済みユーザロール

network-admin

パラメータ

severity: キープアライブログのレベルを、alert、critical、debugging、emergency、error、informational、notification、warning のいずれかで指定します。

説明

info-center loghost keep-alive level コマンドはキープアライブログのレベルを設定します。

undo info-center loghost keep-alive level コマンドはデフォルトに戻します。

装置は指定されたレベルでキープアライブログをログホストへ送信します。

例

キープアライブログのレベルを notification に設定します

<AC> system-view

[AC] info-center loghost keep-alive level notification

関連コマンド

- **info-center loghost keep-alive enable**
- **info-center loghost keep-alive interval**
- **info-center loghost keep-alive message**

9.1.18 info-center loghost source

Syntax

info-center loghost source *interface-type interface-number*

undo info-center loghost source

デフォルト

出力ログの送信元 IP アドレスは、ルートの送信インタフェースに一致するプライマリ IP アドレスです。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: 送信インタフェースのタイプと番号を指定します。ログを出力するため物理インタフェースが使用されても、システムはログ情報の送信元 IP アドレスとして指定された送信インタフェースのプライマリ IP アドレスを使います。

説明

info-center loghost source コマンドは出力ログの送信元 IP アドレスを指定します。

undo info-center loghost source コマンドはデフォルトに戻します。

info-center enable コマンドで有効にしたのち、**info-center loghost source** コマンドは適用されます。

例

出力ログの送信元 IP アドレスとしてループバック 0 の IP アドレスを指定します。

<AC> system-view

[AC] interface loopback 0

[AC-LoopBack0] ip address 2.2.2.2 32

[AC-LoopBack0] quit

[AC] info-center loghost source loopback 0

9.1.19 info-center source

Syntax

info-center source { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** } { **deny** | **level** *severity* }

undo info-center source { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** }

デフォルト

表 9-5 にデフォルトのログ出力ルールを示します。

表 9-5 デフォルト出力ルール

宛先	送信元モジュール	共通ログ	セキュリティログ	Diagnostic ログ	Hidden ログ
コンソール	サポートされるすべてのモジュール	debugging	無効	無効	無効
モニタ端末	サポートされるすべてのモジュール	debugging	無効	無効	無効
ログホスト	サポートされるすべてのモジュール	informational	無効	無効	informational
ログバッファ	サポートされるすべてのモジュール	informational	無効	無効	informational
ログファイル	サポートされるすべてのモジュール	informational	無効	無効	informational
セキュリティログファイル	サポートされるすべてのモジュール。フィルタはできません。	無効	debugging、フィルタはできません。	無効	無効
Diagnosticログファイル	サポートされるすべてのモジュール。フィルタはできません。	無効	無効	debugging。フィルタはできません。	無効

View

System view

定義済みユーザロール

network-admin

パラメータ

module-name: モジュールの名前を指定します。たとえば、FTP の情報を出力する場合、FTP を指定します。装置でサポートされているモジュールを表示する場合、**info-center source ?**コマンドを使用します。

default: すべてのモジュールを指定します。すべてのモジュールを表示するには **info-center source ?**コマンドを使用します。

console: コンソールにログを出力します。

logbuffer: ログバッファにログを出力します。

logfile: ログファイルにログを出力します。

loghost: ログホストにログを出力します。

monitor: モニタ端末にログを出力します。

deny: ログの出力を無効にします。

level *severity*: severity レベルを指定します。設定範囲は 0～7 です。詳細は表 9-1 を参照してください。出力を許可/拒否されたログのもっとも低い severity レベルを指定することができます。

説明

info-center source コマンドはモジュールのログの出力ルールを設定します。

undo info-center source コマンドはデフォルトに戻します。

モジュールの出力ルールを指定しない場合、**default** パラメータを使用して出力ルールを設定することができます。

複数回、モジュールのコマンドを実行した場合、最後に設定したモジュールの出力ルールが適用されます。

モジュールの出力ルールを設定した後、ルールの修正あるいは削除を行う場合、*module-name* パラメータを使用する必要があります。**default** パラメータを使用して設定された新しい出力ルールはモジュールで適用されません。

例

コンソールに emergency 以上の severity の VLAN モジュールの情報を出力します。

<AC> system-view

[AC] info-center source default console deny

[AC] info-center source vlan console level emergency

以前の設定をもとにして、コンソールにシステム情報を出力しないように、VLAN モジュールの情報の出力を無効にします。

<AC> system-view

[AC] undo info-center source vlan console

9.1.20 info-center synchronous

Syntax

info-center synchronous

undo info-center synchronous

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

info-center synchronous コマンドは情報の同期出力を有効にします。

undo info-center synchronous コマンドは情報の同期出力を無効にします。

情報の同期出力とは、システムログの出力によりユーザの入力が中断された場合、中断されたところから操作を継続できるようにします。ログの出力後、編集モードのコマンドプロンプト、あるいは対話モードの“[Y/N]”の文字列を表示し、以前に入力されたコマンドおよび、コマンドプロンプトを表示させることができます。

例

情報の同期出力を有効にし、装置の現在の設定を表示する **display current-configuration** コマンドを行います。

<AC> system-view

[AC] info-center synchronous

Info-center synchronous output is on

[AC] display current-

このとき、システムがログ情報を受信します。最初にログ情報を表示し、次に直前に入力したコマンドを表示します。この例では、display current-です。

```
%May 21 14:33:19:425 2007 AC SHELL/4/LOGIN: VTY login from 192.168.1.44
```

[AC] display current-

display current-configuration コマンドを完全に入力し、Enter キーを押下し、コマンドを実行します。

情報の同期出力を有効にし、現在の設定を保存します。（インタラクティブの情報を入力します）

<AC> system-view

[AC] info-center synchronous

Info-center synchronous output is on

[AC] save

```
The current configuration will be written to the device. Are you sure? [Y/N]:
```

このとき、システムがログ情報を受信します。最初にログ情報を表示し、次に[Y/N]を表示します。

```
%May 21 14:33:19:425 2007 AC SHELL/4/LOGIN: VTY login from 192.168.1.44
[Y/N]:
```

入力を完了するため、“Y”あるいは“N”を入力します。

9.1.21 info-center syslog min-age

Syntax

info-center syslog min-age *min-age*

undo info-center syslog min-age

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

min-age: ログの最小保存期間を指定します。設定範囲は 1～8760 時間です。

説明

info-center syslog min-age コマンドはログをログバッファとログホストに保存する最小保存期間を設定します。

undo info-center syslog min-age コマンドはデフォルトに戻します。

例

ログの最小保存期間を 168 時間に設定します。

<AC> system-view

[AC] info-center syslog min-age 168

9.1.22 info-center timestamp

Syntax

info-center timestamp { **boot** | **date** | **none** }

undo info-center timestamp

デフォルト

date

View

System view

定義済みユーザロール

network-admin

パラメータ

boot: システムが起動してからの経過時間のタイムスタンプを指定します。形式は xxx.yyy です。xxx は上位 32 ビットです。単位はミリ秒です。yyy は下位 32 ビットです。たとえば 0.21990989 は Jun 25 14:09:26:881 2007 です。

date: 現在のシステム時間のタイムスタンプを指定します。形式は MMM DD hh:mm:ss:xxx YYYY です。たとえば、Dec 8 10:12:21:708 2007 です。

- MMM: 省略した月です。Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec があります。
- DD: 日です。9 日までの場合はスペースで始まります。たとえば、7 です。
- hh:mm:ss:xxx: ローカル時間です。hh の設定範囲は 00～23 で、mm と ss の設定範囲は 00～59 です。xxx の設定範囲は 0～999 です。
- YYYY: 年です。

none: 時間の情報を提供しないように指定します。

説明

info-center timestamp コマンドはコンソール、モニタ、ログバッファ、ログファイルに送信するシステム情報のタイムスタンプの形式を設定します。

undo info-center timestamp コマンドはデフォルトに戻します。

例

ログ情報のタイムスタンプの形式を boot に設定します。

<AC> system-view

[AC] info-center timestamp boot

関連コマンド

info-center timestamp loghost

9.1.23 info-center timestamp loghost

Syntax

info-center timestamp loghost { **date** | **iso** | **no-year-date** | **none** }

undo info-center timestamp loghost

デフォルト

date

View

System view

定義済みユーザロール

network-admin

パラメータ

date: 現在のシステム時間のタイムスタンプを指定します。形式は mmm dd hh:mm:ss yyyy です。たとえば、Dec 8 10:12:21 2007 です。

iso: iso 8601 形式のタイムスタンプを指定します。たとえば、2009-09-21T15:32:55 です。

no-year-date: 年を除く現在のシステム日時のタイムスタンプを指定します。

none: 時間の情報を提供しないように指定します。

説明

info-center timestamp loghost コマンドはログホストに送信するシステム情報のタイムスタンプの形式を設定します。

undo info-center timestamp loghost コマンドはデフォルトに戻します。

例

ログホストに送信するシステム情報のタイムスタンプの形式を no-year-date に設定します。

<AC> system-view

[AC] info-center timestamp loghost no-year-date

関連コマンド

info-center timestamp

9.1.24 logfile save

Syntax

logfile save

View

すべての view

定義済みユーザロール

2: System level

説明

logfile save コマンドはログファイルにログファイルバッファのログを手動で保存します。

info-center logfile directory コマンドを使用して、ログファイルに保存するディレクトリを指定することができます。

自動あるいは手動でバッファからログファイルにログを保存したのち、ログファイルのバッファを削除します。

例

ログファイルバッファからログファイルにログを手動で保存します。

<AC> logfile save

```
The contents in the log file buffer have been saved to the file
cfa0:/logfile/logfile.log.
```

関連コマンド

- **info-center logfile enable**
- **info-center logfile directory**

9.1.25 reset logbuffer

Syntax

reset logbuffer

View

User view

定義済みユーザロール

network-admin

説明

reset logbuffer コマンドはログバッファを削除します。

例

ログバッファを削除します。

<AC> reset logbuffer

関連コマンド

display logbuffer

9.1.26 snmp-agent trap enable syslog

Syntax

snmp-agent trap enable syslog

undo snmp-agent trap enable syslog

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable syslog コマンドはログメッセージの SNMP notification の送信を有効にします。

undo snmp-agent trap enable syslog コマンドはログメッセージの SNMP notification の送信を無効にします。

snmp-agent trap enable syslog コマンドを有効にすると、装置はシスログメッセージによる SNMP notification の送信を有効にします。

装置は SNMP notification をカプセル化し、SNMP モジュールとログバッファに送信します。

SNMP モジュールが受信した SNMP notification を正常に送信するため、装置で SNMP の設定を行ってください。SNMP の設定については、オペレーションマニュアルのセクション 11 *システム管理 “SNMP”* を参照してください。

例

ログメッセージの SNMP notification の送信を有効にします。

<AC> system-view

[AC] snmp-agent trap enable syslog

9.1.27 terminal debugging

Syntax

terminal debugging

undo terminal debugging

デフォルト

無効

View

User view

定義済みユーザロール

network-admin

説明

terminal debugging コマンドは現在の端末にデバッグ情報を表示することを有効にします。

undo terminal debugging コマンドは現在の端末にデバッグ情報を表示することを無効にします。

コンソールでデバッグ情報を表示する場合、以下の処理を実行します。

1) **terminal debugging** コマンドを実行します。
2) Information Center を有効にします。（デフォルトで有効です）
3) 関連するデバッグを有効にするため、**debugging** コマンドを使用します。

モニタ端末でデバッグ情報を表示する場合、以下の処理を実行します。

1) **terminal monitor** コマンド、**terminal debugging** コマンドを実行します。
2) Information Center を有効にします。（デフォルトで有効です）
3) 関連するデバッグを有効にするため、**debugging** コマンドを使用します。

このコマンドの設定は端末と装置における現在の接続のみ有効です。新しい接続が確立された場合、デフォルトに戻ります。

端末におけるデバッグ情報の表示設定はデフォルト（無効）となります。

terminal logging level 7 コマンドを実行し、現在の端末でデバッグ情報を表示することができます。**terminal debugging** コマンドとの相違を以下に示します。

- **terminal logging level 7** コマンドは現在の端末のすべてのレベル（レベル 0～レベル 7）のためにログを表示します。
- **terminal logging** コマンドは以下の severity レベルのためにログを表示します。

- debug レベル（レベル 7）
- **terminal logging level** のコマンドによって指定された severity 以上のレベルのために **terminal debugging** コマンドはログを表示します。

例

現在の端末でデバッグ情報を表示することを有効にします。

<AC> terminal debugging

```
The current terminal is enabled to display debugging information.
```

関連コマンド

- **terminal logging level**
- **terminal monitor**

9.1.28 terminal logging level

Syntax

terminal logging level *severity*

undo terminal logging level

デフォルト

6

View

User view

定義済みユーザロール

network-admin

パラメータ

severity: 現在の端末に出力できるログのもっとも低いレベルを指定します。設定範囲は 0～7 です。

説明

terminal logging level コマンドは現在の端末に出力できるログのもっとも低いレベルを設定します。

undo terminal logging level コマンドはデフォルトに戻します。

現在の端末に出力できるログのもっとも低いレベルを指定した場合、装置は指定されたレベル以上の severity レベルのログを出力します。たとえば、現在の端末に出力できるログのもっとも低いレベルを 6（informational）に指定した場合、0～6 の severity レベルのログを設定します。

このコマンドの設定は端末と装置における現在の接続のみ有効です。新しい接続が確立された場合、デフォルトに戻ります。

例

現在の端末に出力できるログのもっとも低いレベルを 7（debug）に設定します。

<AC> terminal logging level 7

9.1.29 terminal monitor

Syntax

terminal monitor

undo terminal monitor

デフォルト

ログの出力はコンソールで有効です。モニタ端末は無効です。

View

User view

定義済みユーザロール

network-admin

説明

terminal monitor コマンドは現在の端末にログを表示することを有効にします。

undo terminal monitor コマンドは現在の端末にログを表示することを無効にします。

このコマンドの設定は端末と装置における現在の接続のみ有効です。新しい接続が確立された場合、デフォルトに戻ります。

例

現在の端末にログを表示することを有効にします。

<AC> terminal monitor

```
The current terminal is enabled to display logs.
```

目次

このセクションのページは **11-x-x** です。

10 章 ポートミラーリング 10-1
10.1 ポートミラーリング設定コマンド 10-1
10.1.1 display mirroring-group 10-1
10.1.2 mirroring-group 10-2
10.1.3 mirroring-group mirroring-port (interface view) 10-3
10.1.4 mirroring-group mirroring-port (system view) 10-4
10.1.5 mirroring-group monitor-port (interface view) 10-5
10.1.6 mirroring-group monitor-port (system view) 10-6

10章 ポートミラーリング

10.1 ポートミラーリング設定コマンド

10.1.1 display mirroring-group

Syntax

display mirroring-group { *group-id* | **all** | **local** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-id: ミラーリンググループの番号を 1～2 の範囲で指定します。

all: すべてのミラーリンググループを指定します。

local: ローカルミラーリンググループを指定します。

説明

display mirroring-group コマンドを使用して、ミラーリンググループを表示します。

ミラーリンググループの情報には、ミラーリンググループのタイプ、ステータス、内容が含まれます。ミラーリンググループ番号でソートされます。

例

すべてのミラーリンググループに関する情報を表示します。

<AC> display mirroring-group all

```
Mirroring group 1:
   Type: Local
   Status: Active
   Mirroring port:
      GigabitEthernet1/0/1  Inbound
   Monitor port: GigabitEthernet1/0/2
```

表 10-1 コマンド出力

フィールド	説明
Mirroring group	ミラーリンググループの番号です。
Type	ミラーリンググループのタイプです。 このデバイスは、ローカルミラーリンググループのみをサポートしています。
Status	ミラーリンググループのステータスです。 ● Active—ミラーリンググループが有効になりました。 ● Incomplete—ミラーリンググループの設定が完了せず、有効になりません。
Mirroring port	送信元ポートです。
Monitor port	宛先ポートです。

10.1.2 mirroring-group

Syntax

mirroring-group *group-id* **local**

undo mirroring-group { *group-id* | **all** | **local** }

デフォルト

ミラーリンググループは存在しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id: ミラーリンググループの番号を 1～2 の範囲で指定します。

local: ローカルミラーリンググループを指定します。

all: すべてのミラーリンググループを指定します。

説明

mirroring-group コマンドを使用して、ミラーリンググループを作成します。

undo mirroring-group コマンドを使用して、ミラーリンググループを削除します。

例

ローカルミラーリンググループを作成します。

<AC> system-view

[AC] mirroring-group 1 local

10.1.3 mirroring-group mirroring-port (interface view)

Syntax

mirroring-group *group-id* **mirroring-port** { **both** | **inbound** | **outbound** }

undo mirroring-group *group-id* **mirroring-port**

デフォルト

ポートは、ミラーリンググループの送信元ポートとして機能しません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

group-id: 1～2 の範囲内の番号でミラーリンググループを指定します。指定したミラーリンググループが既に存在している必要があります。

both: 受信パケットと送信パケットの両方をミラーリングします。

inbound: 受信パケットのみミラーリングします。

outbound: 送信パケットのみミラーリングします。

説明

mirroring-group mirroring-port コマンドを使用して、ポートをミラーリンググループの送信元ポートとして設定します。

undo mirroring-group mirroring-port コマンドを使用して、デフォルトを復元します。

レイヤ 2 アグリゲートインタフェースは、ミラーリンググループの送信元ポートとして設定することはできません。

ポートは、1 つのミラーリンググループの送信元ポートとして機能できます。

送信元ポートはモニタポートとして使用できません。

例

ローカルミラーリンググループ 1 を作成して、GigabitEthernet 1/0/1 の双方向トラフィックを監視します。

<AC> system-view

[AC] mirroring-group 1 local

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] mirroring-group 1 mirroring-port both

関連コマンド

mirroring-group

10.1.4 mirroring-group mirroring-port (system view)

Syntax

mirroring-group *group-id* **mirroring-port** *interface-list* { **both** | **inbound** | **outbound** }

undo mirroring-group *group-id* **mirroring-port** *interface-list*

デフォルト

ミラーリンググループに送信元ポートが設定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id: 1～2 の範囲内の番号でミラーリンググループを指定します。指定したミラーリンググループが既に存在している必要があります。

interface-list: 8 つまでのポート項目のスペース区切りのリストを指定します。各項目は、単一のポートまたはポート範囲を *interface-type interface-number1*～*interface-type interface-number2* の形式で指定します。指定されたインタフェースは同じタイプで、同じカードでなければなりません。*interface-number2* 引数の値は、*interface-number1* 引数の値以上でなければなりません。

both: 受信パケットと送信パケットの両方をミラーリングします。

inbound: 受信パケットのみミラーリングします。

outbound: 送信パケットのみミラーリングします。

説明

mirroring-group mirroring-port コマンドを使用して、ミラーリンググループの送信元ポートを設定します。

undo mirroring-group mirroring-port コマンドを使用して、ミラーリンググループからソースポートを削除します。

レイヤ 2 アグリゲートインタフェースは、ミラーリンググループの送信元ポートとして設定することはできません。

ポートは、1 つのミラーリンググループの送信元ポートとして機能できます。

送信元ポートはモニタポートとして使用できません。

例

ローカルミラーリンググループ 1 を作成して、GigabitEthernet 1/0/1 の双方向トラフィックを監視します。

<AC> system-view

[AC] mirroring-group 1 local

[AC] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both

関連コマンド

mirroring-group

10.1.5 mirroring-group monitor-port (interface view)

Syntax

mirroring-group *group-id* **monitor-port**

undo mirroring-group *group-id* **monitor-port**

デフォルト

ポートは、ミラーリンググループのモニタポートとして機能しません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

group-id: 1～2 の範囲内の番号でミラーリンググループを指定します。指定したミラーリンググループが既に存在している必要があります。

説明

mirroring-group monitor-port コマンドを使用して、ミラーリンググループのモニタポートとして設定します。

undo mirroring-group monitor-port コマンドを使用して、デフォルトを復元します。

ミラーリンググループのモニタポートでスパニングツリー機能を有効にしないでください。

ミラーリンググループのモニタポートとして設定されたレイヤ 2 アグリゲートインタフェースの場合、そのメンバポートをミラーリンググループの送信元ポートとして設定しないでください。

ポートミラーリングにのみモニタポートを使用するため、データ監視デバイスはミラーリングされたトラフィックのみを受信して分析します。

既存のミラーリンググループのポートをモニタポートとして設定しないでください。

例

ローカルミラーリンググループ 1 を作成し、モニタポートとして GigabitEthernet 1/0/1 を設定します。

<AC> system-view

[AC] mirroring-group 1 local

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] mirroring-group 1 monitor-port

関連コマンド

mirroring-group

10.1.6 mirroring-group monitor-port (system view)

Syntax

mirroring-group *group-id* **monitor-port** *interface-list*

undo mirroring-group *group-id* **monitor-port** *interface-list*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id: 1～2 の範囲内の番号でミラーリンググループを指定します。指定したミラーリンググループが既に存在している必要があります。

interface-list: 8 つまでのポート項目のスペース区切りのリストを指定します。各項目は、単一のポートまたはポート範囲を *interface-type interface-number1*～*interface-type interface-number2* の形式で指定します。*interface-number2* 引数の値は、*interface-number1* 引数の値以上でなければなりません。

説明

mirroring-group monitor-port コマンドを使用して、ミラーリンググループのモニタポートを設定します。

undo mirroring-group monitor-port コマンドを使用して、ミラーリンググループからモニタポートを削除します。

ミラーリンググループのモニタポートでスパニングツリー機能を有効にしないでください。

ミラーリンググループのモニタポートとして設定されたレイヤ 2 アグリゲートインタフェースの場合、そのメンバポートをミラーリンググループの送信元ポートとして設定しないでください。

ポートミラーリングにのみモニタポートを使用するため、データ監視デバイスはミラーリングされたトラフィックのみを受信します。

既存のミラーリンググループのポートをモニタポートとして設定しないでください。

例

ローカルミラーリンググループ 1 を作成し、モニタポートとして GigabitEthernet 1/0/1 を設定します。

<AC> system-view

[AC] mirroring-group 1 local

[AC] mirroring-group 1 monitor-port gigabitethernet 1/0/1

関連コマンド

mirroring-group

目次

このセクションのページは **11-x-x** です。

11 章 NetMeister 11-1
11.1 Netmeister コマンド 11-1
11.1.1 display netmeister 11-1
11.1.2 netmeister account 11-3
11.1.3 netmeister alarm enable notice 11-5
11.1.4 netmeister enable 11-5
11.1.5 netmeister event log enable 11-6
11.1.6 netmeister event syslog enable 11-7
11.1.7 netmeister management ip 11-8
11.1.8 netmeister mode 11-9
11.1.9 netmeister parent ip 11-10
11.1.10 netmeister parent-mode mqtt port 11-11
11.1.11 netmeister parent-mode sitename 11-12
11.1.12 netmeister proxy 11-13
11.1.13 netmeister update 11-14
11.1.14 netmeister track 11-15

11章 NetMeister

🕮 **メモ:**

Version 7.2.21 を含む以降のソフトウェアからサポートしています。

11.1 Netmeisterコマンド

11.1.1 display netmeister

Syntax

display netmeister

View

すべての view

定義済みユーザロール

network-admin

説明

display netmeister コマンドは NetMeister 及び親機との接続情報を表示します。

例

子機モードの装置で NetMeisetr 及び親機との接続情報を表示します。

<Switch> display netmeister

```
NetMeister state                              : Enabled
Mode                                           : Child
Connection state with NetMeister              : Connected
Account name                                  : nec
Proxy information:
  State                                 : Connected
  URL                                  : http://www.abc.com:8080
  Username                             : admin
Parent 1:
  IP address                                 : 192.168.0.254
  Port number                                : 443
  Connection state                           : Connected
Parent 2:
  IP address                                 : 192.168.0.255
  Port number                                : 8443
```

```
  Connection state                          : Connected
```

親機モードの装置で NetMeisetr との接続情報を表示します。

<Switch> display netmeister

```
NetMeister state                            : Enabled
Mode                                         : Parent
Connection state with NetMeister            : Connected
Account name                                : nec
Proxy information:
State                                       :  --
Parent information:
Site name                                   : test
Interval                                    : 3600 sec
MQTT interval                               : 60 sec
MQTT status                                 : Connected
```

表 11-1 コマンド出力

フィールド	説明
NetMeister state	NetMeister機能の状態です。 ● **Enabled** —有効 ● **Disabled** —無効
Mode	NetMeisterへの接続モードです。 ● **Parent** —親機モード ● **Child** —子機モード
Connection state with NetMeister	NetMeisterとの接続状況です。 ● **Connected.**—接続 ● **Disconnected.**—切断
Account name	グループIDです。
Proxy information	NetMeisterプロキシサーバとの接続に関する情報です。
State	プロキシサーバへの接続状態です。 ● **Connected.**—接続 ● **Disconnected.**—切断 ● **"--"** —プロキシサーバを設定していない場合に表示されます。
URL	プロキシサーバのURL。形式はhttp :// <domain>:<ポート>です。domainはプロキシサーバのWebアドレスまたはIPアドレス、portはポート番号です。 プロキシサーバが構成されていない場合、このフィールドは表示されません。

フィールド	説明
IP address	親機のIPアドレスです。 子機モード時のみ表示されます。
Port number	親機のポート番号です。 子機モード時のみ表示されます。
Connection state	NetMeister機能による親機への接続状態です。 • **Connected.**—接続 • **Disconnected.**—切断 子機モード時のみ表示されます。
Site name	拠点名です。 親機モード時のみ表示されます。
Interval	親機の更新情報の送信間隔です。 親機モード時のみ表示されます。
MQTT interval	MQTTプロトコルの送信間隔です。 親機モード時のみ表示されます。
MQTT status	MQTTプロトコルの接続状態です。 • **Connected.**—接続 • **Disconnected.**—切断 • **"--"** —接続が成功しなかった場合に表示されます。 親機モード時のみ表示されます。

関連コマンド

- **netmeister account**
- **netmeister enable**
- **netmeister parent**

11.1.2 netmeister account

Syntax

netmeister account *account* **password** { **cipher** *cipherPassword* | **simple** *plainPassword* }

undo netmeister account

デフォルト

設定なし

View

System-view

定義済みユーザロール

network-admin

パラメータ

account: グループ ID を 2～31 文字の文字列で設定します。文字列に使用できるのは小文字、数字、およびハイフン(-)のみで、ハイフン(-)で開始または終了することはできません。

cipher: 暗号テキストのパスワードを設定します。

cipherPassword: 暗号化形式のパスワードを 41～73 文字の文字列で設定します。

simple: プレーンテキストのパスワードを設定します。セキュリティのため、プレーンテキストで設定されたパスワードを含めたすべてのパスワードは、暗号化されて保存されます。

plainPassword: プレーンテキスト形式のパスワードを 8～31 文字の文字列で設定します。文字列には、文字、数字、および!#$%&'()*+,-。/:;<=>@[]^_`{|}~の特殊文字のみを使用できます。文字列には、少なくとも 1 つの文字と 1 桁の数字を含める必要があります。

説明

netmeister account コマンドを使用して、親機への子機認証と NetMeister への装置登録で使用するグループ ID とパスワードを設定します。

undo netmeister account コマンドは、設定したグループ ID とパスワードを削除します。

netmeister account コマンドを設定する前に、**netmeister enable** が無効になっていることを確認してください。

netmeister account コマンドを複数回実行した場合、最新の設定が有効になります。

NetMeister 上で、グループ ID とパスワードがあらかじめ設定されていることを確認して下さい。親機モードの場合、設定するグループ ID とパスワードが、NetMeister のグループ ID とパスワードと同じであることを確認してください。子機モードの場合、親機で設定されているグループ ID とパスワードも同じであることを確認してください。

例

親機への子機認証と NetMeister への装置登録のために、グループ ID **nec** と プレーンテキストのパスワード **nec1234** を装置に設定します。

<Switch> system-view

[Switch] netmeister account nec password simple nec1234

関連コマンド

- **netmeister enable**
- **display netmeister**

11.1.3 netmeister alarm enable notice

🕮 **メモ:**

netmeister alarm enable notice コマンドはソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

netmeister alarm enable notice

undo netmeister alarm enable notice

デフォルト

無効

View

System-view

定義済みユーザロール

network-admin

説明

netmeister alarm enable notice コマンドによって NetMeister の注意レベルのアラーム生成を有効にします。

undo netmeister alarm enable notice コマンドによって NetMeister の注意レベルの NetMeister アラーム生成を無効にします。

この機能により、システムは次のイベントの注意レベルのアラームを生成できます。

- Telnet、ssh などを使用してログインまたはログアウトした場合
- 設定を保存した場合
- 設定を保存しないまま 5 分が経過した場合

例

NetMeister の注意レベルのアラームの生成を有効にします。

<Switch> system-view

[Switch] netmeister alarm enable notice

11.1.4 netmeister enable

Syntax

netmeister enable

undo netmeister enable

デフォルト

無効

View

System-view

定義済みユーザロール

network-admin

説明

netmeister enable コマンドによって NetMeister 機能を有効にします。

undo netmeister enable コマンドによってデフォルトに戻します。

例

NetMeister 機能を有効にします。

<Switch> system-view

[Switch] netmeister enable

11.1.5 netmeister event log enable

🕮 **メモ:**

netmeister event log enable コマンドは Version 7.2.56 を含む以降のソフトウェアからサポートしています。本コマンドはバージョンアップで自動的に有効になります。

Syntax

netmeister event log enable

undo netmeister event log enable

View

System-view

デフォルト

有効

定義済みユーザロール

network-admin

説明

netmeister event log enable コマンドは NetMeister 機能が有効な時、端末がアソシエーションフェーズまたは認証フェーズで接続に失敗した際のイベントログを 5 分間隔で NetMeister に通知します。

undo netmeister event log enable コマンドはイベントログの送信を停止します。

netmeister event log enable コマンドは **netmeister enable** が有効な状態でも変更できます。

例

イベントログの送信を停止する。

<Switch> system-view

[Switch] undo netmeister event log enable

関連コマンド

netmeister enable

11.1.6 netmeister event syslog enable

🕮 **メモ:**

netmeister event syslog enable コマンドは Version 7.2.89 を含む以降のソフトウェアからサポートしています。本コマンドはバージョンアップで自動的に有効になります。

Syntax

netmeister event syslog enable

undo netmeister event syslog enable

View

System-view

デフォルト

有効

定義済みユーザロール

network-admin

説明

netmeister event syslog enable コマンドは NetMeister 機能が有効な時、logbuffer に出力されたログを 5 分間隔で NetMeister にイベントログとして通知します。

undo netmeister event syslog enable コマンドは logbuffer に出力されるログを NetMeister にイベントログとして通知する動作を停止します。

netmeister event syslog enable コマンドは **netmeister enable** が有効な状態でも変更できます。

🕮 **メモ:**

netmeister event syslog enable コマンドは logbuffer に出力されたログを通知するため、**info-center source** *module-name* **logbuffer deny** コマンドによって logbuffer への出力をモジュール単位で無効にした場合はイベントログにも通知されなくなります。Information Center の詳細はセクション 11 *システム管理* の“*Information Center*”を参照してください。

例

logbuffer に出力されたログをイベントログとして通知する動作を停止する。

<AP> system-view

[AP] undo netmeister event syslog enable

11.1.7 netmeister management ip

🕮 **メモ:**

netmeister management ip コマンドは Version7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

netmeister management ip *ip-address*

undo netmeister management ip

デフォルト

無効

View

System-view

定義済みユーザロール

network-admin

説明

netmeister management ip コマンドによって NetMeister 機能[閉域網でリモートログインする]で表示する管理用 IP アドレスを設定します。

undo netmeister management ip コマンドによってデフォルトに戻します。

NetMeister 機能については NetMeister が提供している操作ガイドを参照してください。

例

NetMeister 機能[閉域網でリモートログインする]で表示する管理用 IP アドレスを 10.1.1.10 に設定します。

```
<Sysname> system-view
[Sysname] netmeister management ip 10.1.1.10
```

11.1.8 netmeister mode

🕮 **メモ:**

netmeister mode コマンドは Version 7.2.55 を含む以降のソフトウェアからサポートしています。

Syntax

netmeister mode parent

undo netmeister mode parent

View

System-view

デフォルト

子機モード

定義済みユーザロール

network-admin

説明

netmeister mode parent コマンドを利用して NetMeister への接続モード親機モードにします。

親機モードは NetMeister 機能を有する親機ルータがいない環境において、NetMeisterPrime(有償サービス)を利用して NetMeister で管理する場合に利用します。NetMeister 機能を有する親機ルータがある環境では、それらの機器を親機とし、子機モードで利用して下さい。

undo netmeister mode parent コマンドを利用して NetMeister への接続モードを子機モードに戻します。

netmeister mode parent コマンドを設定する前に、**netmeister enable** や子機モード時に利用する **netmeister parent ip** コマンドが無効になっていることを確認してください。

例

NetMeister 機能を有する親機ルータがいない環境で QX を NetMeister によって管理するために、親機モードを設定します。

<Switch> system-view

[Switch] netmeister mode parent

関連コマンド

- **netmeister enable**
- **display netmeister**

11.1.9 netmeister parent ip

Syntax

netmeister parent ip *ip-address* [**port** *port-number*]

undo netmeister parent ip *ip-address*

View

System-view

デフォルト

設定なし

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: 親機の IP アドレスを設定します。

port *port-number*: 親機のポート番号を 1～65535 の範囲で設定します。デフォルトのポート番号は 443 です。

説明

netmeister parent ip コマンドは、子機モードとして NetMeister に接続する際に、親機とする機器の IP アドレスとポート番号を設定します。

undo netmeister parent ip を使用して、子機として接続する親機の IP アドレスとポート番号を削除します。

netmeister parent ip コマンドを設定する前に、**netmeister enable** が無効になっていることを確認してください。

netmeister parent ip コマンドと **netmeister account** コマンドを設定し、**netmeister enable** コマンドを有効にすると、子機は認証応答を受信するまで親機に子機認証の要求を送信します。**netmeister parent ip** コマンドが複数設定されている場合、装置は設定されたすべてのアドレスに要求を送信し、それぞれの親機との接続を確立します。これにより、親機の障害によるサービスの中断を防ぎ、ネットワークの可用性が向上します。最大で 2 つまで親機 IP アドレスを設定できます。

例

IP アドレス **192.168.0.254** ポート番号 443 の親機に接続する子機として設定します。

<Switch> system-view

[Switch] netmeister parent ip 192.168.0.254 port 443

IP アドレス **192.168.1.254** の親機に接続する子機として設定します。

<Switch> system-view

[Switch] netmeister parent ip 192.168.1.254

関連コマンド

- **netmeister enable**
- **display netmeister**

11.1.10 netmeister parent-mode mqtt port

🕮 **メモ:**

netmeister parent-mode mqtt port コマンドは Version 7.2.55 を含む以降のソフトウェアからサポートしています。

Syntax

netmeister parent-mode mqtt port [8883 | 443]

undo netmeister mode parent

View

System-view

デフォルト

8883

定義済みユーザロール

network-admin

説明

netmeister parent-mode mqtt port コマンドを利用して親機モードの QX が NetMeister に接続する際の MQTT プロトコルのポート番号を変更します。

undo netmeister mode parent コマンドを利用して NetMeister に接続する際の MQTT プロトコルのポート番号をデフォルトに戻します。

例

NetMeister に接続するためにネットワーク環境で 8883 を開放する必要がない様に、MQTT のポート番号を 443 に変更します。

<Switch> system-view

[Switch] netmeister parent-mode mqtt port 443

関連コマンド

- **netmeister enable**
- **display netmeister**

11.1.11 netmeister parent-mode sitename

🕮 **メモ:**

netmeister parent-mode sitename コマンドは Version 7.2.55 を含む以降のソフトウェアからサポートしています。

Syntax

netmeister parent-mode sitename *name*

undo netmeister parent-mode sitename

View

System-view

デフォルト

なし

定義済みユーザロール

network-admin

説明

netmeister parent-mode sitename コマンドを利用して親機モードの QX が NetMeister に接続する際の拠点名を設定します。

undo netmeister mode parent コマンドを利用して拠点名の設定を削除します。

例

親機モードで NetMeister に接続するために拠点名 test を設定します。

<Switch> system-view

[Switch] netmeister parent-mode sitename test

関連コマンド

- **netmeister enable**
- **display netmeister**

11.1.12 netmeister proxy

🕮 **メモ:**

netmeister proxy コマンドは Version 7.2.27 を含む以降のソフトウェアからサポートしています。Version 7.2.56 を含む以降のソフトウェアから親機モードがおこなう MQTT 通信も本コマンドによって proxy サーバを利用します。

Syntax

netmeister proxy url *url* [**username** *username* **password** { **cipher | simple** } *string*]

undo netmeister proxy

View

System-view

デフォルト

設定なし

定義済みユーザロール

network-admin

パラメータ

url *url*:プロキシサーバの URL を指定します。***http://***<*domain*>:<*port*>形式で、大文字と小文字を区別して 8 から 128 文字の文字列を指定します。<*domain*>引数はプロキシサーバのドメイン名または IP アドレスを表し、<*port*>引数は 1 から 65535 の範囲のポート番号を表します。デフォルトのポート番号は 80 です。

username *username*:プロキシサーバへのアクセスに使用するユーザー名を指定します。1 から 31 文字の大文字と小文字が区別されます。文字列には、バックスラッシュ (¥) 、引用符 (") 、疑問符 (?) 、スペースを含めることはできません。。

password:プロキシサーバへのアクセスに使用するパスワードを指定します。

cipher:パスワードを暗号化形式で指定します。

simple:プレーンテキスト形式でパスワードを指定します。セキュリティ上の理由から、プレーンテキスト形式で指定されたパスワードは暗号化形式で保存されます。

string:パスワード文字列を指定します。プレーンテキスト形式は、大文字と小文字を区別する 1 から 31 文字の文字列です。暗号化された形式は、大文字と小文字を区別した 33 から 73 文字の文字列です。プレーンテキストのパスワードには、バックスラッシュ、引用符 (") 、疑問符 (?) 、またはスペースを含めることはできません。

説明

netmeister proxy コマンドは装置が NetMeister 宛の https 通信のために指定された proxy サーバを利用します。親機への https 通信にはプロキシサーバを使用しません。

undo netmeister proxy コマンドはプロキシサーバの指定を削除します。

netmeister proxy コマンドを設定する前に、**netmeister enable** が無効になっていることを確認してください。

netmeister proxy 複数回実行した場合、最新の設定が有効になります。

例

IP アドレス **192.168.1.254** の親機に接続する子機とし、NetMeister にはプロキシサーバ 10.1.1.254 (ポート:8080)を使用するように設定します。

<Switch> system-view

[Switch] netmeister parent ip 192.168.1.254

[Switch] netmeister proxy url http://10.1.1.254:8080

関連コマンド

- **netmeister enable**
- **display netmeister**
-

11.1.13 netmeister update

🕮 **メモ:**

netmeister update コマンドはソフトウェアバージョン 7.2.67 を含む以降のソフトウェアからサポートしています。

Syntax

netmeister update

View

System-view

定義済みユーザロール

network-admin

説明

netmeister update コマンドは NetMeister に登録している装置情報を即時更新します。

例

装置名を変更した後、NetMeister に登録している装置情報を即時更新します。

<AC> system-view

[AC] sysname test

[AC] netmeister update

無線子機の装置名を ap10 から ap9 に変更した後、NetMeister に登録している装置情報を即時更新します。

<AC> system-view

[AC] wlan rename-ap ap10 ap9

[AC] netmeister update

11.1.14 netmeister track

🕮 **メモ:**

netmeister track コマンドはソフトウェアバージョン 7.2.73 を含む以降のソフトウェアからサポートしています。

Syntax

netmeister track *track-entry-number*

undo netmeister track *track-entry-number*

View

System-view

デフォルト

設定なし

定義済みユーザロール

network-admin

パラメータ

track *track-entry-number*: 1～1024 の範囲の番号で指定されたトラックエントリに NetMeister 機能を紐付けます。

説明

netmeister track コマンドは、トラックエントリを NetMeister 機能に関連付けます。

undo netmeister track コマンドは、NetMeister 機能 とトラック エントリの関連付けを解除します。

本コマンドは NetMeister から Ping 監視設定をした場合に自動で設定されます。NetMeister から Ping 監視設定を削除した場合に自動で設定が解除されます。

本コマンドが適用されるトラックエントリは以下の条件と一致する NQA エントリのみです。NetMeister から Ping 監視設定をした場合、本条件と一致する設定が行われます。

- **nqa entry** コマンドで設定された *admin-name* は **nm-ping** である必要があります。
- **type** コマンドで設定された NQA テストタイプは **icmp-echo** である必要があります。
- **reaction checked-element probe-fail** コマンドでリアクションエントリが設定されている必要があります。

QX-W2230AC アクセスコントローラ

コマンドマニュアル

12.IRF スタック

本マニュアルは以下に示す章で構成されています。

01-IRF スタック

目次

このセクションのページは **12-x-x** です。

1 章 IRF スタック 1-1
1.1 IRF スタック設定コマンド 1-1
1.1.1 display irf 1-1
1.1.2 display irf configuration 1-3
1.1.3 display irf forwarding 1-4
1.1.4 display irf link 1-5
1.1.5 display mad 1-7
1.1.6 irf auto-merge enable 1-8
1.1.7 irf auto-update enable 1-9
1.1.8 irf domain 1-10
1.1.9 irf mac-address persistent 1-11
1.1.10 irf member description 1-12
1.1.11 irf member priority 1-13
1.1.12 irf member renumber 1-14
1.1.13 irf member stack enable 1-15
1.1.14 irf topo-domain 1-17
1.1.15 irf-optimize wlan reliable-access 1-17
1.1.16 irf-port 1-18
1.1.17 irf-port-configuration active 1-19
1.1.18 mad arp enable 1-20
1.1.19 mad exclude interface 1-21
1.1.20 mad restore 1-23
1.1.21 port group interface 1-23
1.1.22 wlan ap-backup hot-backup enable global 1-25
1.1.23 wlan client-backup hot-backup enable 1-26
1.1.24 wlan client-backup hot-backup delay 1-27

1章 IRF スタック

QX-W2230AC アクセスコントローラは、QX-W2230AC アクセスコントローラでのみ IRF スタックユニットを形成することができます。

🕮 **メモ:**

QX-W2230AC は最大 2 台の装置で IRF スタックを形成することができます。

1.1 IRFスタック設定コマンド

1.1.1 display irf

Syntax

display irf

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display irf コマンドは IRF スタックユニットの情報を表示します。各 IRF スタックのメンバのメンバ ID、役割、プライオリティ、Bridge MAC アドレス、説明の情報を表示します。

例

IRF スタックユニットの情報を表示します。

<AC> display irf

```
Member ID  Role     Priority   CPU MAC          Description
   1       Loading  1          0440-a969-0140   F1Num001
 *+2       Master   1          48bd-3d1e-86d8   F1Num002
-------------------------------------------------------------
The asterisk (*) indicates the master.
The plus sign (+) indicates the device through which you are logged in.
The right angle bracket (>) indicates the device's stack capability is disabled.
```

```
Bridge MAC of the IRF: 48bd-3d1e-86d8
Auto upgrade           : Disabled
MAC persistence        : Disabled
Topo-domain ID         : 30
Auto merge             : Enabled
```

表 1-1 コマンド出力

フィールド	説明
MemberID	IRFスタックのメンバIDです。 ● メンバIDはアスタリスク（*）で表示されます。 ● ログインしている装置のメンバIDは(+)で表示されます。 ● マルチメンバスタック機能が無効の状態は（>）で表示されます。マルチメンバスタック機能を無効にするには**undo irf member stack enable**コマンドを使用します。
Role	IRFスタックユニットのメンバ装置の役割です。 ● **Standby**—メンバ装置です。 ● **Master**—Master装置です。 ● **Loading**—装置がソフトウェアイメージを読み込んでいます。
Priority	IRFスタックのメンバのプライオリティです。
CPU-MAC	装置のCPU-MACアドレスです。
Description	メンバ装置の説明です。 ● 説明が設定されていない場合、ハイフン線（----）と表示されます。 ● 文字の最大数を超過している場合、超過している個所が省略され、（…）と表示されます。すべての説明を表示する場合、**display current-configuration**コマンドを使用します。
Bridge MAC of the IRF is	IRFスタックのBridge MACアドレスです。
Auto upgrade	ソフトウェアオートアップグレード機能の状態です。 ● **Enabled**—有効です。Masterはソフトウェアイメージを IRFスタックユニットに追加する装置に自動的に送信します。 ● **Disabled**—無効です。IRFスタックユニットへ追加する装置に、Masterと同一のソフトウェアイメージを手動でアップグレードする必要があります。ソフトウェアイメージが異なる場合、新しい装置はIRFスタックユニットに加入することができません。

フィールド	説明
MAC persistent	IRFスタックのBridge MACアドレスを保持する設定です。 ● **6 min**—Master装置が離脱したのち、IRFスタックユニットのBridge MACアドレスは6分間変更しません。 ● **Always**—Masterが離脱した後、IRFスタックユニットのBridge MACアドレスは変更しません。 ● **Disabled**—Masterが離脱した後、すぐに新しいMasterのBridge MACアドレスに切り替わります。
Topo-domain ID	IRFスタックユニットのトポドメインIDです。IRFスタックユニットに割り当てたトポドメインIDは、IRFスタックユニットを識別するために使用されます。
Auto merge	Auto-merge機能の状態です。 ● **Enabled**—IRFスタックユニットは、IRFスタック結合中にMaster装置の選出に失敗すると、メンバ装置を自動で再起動します。 ● **Disabled—**IRFスタック結合を完了させるために、手動で再起動を行う必要があります。

1.1.2 display irf configuration

Syntax

display irf configuration

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display irf configuration コマンドは基本的な IRF スタックの設定を表示します。各メンバの現在のメンバ ID、新しいメンバ ID、トポドメイン ID、スタック機能状態、IRF スタックポートに関連付けられたネットワークインタフェースが含まれます。

例

すべてのメンバ装置で IRF スタックの設定を表示します。

<AC> display irf configuration

```
The New ID, Topo-domain, Stack, and Member interfaces fields display settings for
the next startup.
```

```
Member ID     New ID   Topo-domain      Stack       Member interfaces
1             1        0                Enabled     Disabled
```

表 1-2 コマンド出力

フィールド	説明
MemberID	装置の現在のメンバIDです。
NewID	装置に割り当てられたメンバIDです。メンバIDは再起動後に適用されます。
Topo-domain	IRFスタックトポドメインIDです。トポドメインIDは再起動後に適用されます。
Stack	マルチメンバスタック機能が有効かどうかを示します。 • **Enabled**—装置は他のメンバ装置とIRFスタックユニットを形成できます。 • **Disabled—**装置は他のメンバ装置とIRFスタックユニットを形成できません。装置は最長で5秒後にIRFスタックユニットから除外されます。
Member interfaces	IRFスタックポートに関連付けられたネットワークインタフェースです。IRFスタックポートにネットワークインタフェースが割り当てられていない場合、このフィールドには**Disabled**が表示されます。 IRFスタックリンクのチャネルタイプは括弧でくくられます。使用可能なチャネルタイプは以下の通りです。 • **ctrl**—制御チャネルです。リンクは制御パケットのみ転送できます。 • **data—**データチャネルです。リンクはデータパケットのみ転送できます。 • **ctrl&data—**ハイブリッドチャネルです。リンクは制御パケットとデータパケットの両方を転送できます。

1.1.3 display irf forwarding

Syntax

display irf forwarding [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display irf forwarding コマンドはメンバ装置で受信された IRF スタックハローパケットのリンク情報を表示します。

Examples

Master 装置で受信した IRF スタックハローパケットの情報を表示します。

<AC> display irf forwarding

```
Member ID     CPU MAC            Hello timeout (sec)
1             0440-a969-0140     5
2             48bd-3d1e-86d8     5
```

メンバ装置 2 で受信した IRF スタックハローパケットの情報を表示します。

<AC> display irf forwarding slot 2

```
Member ID     CPU MAC            Hello timeout (sec)
2             0440-a969-0140     5
1             48bd-3d1e-86d8     4
```

表 1-3 コマンド出力

フィールド	説明
Member ID	パケット送信側のIRFスタックメンバIDです。
CPU MAC	パケット送信側のCPU MACアドレスです。
Hello timeout (sec)	ハローパケットタイムアウトまでの残時間（秒）です。既存のハローパケットが期限切れになる前に、新たなハローパケットを受信しない場合、メンバ装置は、送信側がIRFスタックユニットを離れたと判断します。既存のハローパケットが期限切れになる前に、新たなハローパケットを受信した場合、メンバ装置は、受信したパケットに基づき送信側のハローパケットタイムアウト時間を更新します。

1.1.4 display irf link

Syntax

display irf link

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display irf link コマンドは IRF スタックのリンク情報を表示します。IRF スタックメンバ ID、IRF スタックポートに関連付けられたネットワークインタフェース、IRF スタックリンクの状態を含みます。

Examples

IRF スタックのリンク情報を表示します。

<AC> display irf link

```
Member ID    Member interfaces                Status
1            Disabled                         --
```

表 1-4 コマンド出力

フィールド	説明
Member ID	IRFスタックのメンバIDです。
Member interfaces	IRFスタックポートに関連付けられたネットワークインタフェースです。IRFスタックポートにネットワークインタフェースが割り当てられていない場合、このフィールドには**Disabled**が表示されます。 IRFスタックリンクのチャネルタイプは括弧でくくられます。使用可能なチャネルタイプは以下の通りです。 ● **ctrl**—制御チャネルです。リンクは制御パケットのみ転送できます。 ● **data**—データチャネルです。リンクはデータパケットのみ転送できます。 ● **ctrl&data**—ハイブリッドチャネルです。リンクは制御パケットとデータパケットの両方を転送できます。
Status	ネットワークインタフェースのリンク状態です。 ● **UP**－リンクがUP状態です。 ● **DOWN**－リンクがDOWN状態です。 ● **ADM**－ポートが**shutdown**コマンドにより手動でシャットダウンしています。 ● **Blocked**－リンクはブロックされています。この状態では、装置は他の装置で構成されたIRFスタックユニットに加わることはできません。**undo irf member stack enable**コマンドを使用することで、マルチメンバスタック機能を

フィールド	説明
	無効にすることができます。

1.1.5 display mad

Syntax

display mad [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose: 詳細な MAD 情報を表示します。このキーワードを指定しない場合、MAD の設定が有効あるいは無効のみを表示します。

説明

display mad コマンドは MAD の状態と設定を表示します。

例

MAD 情報の概要を表示します。

<AC> display mad

```
MAD ARP enabled.
MAD ND disabled.
MAD LACP disabled.
```

MAD 情報の詳細を表示します。

<AC> display mad verbose

```
Multi-active recovery state: No
Excluded ports (user-configured):
  Vlan-interface4
Excluded ports (system-configured):
  Ten-GigabitEthernet1/0/9
  Ten-GigabitEthernet1/0/10
MAD ARP enabled interface:
  Vlan-interface3
MAD ND disabled.
```

```
MAD LACP disabled.
```

表 1-5 コマンド出力

フィールド	説明
Multi-active recovery state	IRFスタックユニットがRecovery状態であるかどうかを示します。 • **Yes**—IRFスタックユニットがRecovery状態です。IRFスタックユニットが複数のIRFスタックユニットに分裂したとMADが検出したとき、1つのIRFスタックユニットにトラフィックを転送します。ほかのすべてのIRFスタックユニットがRecovery状態に設定されます。Recovery状態ではMADは、IRFスタックネットワークインタフェースとシャットダウンに設定されていないポートを除いてIRFスタックユニットのすべてのネットワークインタフェースをシャットダウンします。 • **No**—IRFスタックユニットがRecovery状態でありません。アクティブでトラフィックを転送できます。
Excluded ports(user-configured)	IRFスタックユニットがRecovery状態へ遷移時にシャットダウンしないよう、手動で設定されたポートです。
Excluded ports(system-configured)	IRFスタックユニットがRecovery状態へ遷移時にシャットダウンしないよう、デフォルトで設定されたポートです。このポートはユーザが設定することができません。

1.1.6 irf auto-merge enable

Syntax

irf auto-merge enable

undo irf auto-merge enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

irf auto-merge enable コマンドは IRF スタック自動結合機能を有効にします。

undo irf auto-update enable コマンドは IRF スタック自動結合機能を無効にします。

IRF スタックユニットは、結合すると Master 装置を選出します。IRF スタック自動結合機能を有効にすることで、IRF スタックユニット内で Master 装置に選出されなかったメンバ装置は自動で再起動され、IRF スタック結合が完了します。IRF スタック自動結合機能が無効の場合、Master 装置に選出されなかった装置の再起動を、システムの指示に従い手動で行う必要があります。

結合を成功させるには、結合する IRF スタックユニットの両方で IRF スタック自動結合機能を有効にしてください。

例えば､IRF スタック自動結合機能は以下の事象によって生じた結合に対して適用されます。

- IRF スタックリンクがリンク障害から復旧した場合。
- メンバ装置の IRF スタックネットワークインタフェースが、IRF スタックポートに関連付いた後に、レイヤ 2 ネットワーク経由で接続した場合。

例

IRF スタック自動結合機能を有効にします。

<AC> system-view

[AC] irf auto-merge enable

1.1.7 irf auto-update enable

Syntax

irf auto-update enable

undo irf auto-update enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

irf auto-update enable コマンドはすべての IRF スタックユニットのメンバのソフトウェアを自動で更新する機能を有効にします。

undo irf auto-update enable コマンドはソフトウェア自動更新機能を無効にします。

このコマンドで、IRF スタックユニットの Master 装置の現在のソフトウェアイメージを IRF スタックユニットに追加するすべての装置に自動的に伝えます。

ソフトウェア自動更新機能を有効にする場合、装置に新しいシステムソフトウェアのための有効な領域があることを確認してください。適切な領域がない場合、装置は現在のソフトウェアイメージを自動的に削除します。もし再利用された空き領域が十分でない場合、装置はソフトウェア自動更新機能を完了することができません。装置を再起動し、ファイルを削除するために Boot ROM メニューに移行してください。

以下の状態の場合、IRF スタックで稼働している新しい装置のソフトウェアイメージを手動で更新する必要があります。

- ソフトウェア自動更新が無効となっています。
- ソフトウェア自動更新が失敗します。IRF スタックユニットが新たな装置で使用されるソフトウェアバージョンを識別できない場合、ソフトウェアの自動更新に失敗する可能性があります。

例

ソフトウェア自動更新機能を有効にします。

<AC> system-view

[AC] irf auto-update enable

1.1.8 irf domain

Syntax

irf domain *domain-id*

undo irf domain

デフォルト

0

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-id: IRF スタック MAD ドメイン ID を指定します。設定範囲は 0～4294967295 です。

説明

irf domain コマンドは IRF スタック MAD ドメイン ID を割り当てます。

undo irf domain コマンドはデフォルトの IRF スタック MAD ドメインの設定に戻します。

IRF スタック MAD ドメイン ID は、IRF スタックマルチアクティブ検出を一意に識別します。IRF スタックユニットが ARP MAD の中継装置として別の IRF スタックユニットを使用する場合、IRF スタック分裂の検出失敗を避けるために、2 つの IRF スタックユニットには中継装置と異なるドメイン ID を割り当てなければなりません。間違って検出されると、IRF スタックの分裂を引き起こします。

IRF スタックユニットには IRF スタック MAD ドメイン ID が 1 つのみあります。**irf domain**、**mad enable**、**mad arp enable** コマンドで IRF スタック MAD ドメイン ID を変更することができます。これらのコマンドで設定された IRF スタック MAD ドメイン ID は互いに上書きされます。

例

IRF スタック MAD ドメイン ID を 10 に設定します。

<AC> system-view

[AC] irf domain 10

1.1.9 irf mac-address persistent

Syntax

irf mac-address persistent { **always** | **timer** }

undo irf mac-address persistent

デフォルト

Master 装置が離脱した後、IRF スタックユニットの Bridge MAC アドレスは 6 分間変更されません。タイマの満了までに Master が IRF スタックに戻ってこない場合、IRF スタックユニットは新しく選出された Master の Bridge MAC アドレスを使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

always: IRF スタックユニットの Bridge MAC アドレスを変更しません。新しい Master の選定が行われたのち IRF スタックユニットは Bridge MAC アドレスを変更しません。

timer: 新しい Master の選定が行われたのち IRF スタックユニットの Bridge MAC アドレスは 6 分間変更しません。時間以内に IRF スタックユニットに装置が再加入した場合、IRF スタックの Bridge MAC アドレスを変更しません。時間以内に IRF スタックユニット

に装置が再加入しない場合、IRF スタックユニットは新しい Master の Bridge MAC アドレスを使用します。

説明

irf mac-address persistent コマンドは IRF スタックの Bridge MAC アドレスを保持するように設定します。

undo irf mac-address persistent コマンドは Master の離脱後、すぐに Bridge MAC アドレスを変更します。

IRF スタックの Bridge MAC アドレスは Master の再選定後に、IRF スタックユニットが Bridge MAC アドレスとして古い Master の Bridge MAC アドレスを使用し続ける時間を指定します。

デフォルトで IRF スタックユニットは Master 装置の Bridge MAC アドレスを使用します。LACP のようなレイヤ 2 プロトコルは IRF スタックユニットを識別するため、Bridge MAC アドレスを使用します。LAN スイッチでは Bridge MAC アドレスは一意にする必要があります。

Bridge MAC アドレスの変更によって Master の再選定で転送遅延やパケットロスを引き起こさないように **irf mac-address persistent always** コマンドを設定してください。

Bridge MAC アドレスの重複を防ぐため、IRF スタックユニットは Master の離脱後、自動的に Bridge MAC アドレスを変更することができます。しかし変更を行うとサービスの中断を引き起こします。ネットワークの状況に依存して、Master の離脱後に IRF スタックユニットの Bridge MAC アドレスを保持するか変更するかを設定することができます。

ARP MAD が使用される場合、IRF スタックの Bridge MAC アドレスの保持を無効にするため、**undo irf mac-address persistent** コマンドを使用します。

IRF スタックユニットが結合するとき、IRF スタックは IRF スタック Bridge MAC アドレスを無視し、IRF スタックユニットの各メンバ装置の Bridge MAC アドレスを調査します。2 台のメンバ装置が同じ Bridge MAC アドレスを持つ場合、IRF スタック結合は失敗します。

例

IRF スタックの Bridge MAC アドレスの保持時間を永久保持に設定します。

<AC> system-view

[AC] irf mac-address persistent always

1.1.10 irf member description

Syntax

irf member *member-id* **description** *text*

undo irf member *member-id* **description**

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

member-id: IRF スタックのメンバ ID を指定します。

text: IRF スタックのメンバの説明を設定します。設定範囲は 1～127 文字です。

説明

irf member description コマンドは IRF スタックのメンバの説明を設定します。

undo irf member description コマンドはデフォルトに戻します。

このコマンドはメンバ装置の位置や目的を記載するために設定します。

例

IRF スタックのメンバ 1 の説明を設定します。

<AC> system-view

[AC] irf member 1 description F1Num001

1.1.11 irf member priority

Syntax

irf member *member-id* **priority** *priority*

undo irf member *member-id* **priority**

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

member-id: IRF スタックのメンバ ID を指定します。

priority: プライオリティを指定します。設定範囲は 1～32 です。プライオリティの値が高い場合、プライオリティは高くなります。Master はプライオリティが高い装置が優先されます。

説明

irf member priority コマンドは IRF スタックのメンバのプライオリティを変更します。

undo irf member priority コマンドはデフォルトに戻します。

新たなプライオリティの設定は次回の Master 装置の選出時に適用されます。しかし、プライオリティを新たに設定しても Master 装置の選出は実行されません。

例

IRF スタックのメンバ 2 のプライオリティを 32 に設定します。

<AC> system-view

[AC] irf member 2 priority 32

1.1.12 irf member renumber

Syntax

irf member *member-id* **renumber** *new-member-id*

undo irf member *member-id* **renumber**

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

member-id: IRF スタックのメンバ ID を指定します。設定範囲は 1～2 です。

new-member-id: IRF スタックのメンバに新しい ID を割り当てます。設定範囲は 1～2 です。

説明

注意:

IRF スタックのメンバ ID の変更を行うと、インタフェースやファイルパスの設定を含むメンバ ID に関する設定が無効になり、データロスが発生する可能性があります。メンバ ID を変更する際は、ご利用のネットワークへの影響を十分ご理解の上、変更してください。

irf member renumber コマンドは装置の IRF スタックのメンバ ID を変更します。

undo irf member renumber コマンドは装置の IRF スタックのメンバ ID をもとに戻します。

装置を IRF スタックユニットに追加するとき、装置に一意の IRF スタックのメンバ ID を割り当てる必要があります。

新たに設定された IRF スタックメンバ ID（**undo irf member renumber** コマンドを使用して設定されたメンバ ID を含む）を適用するには、IRF スタックのメンバの再起動が必要です。

メンバ装置を再起動する前に変更をキャンセルする場合、**undo irf member renumber** コマンドを使用してください。このコマンドにより、新たに設定されるメンバ ID は変更前のメンバ ID と同じになります。

例

IRF スタックのメンバ ID を 1 から 2 に変更します。

<AC> display irf

[AC] irf member 1 renumber 2

```
Warning: Renumbering the member ID may result in configuration change or loss.
Continue?[Y/N]:Y
```

1.1.13 irf member stack enable

Syntax

irf member *member-id* **stack enable**

undo irf member *member-id* **stack enable**

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

パラメータ

member-id: IRF スタックのメンバ ID を指定します。

説明

irf member stack enable コマンドは IRF スタックのメンバ装置に対してマルチメンバスタック機能を有効にします。

undo irf member stack enable コマンドは IRF スタックのメンバ装置に対してマルチメンバスタック機能を無効にします。

マルチメンバスタック機能が無効の場合、メンバ装置は他の装置で構成される IRF スタックユニットに加わることができません。

トラブルシューティングやメンテナンスのため、**undo irf member stack enable** コマンドを使用してメンバ装置を IRF スタックユニットから除外することができます。除外されたメンバ装置は、IRF スタックの設定を保持したまま動作を続けますが、IRF スタック制御パケットの送受信は行いません。

トラブルシューティングやメンテナンス作業が完了しましたら、除外されたメンバ装置にログインし、**irf member stack enable** コマンドを実行することでメンバ装置を IRF スタックユニットに戻すことができます。**irf member stack enable** コマンドを適用するには、設定を保存し、メンバ装置を再起動する必要があります。

例

メンバ装置 2 を IRF スタックユニットから除外します。

<AC> system-view

[AC] undo irf member 2 stack enable

```
Member 2 will leave from the IRF and cannot form an IRF with any other devices.
Continue? [Y/N]: y
Operation succeeded. Please check the configuration on member 2 with the IRF for
configuration collisions.
```

除外された装置を IRF スタックユニットに戻します。

<AC> system-view

[AC] irf member 2 stack enable

```
Please save the configuration, and then reboot the device for the configuration
to take effect.
```

1.1.14 irf topo-domain

Syntax

irf topo-domain *topo-domain-id*

undo irf topo-domain

デフォルト

0

View

System view

定義済みユーザロール

network-admin

パラメータ

topo-domain-id: IRF スタックのトポドメイン ID を指定します。指定範囲は 0～4294967295 です。

説明

irf topo-domain コマンドは、IRF スタックのトポドメイン ID を指定します。

undo irf topo-domain コマンドは、デフォルトに戻します。

IRF スタックのトポドメイン ID により、IRF スタックユニットは一意に識別されます。

メンバ装置を同じ IRF スタックユニットに追加するときは、それらのメンバ装置に同じトポドメイン ID を割り当てる必要があります。

トポドメイン ID の変更を適用するには、メンバ装置を再起動する必要があります。

例

IRF スタックのトポドメイン ID を 10 に設定します。

<AC> system-view

[AC] irf topo-domain 10

```
The configuration will take effect at the next startup.
```

1.1.15 irf-optimize wlan reliable-access

Syntax

irf-optimize wlan reliable-access

undo irf-optimize wlan reliable-access

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

irf-optimize wlan reliable-access コマンドは、信頼できる WLAN アクセスを確立するため、IRF スタックの最適化を行います。

undo irf-optimize wlan reliable-access コマンドは、IRF スタックの最適化を無効にします。

信頼できる AP とクライアントのアクセスを保証するために **irf-optimize wlan reliable-access** コマンドを使用します。**irf-optimize wlan reliable-access** コマンドにより、IRF スタックの Master 装置の選出や、新たなメンバ装置の参加、IRF スタックメンバ装置の役割変更の処理速度が向上し、AP とクライアントのアクセスが不安定になるのを防ぎます。

例

信頼できる WLAN アクセス確立のため、IRF スタックの最適化を有効にします。

<AC> system-view

[AC] irf-optimize wlan reliable-access

1.1.16 irf-port

Syntax

irf-port *member-id*

View

System view

定義済みユーザロール

network-admin

パラメータ

member-id: IRF スタックのメンバの IRF スタックポートを指定します。*member-id* は IRF スタックのメンバ ID を示します。

説明

irf-port コマンドは IRF port view に移行します。

各メンバ装置には IRF スタックポートが 1 つだけあります。

リンクを IRF スタックポートに関連付けるためには、IRF port view に移行する必要があります。

例

メンバ装置 1 で IRF スタックポートの IRF port view に移行します。

<AC> system-view

[AC] irf-port 1

関連コマンド

port group interface

1.1.17 irf-port-configuration active

Syntax

irf-port-configuration active

View

System view

定義済みユーザロール

network-admin

説明

irf-port-configuration active コマンドは装置に設定したすべての IRF スタックポートの設定を有効にします。

IRF スタックポートにリンクを関連付けたのち、IRF スタックポートの設定を有効にするために、このコマンドを使用します。このコマンドは 2 つの装置を 1 つの IRF スタックユニットに結合します。

システムは以下の状況において自動で IRF スタックポートの設定を有効にします。

- 装置が起動するコンフィグレーションファイルが IRF スタックポートの関連付けを含みます。
- IRF スタックが形成したのち、IRF スタックポートにリンクを関連付けます。

例

IRF スタックポート 1 を設定します。

IRF スタックポート 1 に GigabitEthernet 1/0/1 を関連付けます。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] shutdown

[AC-GigabitEthernet1/0/1] quit

[AC] irf-port 1

[AC-irf-port1] port group interface gigabitethernet 1/0/1

IRF スタックのセットアップを行うため、以下の作業を行います。

IRF スタックの設定を完了した後、設定を保存します。

irf-port-configuration active コマンドを実行し、IRF スタックポートを有効にします。

[AC-irf-port1/2] quit

[AC] interface ten-gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] undo shutdown

[AC-GigabitEthernet1/0/1] quit

再起動後に IRF スタックポートの設定が適用されるように設定を保存します。

[AC] save

```
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[cfa0:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
cfa0:/startup.cfg exists, overwrite? [Y/N]:y
 Validating file. Please wait.....................
 Saved the current configuration to mainboard device successfully.
Slot 1:
 Save next configuration file successfully.
 Configuration is saved to device successfully.
```

IRF スタックポートを有効にします。

[AC] irf-port-configuration active

1.1.18 mad arp enable

Syntax

mad arp enable

undo mad arp enable

デフォルト

無効

View

VLAN interface view

定義済みユーザロール

network-admin

説明

mad arp enable コマンドは ARP MAD を有効にします。

undo mad arp enable コマンドは ARP MAD を無効にします。

VLAN インタフェース 1 で ARP MAD を設定することはできません。

ARP MAD の中間装置として、ある IRF スタックユニットが別の IRF スタックユニットを使用する場合、2 つの IRF スタックユニットに異なるドメイン ID を割り当てる必要があります。そうでなければ、IRF スタックの分裂の検出が誤って行われます。

mad arp enable コマンドを使用するとき、システムは MAD ドメイン ID を入力するように画面が表示されます。現在のドメイン ID を変更しない場合、Enter キーを押下します。

IRF スタックユニットは 1 つの IRF スタックのドメイン ID のみサポートします。**irf domain**、**mad enable**、**mad arp enable** のコマンドを使用して IRF スタックの MAD ドメイン ID を変更することができます。これらのコマンドで設定された IRF スタック MAD ドメイン ID は互いに上書きされます。

例

VLAN インタフェース 3 で ARP MAD を有効にします。

<AC> system-view

[AC] interface vlan-interface 3

[AC-Vlan-interface3] mad arp enable

```
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 0]: 1
The assigned  domain ID is: 1
```

関連コマンド

irf domain

1.1.19 mad exclude interface

Syntax

mad exclude interface *interface-type interface-number*

undo mad exclude interface *interface-type interface-number*

デフォルト

IRF スタックポートに関連付いたネットワークインタフェースを除き、Recovery 状態の IRF スタックユニットのすべてのネットワークインタフェースがシャットダウンです。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: ポートのタイプと番号を指定します。

説明

mad exclude interface コマンドは、multi-active 衝突の検出により Recovery 状態の IRF スタックユニットのすべてのネットワークインタフェースをシャットダウンしないように設定します。

undo mad exclude interface コマンドは、multi-active 衝突の検出により Recovery 状態の IRF スタックユニットのすべてのネットワークインタフェースをシャットダウンするように設定します。

Telnet 接続のような特別の目的のためにポートの状態を UP に継続する必要がある場合、シャットダウンを行うアクションからインタフェースを除外します。不正なトラフィックの転送を防ぐため、Telnet で使用するインタフェースを除くいかなるインタフェースも、シャットダウンアクションから除外しないことを推奨します。MAD で使用するアグリゲートインタフェースとメンバインタフェースを、シャットダウンアクションから除外しないでください。

MAD によってシャットダウンとなったインタフェースが up となるのは、回復した IRF スタックユニットに加入するために、メンバ装置が再起動するときです。現在の Master が故障あるいはほかの例外処理が発生したために自動回復が行われなかった場合、**mad restore** コマンドを使用して手動でメンバ装置とポートを up 状態に回復します。

例

MAD が Recovery 状態に遷移したときにシャットダウンとならないように GigabitEthernet 1/0/1 を除外します。

<AC> system-view

[AC] mad exclude interface gigabitethernet 1/0/1

関連コマンド

mad restore

1.1.20 mad restore

Syntax

mad restore

View

System view

定義済みユーザロール

network-admin

説明

mad restore コマンドは Recovery 状態にある IRF スタックユニットの正常な MAD を回復します。

IRF スタックの分裂が回復する前にアクティブの IRF スタックユニットが故障した場合、**mad restore** コマンドを使用して Recovery 状態の IRF スタックユニットを回復します。

回復した IRF スタックユニットはアクティブの IRF スタックユニットの役割を引き継ぎます。

例

Recovery 状態にある IRF スタックユニットの正常な MAD を回復します。

<AC> system-view

[AC] mad restore

```
   This command will restore the device from multi-active conflict state. Continue?
[Y/N]:Y
Restoring from multi-active conflict state, please wait...
```

1.1.21 port group interface

Syntax

port group interface *interface-type interface-number* [**type** { **control** | **data** }]

undo port group interface *interface-name*

デフォルト

設定なし

View

IRF port view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: IRF スタックネットワークインタフェースのタイプと番号を指定します。

interface-name: *interface-typeinterface-number* の形式で IRF スタックネットワークインタフェースを指定します。*interface-type interface-number* の引数の間に半角スペースは入りません。

type: IRF スタックリンクのチャネルタイプを指定します。チャネルタイプを指定しない場合ハイブリッドチャネルが指定されます。ハイブリッドのリンクでは制御パケットとデータパケットの両方を転送することができます。

- **control**: リンクのタイプを control に設定します。このリンクは、IRF プロトコルパケットのような制御パケットのみ転送できます。
- **data**: リンクタイプを data に設定します。このリンクでは、データパケットのみ転送できます。

説明

port group interface コマンドは IRF スタックポートにネットワークインタフェースを割り当てます。

undo port group interface コマンドはネットワークインタフェースと IRF スタックポートの割り当てを削除します。

IRF スタックポートには、少なくとも 1 つのハイブリッドチャネル、あるいはデータチャネルと制御チャネルを少なくとも 1 つずつ設定してください。

大量のデータトラフィックが存在したときに制御トラフィックが遅延しないようにするために、データチャネルとしての物理リンクと制御チャネルとしての物理リンクを分けて使用してください。

IRF スタックリンクのチャネルタイプを変更するには、まず関連付けを削除してから、リンクに再度関連付けてください。

IRF スタックポートにネットワークインタフェースを関連付ける、あるいは関連付けを削除する前に、ポートグループのすべてのポートを **shutdown** コマンドでシャットダウンします。関連付け、あるいは削除の処理が完了した後、すべての IRF スタック物理ポートを **undo shutdown** コマンドで UP の状態にします。

IRF スタックリンクが切断されたとしても IRF スタック物理ポートと IRF スタックポート間の関連付けを直接削除することはできません。関連付けを削除するため、**undo port group interface** コマンドを使用します。

IRF スタック物理ポートの関連付けの設定要件の詳細は、オペレーションマニュアルのセクション 13 *IRF スタック “IRF スタックの設定”* を参照してください。

例

IRF スタックのメンバ 2 の IRF スタックポート 2 にハイブリッドチャネルとして GigabitEthernet 1/0/1 を割り当てます。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] shutdown

[AC-GigabitEthernet1/0/1] quit

[AC] irf-port 2

[AC-irf-port2] port group interface gigabitethernet 1/0/1

[AC-irf-port2] quit

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] undo shutdown

関連コマンド

irf-port

1.1.22 wlan ap-backup hot-backup enable global

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.18 を含む以降のソフトウェアからサポートしています。

Syntax

wlan ap-backup hot-backup enable global

undo wlan ap-backup hot-backup enable global

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

wlan ap-backup hot-backup enable global コマンドを使用して、IRF スタックユニットでの AP バックアップ機能を有効にします。

undo wlan ap-backup hot-backup enable global コマンドを使用して、IRF スタックユニットでの AP バックアップ機能を無効にします。

AP バックアップを有効にすることで、IRF スタックユニットの Master 装置は接続している AP の情報をメンバ装置と同期できます。Master 装置がダウンし、メンバ装置が Master に切り替わる際、サービスの継続性が保証されます。

本機能はすでにオンラインの AP には適用されません。本機能を無効にすると、メンバ装置からバックアップ AP の情報を削除します。

例

AP バックアップを有効にします。

<AC> system-view

[AC] wlan ap-backup hot-backup enable global

1.1.23 wlan client-backup hot-backup enable

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.18 を含む以降のソフトウェアからサポートしています。

Syntax

wlan client-backup hot-backup enable

undo wlan client-backup hot-backup enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

wlan client-backup hot-backup enable コマンドを使用して、IRF スタックユニットでのクライアントバックアップ機能を有効にします。

undo wlan client-backup hot-backup enable コマンドを使用して、IRF スタックユニットでのクライアントバックアップ機能を無効にします。

本コマンドを有効にするには、AP バックアップを有効にする必要があります。

クライアントバックアップを有効にすることで、Master 装置は関連付いているクライアントの情報をメンバ装置にバックアップすることができます。Master 装置がダウンしたとき、クライアントは常にオンラインの状態でメンバ装置に関連付きます。

本コマンドは、クライアントバックアップを有効にした後にオンラインになったクライアントにのみ適用されます。クライアントバックアップを無効にすることで、メンバ装置からクライアントのバックアップ情報を削除します。

例

クライアントバックアップを有効にします。

<AC> system-view

[AC] wlan client-backup hot-backup enable

1.1.24 wlan client-backup hot-backup delay

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.18 を含む以降のソフトウェアからサポートしています。

Syntax

wlan client-backup hot-backup delay *delay-time*

undo wlan client-backup hot-backup delay

デフォルト

60 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

delay-time:クライアントに関する情報をバックアップするまでの遅延時間を 0 秒から 300 秒の範囲で指定します。遅延時間を 0 に設定すると、IRF スタックユニットの Master

装置は関連付けられたクライアントに関する情報の変更を他のメンバ装置にリアルタイムでバックアップします。

説明

wlan client-backup hot-backup delay コマンドは、クライアントに関する情報の変更を、IRF スタックユニットの Master 装置が他のメンバ装置にバックアップするまでの遅延時間を設定します。

undo wlan client-backup hot-backup enable コマンドはデフォルトに戻します。

本コマンドを有効にするには、クライアントバックアップ機能を有効にする必要があります。

本コマンドは、クライアントバックアップ遅延時間を設定した後にオンラインになったクライアントにのみ適用されます。

クライアントが接続されてから遅延時間が経過する前に Master /Standby の切り替わりが発生した場合、情報がバックアップされていないクライアントは再接続が必要になります。

例

クライアントのバックアップ遅延を 240 秒にします。

<AC> system-view

[AC] wlan client-backup hot-backup delay 240

関連コマンド

wlan client-backup hot-backup enable