
AX6700S・AX6600S・AX6300S ソフトウェアマニュアル
コンフィギュレーションガイド Vol.1

Ver. 11.7 対応

AX63S-S001-C0

Alaxala

対象製品

このマニュアルは AX6700S, AX6600S および AX6300S モデルを対象に記載しています。また, AX6700S, AX6600S および AX6300S のソフトウェア Ver. 11.7 の機能について記載しています。ソフトウェア機能は, 基本ソフトウェア OS-SE およびオプションライセンスによってサポートする機能について記載します。

輸出時の注意

本製品を輸出される場合には, 外国為替及び外国貿易法の規制ならびに米国の輸出管理規則など外国の輸出関連法規をご確認のうえ, 必要な手続きをお取りください。なお, 不明な場合は, 弊社担当営業にお問い合わせください。

商標一覧

Cisco は, 米国 Cisco Systems, Inc. の米国および他の国々における登録商標です。

Ethernet は, 富士ゼロックス株式会社の登録商標です。

Internet Explorer は, 米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。

IPX は, Novell, Inc. の商標です。

Microsoft は, 米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Octpower は, 日本電気(株)の登録商標です。

sFlow は, 米国およびその他の国における米国 InMon Corp. の登録商標です。

UNIX は, The Open Group の米国ならびに他の国における登録商標です。

VitalQIP, VitalQIP Registration Manager は, Lucent technologies の商標です。

VLANAccessClient は, NEC ソフトの商標です。

VLANAccessController, VLANAccessAgent は, NEC の商標です。

Windows は, 米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

イーサネットは, 富士ゼロックス株式会社の登録商標です。

そのほかの記載の会社名, 製品名は, それぞれの会社の商標もしくは登録商標です。

マニュアルはよく読み, 保管してください。

製品を使用する前に, 安全上の説明をよく読み, 十分理解してください。

このマニュアルは, いつでも参照できるよう, 手近な所に保管してください。

ご注意

このマニュアルの内容については, 改良のため, 予告なく変更する場合があります。

発行

2012年 1月(第13版) AX63S - S001 - C0

著作権

All Rights Reserved, Copyright(C), 2006, 2012, ALAXALA Networks, Corp.

変更履歴

【Ver. 11.7 対応版】

表 変更履歴

章・節・項・タイトル	追加・変更内容
3.2 AX6700S の収容条件	<ul style="list-style-type: none">「3.2.4 レイヤ 2 スイッチ」に「(7) ポリシーベーススイッチング」を追加しました。「3.2.13 IPv4・IPv6 マルチキャストルーティングプロトコル」の「(1) IPv4 マルチキャスト」の、マルチキャスト送信元の数および IGMP 加入グループ数を変更しました。
3.4 AX6600S の収容条件	<ul style="list-style-type: none">「3.4.4 レイヤ 2 スイッチ」に「(7) ポリシーベーススイッチング」を追加しました。「3.4.13 IPv4・IPv6 マルチキャストルーティングプロトコル」の「(1) IPv4 マルチキャスト」の、マルチキャスト送信元の数および IGMP 加入グループ数を変更しました。
3.6 AX6300S の収容条件	<ul style="list-style-type: none">「3.6.4 レイヤ 2 スイッチ」に「(7) ポリシーベーススイッチング」を追加しました。「3.6.13 IPv4・IPv6 マルチキャストルーティングプロトコル」の「(1) IPv4 マルチキャスト」の、マルチキャスト送信元の数および IGMP 加入グループ数を変更しました。
7.2.6 VRF での telnet によるログインを許可する	<ul style="list-style-type: none">「(2) 指定 VRF から telnet によるログインを許可する場合」を追加しました。
7.2.7 VRF での ftp によるログインを許可する	<ul style="list-style-type: none">「(2) 指定 VRF から ftp によるログインを許可する場合」を追加しました。
25 ポリシーベーススイッチング	<ul style="list-style-type: none">本章を追加しました。

なお、単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 11.5 対応版】

表 変更履歴

項目	追加・変更内容
ソフトウェア	<ul style="list-style-type: none">オプションライセンス OP-MBSE の記述を追加しました。
AX6700S の収容条件	<ul style="list-style-type: none">「IPv4・IPv6 マルチキャストルーティングプロトコル」の「(1) IPv4 マルチキャスト」に PIM-DM に関する記述を追加しました。
AX6600S の収容条件	<ul style="list-style-type: none">「IPv4・IPv6 マルチキャストルーティングプロトコル」の「(1) IPv4 マルチキャスト」に PIM-DM に関する記述を追加しました。
AX6300S の収容条件	<ul style="list-style-type: none">「IPv4・IPv6 マルチキャストルーティングプロトコル」の「(1) IPv4 マルチキャスト」に PIM-DM に関する記述を追加しました。
RADIUS/TACACS+ を使用した認証	<ul style="list-style-type: none">「(1) 認証サービスの選択」に end-by-reject の記述を追加しました。「(3) RADIUS/TACACS+ サーバへの登録情報」に装置管理者モードへの変更時のユーザ名属性について記述を追加しました。
装置の状態確認	<ul style="list-style-type: none">装置の環境状態および温度履歴情報の確認について記述を追加しました。
マスタノードの両リングポートが共有リンクとなる構成	<ul style="list-style-type: none">本項を追加しました。
隣接リング用フラッシュ制御フレームの送信設定	<ul style="list-style-type: none">本項を追加しました。

【Ver. 11.4 対応版】

表 変更履歴

項目	追加・変更内容
ソフトウェア	<ul style="list-style-type: none"> オプションライセンス OP-DH6R の記述を追加しました。
AX6700S の収容条件	<ul style="list-style-type: none"> 「(1) テーブルエントリ数」の「(c) 配分パターン」に DHCP snooping が有効な場合のフィルタエントリ数の記述を追加しました。 「(13) レイヤ 2 認証」を追加しました。 「(14) Web 認証」にダイナミック VLAN モードの記述を追加しました。 「(15) MAC 認証」にダイナミック VLAN モードの記述を追加しました。 「(18) DHCP snooping」を追加しました。 「(23) IPv6 DHCP リレー」を追加しました。 「(31) IPv6 マルチキャスト」にエクストラネット関連の記述を追加しました。
AX6600S の収容条件	<ul style="list-style-type: none"> 「(1) テーブルエントリ数」の「(c) 配分パターン」に DHCP snooping が有効な場合のフィルタエントリ数の記述を追加しました。 「(13) レイヤ 2 認証」を追加しました。 「(14) Web 認証」にダイナミック VLAN モードの記述を追加しました。 「(15) MAC 認証」にダイナミック VLAN モードの記述を追加しました。 「(18) DHCP snooping」を追加しました。 「(23) IPv6 DHCP リレー」を追加しました。 「(31) IPv6 マルチキャスト」にエクストラネット関連の記述を追加しました。
AX6300S の収容条件	<ul style="list-style-type: none"> 「(1) テーブルエントリ数」の「(c) 配分パターン」に DHCP snooping が有効な場合のフィルタエントリ数の記述を追加しました。 「(13) レイヤ 2 認証」を追加しました。 「(14) Web 認証」にダイナミック VLAN モードの記述を追加しました。 「(15) MAC 認証」にダイナミック VLAN モードの記述を追加しました。 「(18) DHCP snooping」を追加しました。 「(23) IPv6 DHCP リレー」を追加しました。 「(31) IPv6 マルチキャスト」にエクストラネット関連の記述を追加しました。
VRF での telnet によるログインを許可する	<ul style="list-style-type: none"> 本項を追加しました。
VRF での ftp によるログインを許可する	<ul style="list-style-type: none"> 本項を追加しました。
VRF でのリモート運用端末からのログインの許可	<ul style="list-style-type: none"> 本項を追加しました。
VRF でのリモート運用端末からのログインを許可する IP アドレスの設定	<ul style="list-style-type: none"> 本項を追加しました。
省電力機能	<ul style="list-style-type: none"> トラフィック量による省電力機能のサポートに伴い記述を追加しました。 NIF の冗長化サポートに伴い記述を追加しました。
レイヤ 2 認証機能との連携について	<ul style="list-style-type: none"> MAC 認証の記述を追加しました。
レイヤ 2 中継遮断機能の解説	<ul style="list-style-type: none"> 本節を追加しました。
レイヤ 2 中継遮断機能のコンフィグレーション	<ul style="list-style-type: none"> 本節を追加しました。

【Ver. 11.3 対応版】

表 変更履歴

項目	追加・変更内容
AX6700S の収容条件	<ul style="list-style-type: none"> 「(12) アクセスリストロギング」を追加しました。 「(30) IPv6 マルチキャスト」に VRF に関する記述を追加しました。

項目	追加・変更内容
AX6600S の収容条件	<ul style="list-style-type: none"> 「(12) アクセスリストロギング」を追加しました。 「(30) IPv6 マルチキャスト」に VRF に関する記述を追加しました。
AX6300S の収容条件	<ul style="list-style-type: none"> 「(12) アクセスリストロギング」を追加しました。 「(30) IPv6 マルチキャスト」に VRF に関する記述を追加しました。

【Ver. 11.2 対応版】

表 変更履歴

項目	追加・変更内容
AX6700S の収容条件	<ul style="list-style-type: none"> 「(1) テーブルエントリ数」のフロー系テーブル容量に、standard-advance と extended-advance を追加しました。 「(20) CFM」の、CFM の収容条件および CFM のデータベース収容条件を変更しました。また、CCM 送信間隔による収容条件を追加しました。 「(26) DHCP サーバ」の最大インタフェース数と最大管理サブネット数を変更しました。 「(28) ユニキャストルーティングリソース」の経路エントリ数と最大隣接ルータ数の関係に、OSPFv3 で VRF を使用する場合の条件を追加しました。また、コンフィギュレーションの最大設定数で、OSPFv3 と経路フィルタの最大設定数を変更しました。 「(29) IPv4 マルチキャスト」にエクストラネット関連の記述を追加しました。 「(31) VRF」に、VRF 動作モードの記述を追加しました。
AX6600S の収容条件	<ul style="list-style-type: none"> 「(1) テーブルエントリ数」のフロー系テーブル容量に、standard-advance と extended-advance を追加しました。 「(20) CFM」の、CFM の収容条件および CFM のデータベース収容条件を変更しました。また、CCM 送信間隔による収容条件を追加しました。 「(26) DHCP サーバ」の最大インタフェース数と最大管理サブネット数を変更しました。 「(28) ユニキャストルーティングリソース」の経路エントリ数と最大隣接ルータ数の関係に、OSPFv3 で VRF を使用する場合の条件を追加しました。また、コンフィギュレーションの最大設定数で、OSPFv3 と経路フィルタの最大設定数を変更しました。 「(29) IPv4 マルチキャスト」にエクストラネット関連の記述を追加しました。 「(31) VRF」に、VRF 動作モードの記述を追加しました。
AX6300S の収容条件	<ul style="list-style-type: none"> 「(1) テーブルエントリ数」のフロー系テーブル容量に、standard-advance と extended-advance を追加しました。 「(20) CFM」の、CFM の収容条件および CFM のデータベース収容条件を変更しました。また、CCM 送信間隔による収容条件を追加しました。 「(26) DHCP サーバ」の最大インタフェース数と最大管理サブネット数を変更しました。 「(27) ユニキャストルーティングリソース」の経路エントリ数と最大隣接ルータ数の関係に、OSPFv3 で VRF を使用する場合の条件を追加しました。また、コンフィギュレーションの最大設定数で、OSPFv3 と経路フィルタの最大設定数を変更しました。 「(28) IPv4 マルチキャスト」にエクストラネット関連の記述を追加しました。 「(31) VRF」に、VRF 動作モードの記述を追加しました。
RADIUS/TACACS+ の適用機能および範囲	<ul style="list-style-type: none"> コンソールからのログイン認証および装置管理者モードへの変更 (enable コマンド) 時の認証の記述を追加しました。
RADIUS/TACACS+ を使用した認証	<ul style="list-style-type: none"> コンソールからのログイン認証および装置管理者モードへの変更 (enable コマンド) 時の認証の記述を追加しました。

項目	追加・変更内容
RADIUS サーバによる認証の設定	• 「(2) 装置管理者モードへの変更 (enable コマンド) 時の認証の設定例」を追加しました。
TACACS+ サーバによる認証の設定	• 「(2) 装置管理者モードへの変更 (enable コマンド) 時の認証の設定例」を追加しました。
VRF での NTP による時刻同期の設定	• 本項を追加しました。
テーブルエントリの配分パターンの設定	• フローテーブル容量に、standard-advance と extended-advance を追加しました。
10BASE-T/100BASE-TX/1000BASE-T 用 SFP	• 本項を追加しました。
経路切り戻し抑止および解除時の動作	• 本項を追加しました。
経路切り戻し抑止および解除時の動作	• 本項を追加しました。
Ring Protocol 使用時の注意事項	• 「(16) 経路切り戻し抑止機能適用時のフラッシュ制御フレーム受信待ち保護時間の設定について」を追加しました。
各種パラメータの設定	• 「(6) 経路切り戻し抑止機能の有効化および抑止時間の設定」を追加しました。

【Ver. 11.1 対応版】

表 変更履歴

項目	追加・変更内容
本装置のモデル	• AX6600S の記述を追加しました。
AX6700S ハードウェアの構成	• BCU-S11 の記述を追加しました。
AX6600S ハードウェアの構成	• 本項を追加しました。
AX6300S ハードウェアの構成	• MSU-1A1 および MSU-1B1 の記述を追加しました。
AX6600S の搭載条件	• 本項を追加しました。
AX6700S の収容条件	• 「(19) L2 ループ検知」「(b) ネットワーク全体での動作可能装置数」の記述を変更しました。 • 「(20) CFM」を追加しました。
AX6600S の収容条件	• 本項を追加しました。
AX6300S の収容条件	• 「(1) テーブルエントリ数」に MSU-1A1 および MSU-1B1 の記述を追加しました。 • 「(2) MSU 経路配分パターン」に MSU-1A1 および MSU-1B1 の記述を追加しました。 • 「(10) IGMP snooping / MLD snooping」に MSU-1A1 および MSU-1B1 の記述を追加しました。 • 「(11) フィルタ・QoS」に MSU-1A1 および MSU-1B1 の記述を追加しました。 • 「(19) L2 ループ検知」「(b) ネットワーク全体での動作可能装置数」の記述を変更しました。 • 「(20) CFM」を追加しました。 • 「(27) ユニキャストルーティングリソース」に MSU-1A1 および MSU-1B1 の記述を追加しました。 • 「(28) IPv4 マルチキャスト」に MSU-1A1 および MSU-1B1 の記述を追加しました。 • 「(29) IPv6 マルチキャスト」に MSU-1A1 および MSU-1B1 の記述を追加しました。
NIF ポートの LED 確認	• 本項を追加しました。
装置の温度監視	• 本節を追加しました。
省電力機能	• 本章を追加しました。

項目	追加・変更内容
無停止ソフトウェアアップデート	<ul style="list-style-type: none"> AX6600S の記述を追加しました。

【Ver. 11.0 対応版】

表 変更履歴

項目	追加・変更内容
本装置の概要	<ul style="list-style-type: none"> ネットワーク・パーティションの記述を追加しました。
本装置の特長	<ul style="list-style-type: none"> 「(6) ネットワーク・パーティション対応」を追加しました。
AX6700S ハードウェアの構成	<ul style="list-style-type: none"> 「(5) NIF (ネットワークインタフェース機構)」に NK1GS-8M に関する記述を追加しました。
AX6300S ハードウェアの構成	<ul style="list-style-type: none"> 「(4) NIF (ネットワークインタフェース機構)」に NH1GS-6M に関する記述を追加しました。
ソフトウェア	<ul style="list-style-type: none"> VRF およびオプションライセンス OP-NPAR の記述を追加しました。
AX6700S の搭載条件	<ul style="list-style-type: none"> 「(2) 最大搭載数」に NK1GS-8M に関する記述を追加しました。
AX6300S の搭載条件	<ul style="list-style-type: none"> 「(2) 最大搭載数」に NH1GS-6M に関する記述を追加しました。
AX6700S の収容条件	<ul style="list-style-type: none"> 「(2) BSU 経路配分パターン」に VRF に関する記述を追加しました。 「(9) Ring Protocol」に VRF 機能との併用の記述を追加しました。また、NK1GS-8M の記述を追加しました。 「(11) フィルタ・QoS」に「(c) 階層化シェーパ」を追加しました。 「(17) VRRP」の記述を変更しました。また、グループ切替機能使用時の記述を追加しました。 「(24) DHCP/BOOTP リレー」に VRF に関する記述を追加しました。また、装置当たりの収容条件を変更しました。 「(27) ユニキャストルーティングリソース」に VRF に関する記述を追加しました。また、本装置に設定できるコンフィギュレーションの最大数を追加しました。 「(28) IPv4 マルチキャスト」に VRF に関する記述を追加しました。 「(30) VRF」を追加しました。
AX6300S の収容条件	<ul style="list-style-type: none"> 「(1) テーブルエントリ数」に VRF に関する記述を追加しました。 「(9) Ring Protocol」に VRF 機能との併用の記述を追加しました。また、NH1GS-6M の記述を追加しました。 「(11) フィルタ・QoS」に「(c) 階層化シェーパ」を追加しました。 「(17) VRRP」の記述を変更しました。また、グループ切替機能使用時の記述を追加しました。 「(24) DHCP/BOOTP リレー」に VRF に関する記述を追加しました。また、装置当たりの収容条件を変更しました。 「(27) ユニキャストルーティングリソース」に VRF に関する記述を追加しました。また、本装置に設定できるコンフィギュレーションの最大数を追加しました。 「(28) IPv4 マルチキャスト」に VRF に関する記述を追加しました。 「(30) VRF」を追加しました。
10BASE-T/100BASE-TX/1000BASE-T・1000BASE-X 選択型ポート	<ul style="list-style-type: none"> 本項を追加しました。
選択型ポートでの 10BASE-T/100BASE-TX/1000BASE-T の設定	<ul style="list-style-type: none"> 本項を追加しました。
MAC アドレステーブルのクリア	<ul style="list-style-type: none"> 本項を追加しました。
サポート仕様	<ul style="list-style-type: none"> VLAN マッピングに関する記述を追加しました。また、VRF 機能との併用の記述を追加しました。
Ring Protocol 使用時の注意事項	<ul style="list-style-type: none"> 「(18) Ring Protocol と VRF 機能の併用について」を追加しました。
IGMP snooping/MLD snooping の解説	<ul style="list-style-type: none"> IGMP 即時離脱機能の記述を追加しました。

【Ver. 10.7 対応版】

表 変更履歴

項目	追加・変更内容
AX6700S の収容条件	<ul style="list-style-type: none"> 「(16) L2 ループ検知」の記述を追加しました。 「(27) IPv4 マルチキャスト」のランデブーポイント数および BSR 候補数を変更しました。
AX6300S の収容条件	<ul style="list-style-type: none"> 「(16) L2 ループ検知」の記述を追加しました。 「(27) IPv4 マルチキャスト」のランデブーポイント数および BSR 候補数を変更しました。
CLI 設定のカスタマイズ	<ul style="list-style-type: none"> 本項を追加しました。
RADIUS/TACACS+ の適用機能および範囲	<ul style="list-style-type: none"> NAS-IPv6-Address の記述を追加しました。
Port 情報の表示	<ul style="list-style-type: none"> 1000BASE-LHB の記述を追加しました。
HDC アップデート設定	<ul style="list-style-type: none"> 本項を追加しました。
NIF の状態確認	<ul style="list-style-type: none"> NIF の HDC アップデート要否の確認について記述を追加しました。
無停止ソフトウェアアップデートに関する注意事項	<ul style="list-style-type: none"> NIF に関する注意事項を追加しました。
リンクアップ検出タイマの設定	<ul style="list-style-type: none"> 本項を追加しました。
自動 MDIX の設定	<ul style="list-style-type: none"> 本項を追加しました。
機能一覧	<ul style="list-style-type: none"> 1000BASE-LHB の記述を追加しました。
レイヤ 2 スイッチ機能と他機能の共存について	<ul style="list-style-type: none"> 「表 16-3 スパニングツリーでの制限事項」から Ring Protocol を削除しました。 「表 16-4 Ring Protocol での制限事項」からマルチプルスパニングツリーおよび GSRP を削除しました。
VLAN debounce 機能の解説	<ul style="list-style-type: none"> 本節を追加しました。
VLAN debounce 機能のコンフィギュレーション	<ul style="list-style-type: none"> 本節を追加しました。
動作仕様	<ul style="list-style-type: none"> Ring Protocol とマルチプルスパニングツリーとの共存サポートに伴い記述を追加しました。
各種スパニングツリーとの共存について	<ul style="list-style-type: none"> Ring Protocol とマルチプルスパニングツリーとの共存サポートに伴い記述を追加しました。
Ring Protocol とスパニングツリー併用時の注意事項	<ul style="list-style-type: none"> Ring Protocol とマルチプルスパニングツリーとの共存サポートに伴い記述を追加および変更しました。
Ring Protocol と GSRP との併用	<ul style="list-style-type: none"> 本節を追加しました。
Ring Protocol とマルチプルスパニングツリーとの併用設定	<ul style="list-style-type: none"> 本項を追加しました。
Ring Protocol と GSRP との併用設定	<ul style="list-style-type: none"> 本項を追加しました。
仮想リンクの状態の確認	<ul style="list-style-type: none"> Ring Protocol と GSRP の共存サポートに伴い記述を追加しました。

【Ver. 10.6 対応版】

表 変更履歴

項目	追加・変更内容
AX6700S の搭載条件	<ul style="list-style-type: none"> 「(1) 最大収容ポート数」に 10GBASE-ZR の記述を追加しました。
AX6300S の搭載条件	<ul style="list-style-type: none"> 「(1) 最大収容ポート数」に 10GBASE-ZR の記述を追加しました。

項目	追加・変更内容
AX6700S の収容条件	<ul style="list-style-type: none"> 「(9) Ring Protocol」に Ring Protocol とスパニングツリーの併用時の記述を追加しました。 「(14) MAC 認証」を追加しました。
AX6300S の収容条件	<ul style="list-style-type: none"> 「(9) Ring Protocol」に Ring Protocol とスパニングツリーの併用時の記述を追加しました。 「(14) MAC 認証」を追加しました。
電力制御	<ul style="list-style-type: none"> 電力制御の設定を有効にするための記述を変更しました。
障害部位と復旧内容	<ul style="list-style-type: none"> BSU の固定モードサポートに伴って記述を変更しました。
10GBASE-R の解説	<ul style="list-style-type: none"> 10GBASE-ZR の記述を追加しました。
レイヤ 2 スイッチ機能と他機能の共存について	<ul style="list-style-type: none"> Ring Protocol とスパニングツリーの併用サポートに伴い記述を変更しました。
ループガード	<ul style="list-style-type: none"> 「(2) ループガードに関する注意事項」の記述を変更しました。
VLAN マッピングの使用法	<ul style="list-style-type: none"> 本項を追加しました。
制御 VLAN の forwarding-delay-time の使用法	<ul style="list-style-type: none"> 本項を追加しました。
リングポートにリンクアグリゲーションを使用する場合について	<ul style="list-style-type: none"> リンクアグリゲーションを使用できるリングポート数の算出式を変更しました。
Ring Protocol 設定の流れ	<ul style="list-style-type: none"> 「(1) スパニングツリーの停止」にスパニングツリーとの併用について記述を追加しました。
制御 VLAN の設定	<ul style="list-style-type: none"> 「(1) 制御 VLAN の設定」を追加しました。 「(2) 制御 VLAN のフォワーディング遷移時間の設定」を追加しました。
VLAN マッピングの設定	<ul style="list-style-type: none"> 「(1) VLAN 新規設定」にリングネットワーク内で使用するデータ転送用 VLAN の設定について記述を追加しました。
Ring Protocol とスパニングツリーの併用	<ul style="list-style-type: none"> 本章を追加しました。

【Ver. 10.5 対応版】

表 変更履歴

項目	追加・変更内容
AX6700S の搭載条件	<ul style="list-style-type: none"> 1000BASE-SX2 および 1000BASE-BX を追加しました。
AX6300S の搭載条件	<ul style="list-style-type: none"> 1000BASE-SX2 および 1000BASE-BX を追加しました。
AX6700S の収容条件	<ul style="list-style-type: none"> 「(13) Web 認証」に Web 認証の画面入れ替えについての記述を追加しました。
AX6300S の収容条件	<ul style="list-style-type: none"> 「(13) Web 認証」に Web 認証の画面入れ替えについての記述を追加しました。
Port 情報の表示	<ul style="list-style-type: none"> 1000BASE-SX2 および 1000BASE-BX を追加しました。
1000BASE-X の解説	<ul style="list-style-type: none"> 1000BASE-SX2 および 1000BASE-BX を追加しました。
STP 互換モード	<ul style="list-style-type: none"> 本項を追加しました。
IGMP snooping/MLD snooping の解説	<ul style="list-style-type: none"> IGMPv3/MLDv2 snooping の記述を追加しました。

【Ver. 10.4 対応版】

表 変更履歴

項目	追加・変更内容
AX6700S の収容条件	<ul style="list-style-type: none"> • スパニングツリーの記述を変更しました。 • Ring Protocol の記述を追加しました。
AX6300S の収容条件	<ul style="list-style-type: none"> • スパニングツリーの記述を変更しました。 • Ring Protocol の記述を追加しました。
Ring Protocol の解説	<ul style="list-style-type: none"> • 本章を追加しました。
Ring Protocol の設定と運用	<ul style="list-style-type: none"> • 本章を追加しました。

【Ver. 10.3 対応版】

表 変更履歴

項目	追加・変更内容
装置の外観	<ul style="list-style-type: none"> • AX6700S の記述を追加しました。
AX6700S ハードウェアの構成	<ul style="list-style-type: none"> • 本項を追加しました。
AX6700S の搭載条件	<ul style="list-style-type: none"> • 本項を追加しました。
AX6700S の収容条件	<ul style="list-style-type: none"> • 本項を追加しました。
運用端末の接続形態	<ul style="list-style-type: none"> • シリアル接続ポート (AUX) の記述を追加しました。
運用端末	<ul style="list-style-type: none"> • シリアル接続ポート (AUX) の記述を追加しました。
ダイヤルアップ IP 接続	<ul style="list-style-type: none"> • 本項を追加しました。
障害時の復旧	<ul style="list-style-type: none"> • 本節を追加しました。
BSU/NIF の管理	<ul style="list-style-type: none"> • BSU の説明を追加しました。
無停止ソフトウェアアップデート	<ul style="list-style-type: none"> • 本節を追加しました。
IGMP snooping/MLD snooping の解説	<ul style="list-style-type: none"> • 本章を追加しました。
IGMP snooping/MLD snooping の設定と運用	<ul style="list-style-type: none"> • 本章を追加しました。

はじめに

対象製品およびソフトウェアバージョン

このマニュアルは AX6700S, AX6600S および AX6300S モデルを対象に記載しています。また, AX6700S, AX6600S および AX6300S のソフトウェア Ver. 11.7 の機能について記載しています。ソフトウェア機能は, 基本ソフトウェア OS-SE およびオプションライセンスによってサポートする機能について記載します。

操作を行う前にこのマニュアルをよく読み, 書かれている指示や注意を十分に理解してください。また, このマニュアルは必要なときにすぐ参照できるように使いやすい場所に保管してください。

なお, このマニュアルでは特に断らないかぎり AX6700S, AX6600S および AX6300S に共通の機能について記載しますが, 機種固有の機能については以下のマークで示します。

【AX6700S】:

AX6700S についての記述です。

【AX6600S】:

AX6600S についての記述です。

【AX6300S】:

AX6300S についての記述です。

また, このマニュアルでは特に断らないかぎり基本ソフトウェア OS-SE の機能について記載しますが, オプションライセンスでサポートする機能については以下のマークで示します。

【OP-BGP】:

オプションライセンス OP-BGP についての記述です。

【OP-DH6R】:

オプションライセンス OP-DH6R についての記述です。

【OP-MBSE】:

オプションライセンス OP-MBSE についての記述です。

【OP-NPAR】:

オプションライセンス OP-NPAR についての記述です。

【OP-VAA】:

オプションライセンス OP-VAA についての記述です。

このマニュアルの訂正について

このマニュアルに記載の内容は, ソフトウェアと共に提供する「リリースノート」および「マニュアル訂正資料」で訂正する場合があります。

対象読者

本装置を利用したネットワークシステムを構築し, 運用するシステム管理者の方を対象としています。また, 次に示す知識を理解していることを前提としています。

- ネットワークシステム管理の基礎的な知識

このマニュアルの URL

このマニュアルの内容は下記 URL に掲載しております。

<http://www.alaxala.com>

マニュアルの読書手順

本装置の導入，セットアップ，日常運用までの作業フローに従って，それぞれの場合に参照するマニュアルを次に示します。

●装置の開梱から，初期導入時の基本的な設定を知りたい

AX6700S クイックスタートガイド (AX67S-Q001)	AX6600S クイックスタートガイド (AX66S-Q001)	AX6300S クイックスタートガイド (AX63S-Q001)
--	--	--

●ハードウェアの設備条件，取扱方法を調べる

AX6700S ハードウェア取扱説明書 (AX67S-H001)	AX6600S ハードウェア取扱説明書 (AX66S-H001)	AX6300S ハードウェア取扱説明書 (AX63S-H001)
--	--	--

●ソフトウェアの機能，コンフィグレーションの設定，運用コマンドを知りたい

▽まず，ガイドで使用する機能や収容条件についてご確認ください。

- | | | |
|--|---|--|
| <ul style="list-style-type: none"> ・収容条件 ・ログインなどの基本操作 ・VLAN，スパンニングツリー | <ul style="list-style-type: none"> ・フィルタ，QoS ・レイヤ2認証 ・高信頼化機能 | <ul style="list-style-type: none"> ・IPv4，IPv6パケット中継 ・IPv4，IPv6ルーティング
プロトコル |
|--|---|--|

コンフィグレーションガイド Vol. 1 (AX63S-S001)	コンフィグレーションガイド Vol. 2 (AX63S-S002)	コンフィグレーションガイド Vol. 3 (AX63S-S003)
---	---	---

▽必要に応じて，レファレンスをご確認ください。

- ・コマンドの入カシンタックス，パラメータ詳細について

コンフィグレーション コマンドレファレンス Vol. 1 (AX63S-S004)	コンフィグレーション コマンドレファレンス Vol. 2 (AX63S-S010)	コンフィグレーション コマンドレファレンス Vol. 3 (AX63S-S005)
--	--	--

運用コマンドレファレンス Vol. 1 (AX63S-S006)	運用コマンドレファレンス Vol. 2 (AX63S-S011)	運用コマンドレファレンス Vol. 3 (AX63S-S007)
--	--	--

- ・メッセージとログについて

メッセージ・ログレファレンス (AX63S-S008)

- ・MIBについて

MIBレファレンス (AX63S-S009)

●トラブル発生時の対処方法について知りたい

トラブルシューティングガイド (AX36S-T001)

このマニュアルでの表記

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BCU	Basic Control Unit
BGP	Border Gateway Protocol

BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second *bpsと表記する場合もあります。
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
BSU	Basic Switching Unit
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
CSU	Control and Switching Unit
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLPQ	Low Latency Priority Queueing
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LLRLQ	Low Latency Rate Limited Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MA	Maintenance Association
MAC	Media Access Control

MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MSU	Management and Switching Unit
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NIF	Network Interface
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations,Administration,and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
packet/s	packets per second *ppsと表記する場合があります。
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PID	Protocol Identifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
PSP	Packet Switching Processor
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RGQ	Rate Guaranteed Queueing
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SElector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SOP	System Operational Panel
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter

TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
uRPF	unicast Reverse Path Forwarding
VAA	VLAN Access Agent
VLAN	Virtual LAN
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WGQ	Weighted Guaranteed Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

kB(バイト)などの単位表記について

1kB(キロバイト), 1MB(メガバイト), 1GB(ギガバイト), 1TB(テラバイト)はそれぞれ 1024 バイト, 1024^2 バイト, 1024^3 バイト, 1024^4 バイトです。

目次

第 1 編 本装置の概要と収容条件

1	本装置の概要	1
1.1	本装置の概要	2
1.2	本装置の特長	3
2	装置構成	7
2.1	本装置のモデル	8
2.1.1	装置の外観	8
2.2	装置の構成要素	16
2.2.1	AX6700S ハードウェアの構成【AX6700S】	16
2.2.2	AX6600S ハードウェアの構成【AX6600S】	18
2.2.3	AX6300S ハードウェアの構成【AX6300S】	19
2.2.4	ソフトウェア	21
3	収容条件	23
3.1	AX6700S の搭載条件【AX6700S】	24
3.1.1	最大収容ポート数	24
3.1.2	最大搭載数	24
3.2	AX6700S の収容条件【AX6700S】	25
3.2.1	テーブルエントリ数	25
3.2.2	BSU 経路配分パターン	28
3.2.3	リンクアグリゲーション	31
3.2.4	レイヤ 2 スイッチ	31
3.2.5	フィルタ・QoS	39
3.2.6	レイヤ 2 認証	41
3.2.7	DHCP snooping	44
3.2.8	冗長化構成による高信頼化	45
3.2.9	ネットワークの障害検出による高信頼化機能	46
3.2.10	隣接装置情報の管理 (LLDP/OADP)	49
3.2.11	IPv4・IPv6 パケット中継	49
3.2.12	IPv4・IPv6 ルーティングプロトコル	54
3.2.13	IPv4・IPv6 マルチキャストルーティングプロトコル	58
3.2.14	VRF【OP-NPAR】	66
3.3	AX6600S の搭載条件【AX6600S】	67
3.3.1	最大収容ポート数	67
3.3.2	最大搭載数	67
3.4	AX6600S の収容条件【AX6600S】	68

3.4.1	テーブルエン트리数	68
3.4.2	CSU 経路配分パターン	71
3.4.3	リンクアグリゲーション	74
3.4.4	レイヤ 2 スイッチ	74
3.4.5	フィルタ・QoS	82
3.4.6	レイヤ 2 認証	85
3.4.7	DHCP snooping	88
3.4.8	冗長化構成による高信頼化	89
3.4.9	ネットワークの障害検出による高信頼化機能	90
3.4.10	隣接装置情報の管理 (LLDP/OADP)	92
3.4.11	IPv4・IPv6 パケット中継	93
3.4.12	IPv4・IPv6 ルーティングプロトコル	98
3.4.13	IPv4・IPv6 マルチキャストルーティングプロトコル	102
3.4.14	VRF 【OP-NPAR】	109
3.5	AX6300S の搭載条件【AX6300S】	111
3.5.1	最大収容ポート数	111
3.5.2	最大搭載数	111
3.6	AX6300S の収容条件【AX6300S】	113
3.6.1	テーブルエン트리数	113
3.6.2	MSU 経路配分パターン	116
3.6.3	リンクアグリゲーション	119
3.6.4	レイヤ 2 スイッチ	119
3.6.5	フィルタ・QoS	127
3.6.6	レイヤ 2 認証	129
3.6.7	DHCP snooping	133
3.6.8	冗長化構成による高信頼化	134
3.6.9	ネットワークの障害検出による高信頼化機能	135
3.6.10	隣接装置情報の管理 (LLDP/OADP)	137
3.6.11	IPv4・IPv6 パケット中継	137
3.6.12	IPv4・IPv6 ルーティングプロトコル	142
3.6.13	IPv4・IPv6 マルチキャストルーティングプロトコル	146
3.6.14	VRF 【OP-NPAR】	154

第 2 編 運用管理

4	装置へのログイン	155
4.1	運用端末による管理	156
4.1.1	運用端末の接続形態	156
4.1.2	運用端末	157
4.1.3	運用管理機能の概要	158

4.2	装置起動	160
4.2.1	起動から停止までの概略	160
4.2.2	装置の起動	160
4.2.3	装置の停止	161
4.3	ログイン・ログアウト	162

5

	コマンド操作	163
5.1	コマンド入力モード	164
5.1.1	運用コマンド一覧	164
5.1.2	コマンド入力モード	164
5.2	CLI での操作	166
5.2.1	補完機能	166
5.2.2	ヘルプ機能	166
5.2.3	入力エラー位置指摘機能	166
5.2.4	コマンド短縮実行	167
5.2.5	ヒストリ機能	167
5.2.6	パイプ機能	169
5.2.7	リダイレクト	169
5.2.8	ページング	169
5.2.9	CLI 設定のカスタマイズ	169
5.3	CLI の注意事項	171
5.3.1	ログイン後に運用端末がダウンした場合	171
5.3.2	CLI の特殊キー操作時にログアウトした場合	171
5.3.3	待機系のファイルにアクセスする場合	171

6

	コンフィグレーション	173
6.1	コンフィグレーション	174
6.1.1	起動時のコンフィグレーション	174
6.1.2	運用中のコンフィグレーション	174
6.2	ランニングコンフィグレーションの編集概要	175
6.3	コンフィグレーションコマンド入力におけるモード遷移	176
6.4	コンフィグレーションの編集方法	178
6.4.1	コンフィグレーション・運用コマンド一覧	178
6.4.2	configure (configure terminal) コマンド	178
6.4.3	コンフィグレーションの表示・確認 (show コマンド)	179
6.4.4	コンフィグレーションの追加・変更・削除	181
6.4.5	コンフィグレーションの運用への反映	182
6.4.6	コンフィグレーションのファイルへの保存 (save コマンド)	183
6.4.7	コンフィグレーションの編集終了 (exit コマンド)	183
6.4.8	初期導入時のコンフィグレーションについて	184
6.4.9	コンフィグレーションの編集時の注意事項	184

6.5	コンフィグレーションの操作	186
6.5.1	コンフィグレーションのバックアップ	186
6.5.2	バックアップコンフィグレーションファイルの本装置への反映	186
6.5.3	ftp コマンドを使用したファイル転送	187
6.5.4	MC を使用したファイル転送	189
6.5.5	バックアップコンフィグレーションファイル反映時の注意事項	189

7

リモート運用端末から本装置へのログイン	191
---------------------	-----

7.1	解説	192
7.1.1	マネージメントポート接続	192
7.1.2	通信用ポート接続	194
7.1.3	ダイヤルアップ IP 接続	194
7.2	コンフィグレーション	198
7.2.1	コンフィグレーションコマンド一覧	198
7.2.2	マネージメントポートの設定	198
7.2.3	本装置への IP アドレスの設定	201
7.2.4	telnet によるログインを許可する	201
7.2.5	ftp によるログインを許可する	202
7.2.6	VRF での telnet によるログインを許可する【OP-NPAR】	202
7.2.7	VRF での ftp によるログインを許可する【OP-NPAR】	203
7.3	オペレーション	204
7.3.1	運用コマンド一覧	204
7.3.2	マネージメントポートの確認	205
7.3.3	リモート運用端末と本装置との通信の確認	205

8

ログインセキュリティと RADIUS/TACACS+	207
----------------------------	-----

8.1	ログインセキュリティの設定	208
8.1.1	コンフィグレーション・運用コマンド一覧	208
8.1.2	ログイン制御の概要	209
8.1.3	ログインユーザの作成と削除	209
8.1.4	装置管理者モード変更のパスワードの設定	210
8.1.5	リモート運用端末からのログインの許可	210
8.1.6	同時にログインできるユーザ数の設定	211
8.1.7	リモート運用端末からのログインを許可する IP アドレスの設定	211
8.1.8	ログインバナーの設定	212
8.1.9	VRF でのリモート運用端末からのログインの許可【OP-NPAR】	213
8.1.10	VRF でのリモート運用端末からのログインを許可する IP アドレスの設定【OP-NPAR】	214
8.2	RADIUS/TACACS+ の解説	217
8.2.1	RADIUS/TACACS+ の概要	217
8.2.2	RADIUS/TACACS+ の適用機能および範囲	217
8.2.3	RADIUS/TACACS+ を使用した認証	222

8.2.4	RADIUS/TACACS+/ ローカルを使用したコマンド承認	226
8.2.5	RADIUS/TACACS+ を使用したアカウントティング	237
8.2.6	RADIUS/TACACS+ との接続	240
8.3	RADIUS/TACACS+ のコンフィグレーション	241
8.3.1	コンフィグレーションコマンド一覧	241
8.3.2	RADIUS サーバによる認証の設定	241
8.3.3	TACACS+ サーバによる認証の設定	242
8.3.4	RADIUS/TACACS+/ ローカルによるコマンド承認の設定	243
8.3.5	RADIUS/TACACS+ によるログイン・ログアウトアカウントティングの設定	245
8.3.6	TACACS+ サーバによるコマンドアカウントティングの設定	246

9

時刻の設定と NTP	247
------------	-----

9.1	時刻の設定と NTP 確認	248
9.1.1	コンフィグレーションコマンド・運用コマンド一覧	248
9.1.2	システムクロックの設定	248
9.1.3	NTP によるタイムサーバと時刻同期の設定	249
9.1.4	NTP サーバとの時刻同期の設定	249
9.1.5	NTP 認証の設定	250
9.1.6	VRF での NTP による時刻同期の設定【OP-NPAR】	250
9.1.7	時刻変更に関する注意事項	251
9.1.8	時刻の確認	251

10

ホスト名と DNS	253
-----------	-----

10.1	解説	254
10.2	コンフィグレーション	255
10.2.1	コンフィグレーションコマンド一覧	255
10.2.2	ホスト名の設定	255
10.2.3	DNS の設定	255

11

装置の管理	257
-------	-----

11.1	システム操作パネル	258
11.1.1	メニュー構造	258
11.1.2	Port 情報の表示	259
11.1.3	CPU 使用率の表示	261
11.1.4	メモリ使用率の表示	261
11.1.5	バージョンの表示	262
11.1.6	温度情報の表示	264
11.1.7	ボードの交換	265
11.1.8	装置の停止	269
11.1.9	障害の表示	270

11.1.10	NIF ポートの LED 確認	271
11.2	装置の状態確認，および運用形態に関する設定	273
11.2.1	コンフィグレーション・運用コマンド一覧	273
11.2.2	ソフトウェアバージョンの確認	274
11.2.3	装置の状態確認	274
11.2.4	装置内メモリの確認	278
11.2.5	運用メッセージの出力抑止と確認	278
11.2.6	運用ログ情報の確認	278
11.2.7	テーブルエントリの配分パターンの設定	279
11.2.8	ハードウェアモードの設定	281
11.3	運用情報のバックアップ・リストア	283
11.3.1	運用コマンド一覧	283
11.3.2	BCU/CSU/MSU 二重化時の手順	283
11.3.3	BCU/CSU/MSU 一重化時の backup/restore コマンドを用いる手順	284
11.4	装置の温度監視	285
11.4.1	装置入気温度の監視対象	285
11.4.2	入気温度の監視レベルと動作	285
11.5	障害時の復旧	287
11.5.1	障害部位と復旧内容	287

12 BSU/NIF の管理 289

12.1	BSU の状態確認，および運用形態に関する設定 【AX6700S】	290
12.1.1	コンフィグレーション・運用コマンド一覧	290
12.1.2	ボードの disable 設定	290
12.1.3	BSU の状態確認	290
12.2	NIF の状態確認，および運用形態に関する設定	292
12.2.1	コンフィグレーション・運用コマンド一覧	292
12.2.2	ボードの disable 設定	292
12.2.3	HDC アップデート設定	292
12.2.4	NIF の状態確認	293

13 省電力機能 295

13.1	省電力機能の解説	296
13.1.1	省電力機能の概要	296
13.1.2	省電力機能 【AX6700S】	297
13.1.3	省電力機能 【AX6600S】	300
13.1.4	省電力機能 【AX6300S】	303
13.1.5	省電力機能のスケジューリング 【AX6700S】【AX6600S】	304
13.1.6	トラフィック量による省電力機能 【AX6700S】【AX6600S】	308
13.1.7	省電力機能に関する注意事項	309
13.2	省電力機能のコンフィグレーション	311

13.2.1	コンフィグレーションコマンド一覧	311
13.2.2	コンフィグレーションコマンド設定例【AX6700S】	313
13.2.3	コンフィグレーションコマンド設定例【AX6600S】	316
13.2.4	コンフィグレーションコマンド設定例【AX6300S】	318
13.3	省電力機能のオペレーション	320
13.3.1	運用コマンド一覧	320
13.3.2	省電力機能の状態確認	320
13.3.3	消費電力情報およびトラフィック情報の確認	321

14	ソフトウェアの管理	325
14.1	運用コマンド一覧	326
14.2	ソフトウェアのアップデート	327
14.3	無停止ソフトウェアアップデート	328
14.3.1	概要	328
14.3.2	無停止ソフトウェアアップデートの適用条件	328
14.3.3	無停止ソフトウェアアップデートの手順	328
14.3.4	無停止ソフトウェアアップデートに関する注意事項	329
14.4	オプションライセンスの設定	330

第3編 ネットワークインタフェース

15	イーサネット	331
15.1	イーサネット共通の解説	332
15.1.1	ネットワーク構成例	332
15.1.2	物理インタフェース	332
15.1.3	MACおよびLLC副層制御	333
15.1.4	本装置のMACアドレス	335
15.2	イーサネット共通のコンフィグレーション	336
15.2.1	コンフィグレーションコマンド一覧	336
15.2.2	複数インタフェースの一括設定	336
15.2.3	イーサネットのシャットダウン	337
15.2.4	ジャンボフレームの設定	337
15.2.5	リンクダウン検出タイマの設定	338
15.2.6	リンクアップ検出タイマの設定	339
15.2.7	フレーム送受信エラー通知の設定	339
15.3	イーサネット共通のオペレーション	342
15.3.1	運用コマンド一覧	342
15.3.2	イーサネットの動作状態を確認する	342
15.4	10BASE-T/100BASE-TX/1000BASE-Tの解説	343

15.4.1	機能一覧	343
15.4.2	10BASE-T/100BASE-TX/1000BASE-T・1000BASE-X 選択型ポート【AX6700S】【AX6600S】	348
15.4.3	10BASE-T/100BASE-TX/1000BASE-T 用 SFP	349
15.5	10BASE-T/100BASE-TX/1000BASE-T のコンフィグレーション	350
15.5.1	イーサネットの設定	350
15.5.2	フローコントロールの設定	351
15.5.3	自動 MDIX の設定	351
15.5.4	選択型ポートでの 10BASE-T/100BASE-TX/1000BASE-T の設定【AX6700S】【AX6600S】	351
15.6	1000BASE-X の解説	353
15.6.1	機能一覧	353
15.7	1000BASE-X のコンフィグレーション	358
15.7.1	ポートの設定	358
15.7.2	フローコントロールの設定	358
15.8	10GBASE-R の解説	359
15.8.1	機能一覧	359
15.9	10GBASE-R のコンフィグレーション	361
15.9.1	フローコントロールの設定	361

16 リンクアグリゲーション 363

16.1	リンクアグリゲーション基本機能の解説	364
16.1.1	概要	364
16.1.2	リンクアグリゲーションの構成	364
16.1.3	サポート仕様	364
16.1.4	チャンネルグループの MAC アドレス	365
16.1.5	フレーム送信時のポート振り分け	365
16.1.6	リンクアグリゲーション使用時の注意事項	366
16.2	リンクアグリゲーション基本機能のコンフィグレーション	368
16.2.1	コンフィグレーションコマンド一覧	368
16.2.2	スタティックリンクアグリゲーションの設定	368
16.2.3	LACP リンクアグリゲーションの設定	368
16.2.4	ポートチャンネルインタフェースの設定	370
16.2.5	チャンネルグループの削除	372
16.3	リンクアグリゲーション拡張機能の解説	374
16.3.1	スタンバイリンク機能	374
16.3.2	離脱ポート制限機能	375
16.3.3	異速度混在モード	375
16.4	リンクアグリゲーション拡張機能のコンフィグレーション	377
16.4.1	コンフィグレーションコマンド一覧	377
16.4.2	スタンバイリンク機能のコンフィグレーション	377
16.4.3	離脱ポート制限機能のコンフィグレーション	378
16.4.4	異速度混在モードのコンフィグレーション	378

16.5	リンクアグリゲーションのオペレーション	379
16.5.1	運用コマンド一覧	379
16.5.2	リンクアグリゲーションの状態の確認	379

第4編 レイヤ2スイッチ

17	レイヤ2スイッチ概説	381
17.1	概要	382
17.1.1	MAC アドレス学習	382
17.1.2	VLAN	382
17.2	サポート機能	383
17.3	レイヤ2スイッチ機能と他機能の共存について	384
18	MAC アドレス学習	387
18.1	MAC アドレス学習の解説	388
18.1.1	送信元 MAC アドレス学習	388
18.1.2	MAC アドレス学習の移動検出	388
18.1.3	学習 MAC アドレスのエージング	388
18.1.4	MAC アドレスによるレイヤ2スイッチング	388
18.1.5	スタティックエントリの登録	389
18.1.6	MAC アドレス学習の制限	389
18.1.7	MAC アドレステーブルのクリア	390
18.1.8	注意事項	391
18.2	MAC アドレス学習のコンフィグレーション	392
18.2.1	コンフィグレーションコマンド一覧	392
18.2.2	エージングタイムの設定	392
18.2.3	スタティックエントリの設定	392
18.2.4	MAC アドレス学習抑止の設定	393
18.2.5	MAC アドレス学習数制限の設定	393
18.3	MAC アドレス学習のオペレーション	394
18.3.1	運用コマンド一覧	394
18.3.2	MAC アドレス学習の状態の確認	394
18.3.3	MAC アドレス学習数の確認	394
19	VLAN	397
19.1	VLAN 基本機能の解説	398
19.1.1	VLAN の種類	398
19.1.2	ポートの種類	398

19.1.3	デフォルト VLAN	399
19.1.4	VLAN の優先順位	400
19.1.5	VLAN Tag	401
19.1.6	VLAN 使用時の注意事項	403
19.2	VLAN 基本機能のコンフィグレーション	404
19.2.1	コンフィグレーションコマンド一覧	404
19.2.2	VLAN の設定	404
19.2.3	ポートの設定	405
19.2.4	トランクポートの設定	405
19.2.5	VLAN Tag の TPID の設定	406
19.3	ポート VLAN の解説	408
19.3.1	アクセスポートとトランクポート	408
19.3.2	ネイティブ VLAN	408
19.3.3	ポート VLAN 使用時の注意事項	409
19.4	ポート VLAN のコンフィグレーション	410
19.4.1	コンフィグレーションコマンド一覧	410
19.4.2	ポート VLAN の設定	410
19.4.3	トランクポートのネイティブ VLAN の設定	411
19.5	プロトコル VLAN の解説	413
19.5.1	概要	413
19.5.2	プロトコルの識別	413
19.5.3	プロトコルポートとトランクポート	414
19.5.4	プロトコルポートのネイティブ VLAN	414
19.6	プロトコル VLAN のコンフィグレーション	415
19.6.1	コンフィグレーションコマンド一覧	415
19.6.2	プロトコル VLAN の作成	415
19.6.3	プロトコルポートのネイティブ VLAN の設定	417
19.7	MAC VLAN の解説	419
19.7.1	概要	419
19.7.2	装置間の接続と MAC アドレス設定	419
19.7.3	レイヤ 2 認証機能との連携について	420
19.7.4	VLAN 混在時のマルチキャストについて	420
19.8	MAC VLAN のコンフィグレーション	422
19.8.1	コンフィグレーションコマンド一覧	422
19.8.2	MAC VLAN の設定	422
19.8.3	MAC ポートのネイティブ VLAN の設定	425
19.9	VLAN インタフェース	426
19.9.1	IP アドレスを設定するインタフェース	426
19.9.2	VLAN インタフェースの MAC アドレス	426
19.10	VLAN インタフェースのコンフィグレーション	427
19.10.1	コンフィグレーションコマンド一覧	427
19.10.2	レイヤ 3 インタフェースとしての VLAN の設定	427

19.10.3	VLAN インタフェースの MAC アドレスの設定	427
19.11	VLAN のオペレーション	429
19.11.1	運用コマンド一覧	429
19.11.2	VLAN の状態の確認	429

20 VLAN 拡張機能 435

20.1	VLAN トンネリングの解説	436
20.1.1	概要	436
20.1.2	VLAN トンネリングを使用するための必須条件	436
20.1.3	VLAN トンネリング使用時の注意事項	437
20.2	VLAN トンネリングのコンフィグレーション	438
20.2.1	コンフィグレーションコマンド一覧	438
20.2.2	VLAN トンネリングの設定	438
20.3	Tag 変換の解説	439
20.3.1	概要	439
20.3.2	Tag 変換使用時の注意事項	439
20.4	Tag 変換のコンフィグレーション	440
20.4.1	コンフィグレーションコマンド一覧	440
20.4.2	Tag 変換の設定	440
20.5	L2 プロトコルフレーム透過機能の解説	442
20.5.1	概要	442
20.5.2	L2 プロトコルフレーム透過機能の注意事項	442
20.6	L2 プロトコルフレーム透過機能のコンフィグレーション	443
20.6.1	コンフィグレーションコマンド一覧	443
20.6.2	L2 プロトコルフレーム透過機能の設定	443
20.7	VLAN debounce 機能の解説	444
20.7.1	概要	444
20.7.2	VLAN debounce 機能の動作契機	444
20.7.3	VLAN debounce 機能と他機能との関係	445
20.7.4	VLAN debounce 機能使用時の注意事項	445
20.8	VLAN debounce 機能のコンフィグレーション	447
20.8.1	コンフィグレーションコマンド一覧	447
20.8.2	VLAN debounce 機能の設定	447
20.9	レイヤ 2 中継遮断機能の解説	448
20.9.1	概要	448
20.10	レイヤ 2 中継遮断機能のコンフィグレーション	449
20.10.1	コンフィグレーションコマンド一覧	449
20.10.2	レイヤ 2 中継遮断機能の設定	449
20.11	VLAN 拡張機能のオペレーション	450
20.11.1	運用コマンド一覧	450
20.11.2	VLAN 拡張機能の確認	450

21	スパンングツリー	451
21.1	スパンングツリーの概説	452
21.1.1	概要	452
21.1.2	スパンングツリーの種類	452
21.1.3	スパンングツリーと高速スパンングツリー	453
21.1.4	スパンングツリートポロジーの構成要素	454
21.1.5	スパンングツリーのトポロジー設計	456
21.1.6	STP 互換モード	457
21.1.7	スパンングツリー共通の注意事項	458
21.2	スパンングツリー動作モードのコンフィグレーション	459
21.2.1	コンフィグレーションコマンド一覧	459
21.2.2	動作モードの設定	459
21.3	PVST+ 解説	462
21.3.1	PVST+ によるロードバランシング	462
21.3.2	アクセスポートの PVST+	463
21.3.3	PVST+ 使用時の注意事項	464
21.4	PVST+ のコンフィグレーション	465
21.4.1	コンフィグレーションコマンド一覧	465
21.4.2	PVST+ の設定	465
21.4.3	PVST+ のトポロジー設定	466
21.4.4	PVST+ のパラメータ設定	467
21.5	PVST+ のオペレーション	470
21.5.1	運用コマンド一覧	470
21.5.2	PVST+ の状態の確認	470
21.6	シングルスパンングツリー解説	471
21.6.1	概要	471
21.6.2	PVST+ との併用	471
21.6.3	シングルスパンングツリー使用時の注意事項	472
21.7	シングルスパンングツリーのコンフィグレーション	473
21.7.1	コンフィグレーションコマンド一覧	473
21.7.2	シングルスパンングツリーの設定	473
21.7.3	シングルスパンングツリーのトポロジー設定	474
21.7.4	シングルスパンングツリーのパラメータ設定	475
21.8	シングルスパンングツリーのオペレーション	478
21.8.1	運用コマンド一覧	478
21.8.2	シングルスパンングツリーの状態の確認	478
21.9	マルチプルスパンングツリー解説	479
21.9.1	概要	479
21.9.2	マルチプルスパンングツリーのネットワーク設計	481
21.9.3	ほかのスパンングツリーとの互換性	483
21.9.4	マルチプルスパンングツリー使用時の注意事項	484

21.10	マルチブラスパニングツリーのコンフィグレーション	486
21.10.1	コンフィグレーションコマンド一覧	486
21.10.2	マルチブラスパニングツリーの設定	486
21.10.3	マルチブラスパニングツリーのトポロジー設定	487
21.10.4	マルチブラスパニングツリーのパラメータ設定	489
21.11	マルチブラスパニングツリーのオペレーション	492
21.11.1	運用コマンド一覧	492
21.11.2	マルチブラスパニングツリーの状態の確認	492
21.12	スパニングツリー共通機能解説	493
21.12.1	PortFast	493
21.12.2	BPDU フィルタ	493
21.12.3	ループガード	494
21.12.4	ルートガード	495
21.13	スパニングツリー共通機能のコンフィグレーション	497
21.13.1	コンフィグレーションコマンド一覧	497
21.13.2	PortFast の設定	497
21.13.3	BPDU フィルタの設定	498
21.13.4	ループガードの設定	499
21.13.5	ルートガードの設定	499
21.13.6	リンクタイプの設定	500
21.14	スパニングツリー共通機能のオペレーション	501
21.14.1	運用コマンド一覧	501
21.14.2	スパニングツリー共通機能の状態の確認	501

22	Ring Protocol の解説	505
22.1	Ring Protocol の概要	506
22.1.1	概要	506
22.1.2	特長	508
22.1.3	サポート仕様	508
22.2	Ring Protocol の基本原理	510
22.2.1	ネットワーク構成	510
22.2.2	制御 VLAN	512
22.2.3	障害監視方法	512
22.2.4	通信経路の切り替え	512
22.3	シングルリングの動作概要	515
22.3.1	リング正常時の動作	515
22.3.2	障害検出時の動作	515
22.3.3	復旧検出時の動作	517
22.3.4	経路切り戻し抑止および解除時の動作	518
22.4	マルチリングの動作概要	521
22.4.1	リング正常時の動作	521

22.4.2	共有リンク障害・復旧時の動作	523
22.4.3	共有リンク非監視リングでの共有リンク以外の障害・復旧時の動作	525
22.4.4	共有リンク監視リングでの共有リンク以外の障害・復旧時の動作	527
22.4.5	経路切り戻し抑止および解除時の動作	529
22.5	Ring Protocol のネットワーク設計	530
22.5.1	VLAN マッピングの使用方法	530
22.5.2	制御 VLAN の forwarding-delay-time の使用方法	530
22.5.3	プライマリポートの自動決定	531
22.5.4	同一装置内でのノード種別混在構成	532
22.5.5	共有ノードでのノード種別混在構成	532
22.5.6	リンクアグリゲーションを用いた場合の障害監視時間の設定	533
22.5.7	IEEE802.3ah/UDLD 機能との併用	534
22.5.8	リンクダウン検出タイマおよびリンクアップ検出タイマとの併用	534
22.5.9	Ring Protocol の禁止構成	535
22.5.10	リングポートにリンクアグリゲーションを使用する場合について	537
22.5.11	マスタノードの両リングポートが共有リンクとなる構成	538
22.6	Ring Protocol 使用時の注意事項	540

23 Ring Protocol の設定と運用 545

23.1	コンフィグレーション	546
23.1.1	コンフィグレーションコマンド一覧	546
23.1.2	Ring Protocol 設定の流れ	546
23.1.3	リング ID の設定	547
23.1.4	制御 VLAN の設定	547
23.1.5	VLAN マッピングの設定	548
23.1.6	VLAN グループの設定	549
23.1.7	モードとリングポートに関する設定 (シングルリングと共有リンクなしマルチリング構成)	549
23.1.8	モードとリングポートに関する設定 (共有リンクありマルチリング構成)	551
23.1.9	各種パラメータの設定	556
23.1.10	隣接リング用フラッシュ制御フレームの送信設定	558
23.2	オペレーション	559
23.2.1	運用コマンド一覧	559
23.2.2	Ring Protocol の状態確認	559

24 Ring Protocol とスパニングツリー /GSRP の併用 563

24.1	Ring Protocol とスパニングツリーとの併用	564
24.1.1	概要	564
24.1.2	動作仕様	565
24.1.3	各種スパニングツリーとの共存について	568
24.1.4	禁止構成	573
24.1.5	Ring Protocol とスパニングツリー併用時の注意事項	573

24.2	Ring Protocol と GSRP との併用	576
24.2.1	動作概要	576
24.2.2	併用条件	577
24.2.3	リングポートの扱い	577
24.2.4	Ring Protocol の制御 VLAN の扱い	577
24.2.5	GSRP ネットワーク切り替え時の MAC アドレステーブルクリア	578
24.2.6	Ring Protocol と GSRP 併用動作時の注意事項	578
24.2.7	単独動作時の動作概要（レイヤ 3 冗長切替機能の適用例）	580
24.3	仮想リンクのコンフィグレーション	583
24.3.1	コンフィグレーションコマンド一覧	583
24.3.2	仮想リンクの設定	583
24.3.3	Ring Protocol と PVST+ との併用設定	583
24.3.4	Ring Protocol とマルチブルスパニングツリーとの併用設定	584
24.3.5	Ring Protocol と GSRP との併用設定	584
24.4	仮想リンクのオペレーション	586
24.4.1	運用コマンド一覧	586
24.4.2	仮想リンクの状態の確認	586

25 ポリシーベーススイッチング 589

25.1	解説	590
25.1.1	ポリシーベーススイッチングの制御	590
25.1.2	ポリシーベーススイッチンググループ	591
25.1.3	ポリシーベーススイッチング対象フレーム	595
25.1.4	ポリシーベーススイッチングと他機能との共存	596
25.1.5	ポリシーベーススイッチングの注意事項	597
25.2	コンフィグレーション	599
25.2.1	コンフィグレーションコマンド一覧	599
25.2.2	ポリシーベーススイッチングの設定	599
25.3	オペレーション	602
25.3.1	運用コマンド一覧	602
25.3.2	ポリシーベーススイッチングの確認	602

26 IGMP snooping/MLD snooping の解説 605

26.1	IGMP snooping/MLD snooping の概要	606
26.1.1	マルチキャスト概要	606
26.1.2	IGMP snooping および MLD snooping 概要	607
26.2	IGMP snooping/MLD snooping サポート機能	608
26.3	IGMP snooping	609
26.3.1	MAC アドレスの学習	609
26.3.2	IPv4 マルチキャストパケットのレイヤ 2 中継	610
26.3.3	マルチキャストルータとの接続	610

26.3.4	IGMP クエリア機能	611
26.3.5	IGMP 即時離脱機能	612
26.3.6	同一 VLAN 上での IPv4 マルチキャストが動作する場合	612
26.4	MLD snooping	613
26.4.1	MAC アドレスの学習	613
26.4.2	IPv6 マルチキャストパケットのレイヤ 2 中継	614
26.4.3	マルチキャストルータとの接続	614
26.4.4	MLD クエリア機能	615
26.4.5	同一 VLAN 上での IPv6 マルチキャストが動作する場合	616
26.5	IGMP snooping/MLD snooping 使用時の注意事項	617

27

IGMP snooping/MLD snooping の設定と運用		621
27.1	IGMP snooping のコンフィグレーション	622
27.1.1	コンフィグレーションコマンド一覧	622
27.1.2	IGMP snooping の設定	622
27.1.3	IGMP クエリア機能の設定	622
27.1.4	マルチキャストルータポートの設定	622
27.2	IGMP snooping のオペレーション	624
27.2.1	運用コマンド一覧	624
27.2.2	IGMP snooping の確認	624
27.3	MLD snooping のコンフィグレーション	626
27.3.1	コンフィグレーションコマンド一覧	626
27.3.2	MLD snooping の設定	626
27.3.3	MLD クエリア機能の設定	626
27.3.4	マルチキャストルータポートの設定	626
27.4	MLD snooping のオペレーション	628
27.4.1	運用コマンド一覧	628
27.4.2	MLD snooping の確認	628

付録

付録 A 準拠規格		631
付録 A 準拠規格		632
付録 A.1	TELNET/FTP	632
付録 A.2	RADIUS/TACACS+	632
付録 A.3	NTP	632
付録 A.4	DNS	632
付録 A.5	イーサネット	633
付録 A.6	リンクアグリゲーション	633
付録 A.7	VLAN	633
付録 A.8	スパニングツリー	633
付録 A.9	IGMP snooping/MLD snooping	634
付録 B 謝辞 (Acknowledgments)		635

索引

651

1

本装置の概要

この章では、本装置の特長について説明します。

1.1 本装置の概要

1.2 本装置の特長

1.1 本装置の概要

企業内のネットワークは、IP 電話、インターネット接続、基幹業務などに使われ、PC は一人に 1 台が配布されるなど企業内の通信トラフィックは増大し続ける一方で。

また、ネットワークに流れるデータは企業の利益を左右するミッションクリティカルな重要データが流れています。ミッションクリティカルな市場は、ISP やネットワーク事業者が中心でしたが、今後は企業や公共の構内網に拡大されていく傾向にあります。

本装置は、ミッションクリティカルの分野に適用できる信頼性・可用性・拡張性の高い情報ネットワーク基盤を柔軟に構築するスイッチ製品です。

製品コンセプト

本装置は、弊社が目指す「ギャランティード・ネットワーク」を実現するために開発してきたキャリアアップグレードスイッチの技術を継承しつつ、企業ネットワークに必要とされる高密度収容能力とセキュリティ機能を強化した製品です。また、集中エンジン型アーキテクチャを採用したことによって、装置全体の消費電力を低減しています。

本装置は次の機能を実現します。

- 大規模ネットワークで使用される OSPF、BGP4 などのルーティングプロトコルや、先進の IPv6、マルチキャストなどを装備し、多様で柔軟なネットワークを実現
- さまざまなネットワーク冗長機能をサポートし、高信頼・高可用性なネットワークを実現
- リンクアグリゲーションや 10Gbit/s ポートを用意し、トラフィック増大に対して余裕を持ったネットワークを実現
- 企業内で扱われるさまざまなトラフィック（基幹業務データ、VoIP 電話データ、テレビ会議、ストリーミング配信、CAD データなど）を QoS 技術などで保護するギャランティ型ネットワークを実現
- 高機能フィルタ、ユーザ認証などのセキュリティ機能で安全なネットワークを実現
- フルワイヤレートでのパケットフォワーディングを実現
- パケットフォワーディング機能を共通部に配置させることによって装置のコンパクト化を実現
- 集中エンジン方式の採用によって装置全体の消費電力を低減
- ネットワークの設計・構築・運用のトータルコストを削減する OAN への対応
- 複数のサービスネットワークを一つの物理ネットワーク内に仮想的に収容し、統合化することによって、ネットワークの構築・運用コストを削減するネットワーク・パーティションを実現

1.2 本装置の特長

(1) 高速で多様な VLAN 機能をサポート

レイヤ 2 の VLAN 機能

- ポート VLAN, プロトコル VLAN, MAC VLAN 機能を実装
- 用途に応じた VLAN 構築が可能

スパニングツリープロトコル

- スパニングツリー (IEEE 802.1D), 高速スパニングツリー (IEEE 802.1w), PVST+, マルチブル
スパニングツリー (IEEE 802.1s) を実装

VLAN トンネリングによる L2-VPN の実現

ポリシーベーススイッチング

- MAC アドレステーブルによる経路情報に従わないで、ユーザが設定した送信先インタフェースに
レイヤ 2 中継するポリシーベーススイッチングをサポート
- 中継先の経路状態に合わせて最適な経路を選択可能

(2) 強固なセキュリティ機能

認証・検疫ソリューション

- レイヤ 2 認証機能 (IEEE802.1X, Web 認証, MAC 認証, 認証 VLAN) によって, エッジの物理構
成の自由度を保ちつつ, PC1 台 1 台を認証し, VLAN に加入させることが可能
- 認証サーバと検疫サーバとの組み合わせによって, 検疫チェックをパスした PC だけを業務 VLAN に
自動接続する検疫ソリューションを構築可能

高性能できめ細かなパケットフィルタが可能

- ハードウェアによる高性能なフィルタ処理
- L2/L3/L4 条件の指定が可能

RADIUS / TACACS+ による装置へのログイン・パスワード認証およびユーザごとに実行可能コマンド
を制限可能

不正な DHCP サーバ / 固定 IP アドレス端末の排除が可能

- DHCP snooping によって, 不正な DHCP サーバや固定 IP アドレス端末の排除が可能

(3) ハードウェアによる強力な QoS で通信品質を保証

ハードウェアによる高性能な QoS 処理

きめ細かなパラメータ (L2/L3/L4 条件) 指定が可能

多様な QoS 制御機能

L2-QoS (IEEE 802.1p, 優先制御, 廃棄制御など), IP-QoS (Diff-Serv, 優先制御, 廃棄制御など)

(4) 10G イーサネット収容能力

10G イーサネット ポートでフル帯域を使いきる転送処理を実現

(5) 実績あるルーティング機能

安定した高機能ルーティング

- 広域イーサネットサービスや IP-VPN サービスを利用した拠点間接続に, OSPF 機能や BGP 機能
を使用した信頼性の高いルーティングと, マルチパスを使った負荷分散を実現

1. 本装置の概要

- ルーティングソフトウェアには、実績ある弊社上位機種と同等のものを搭載

IPv6 マルチキャスト対応

- IPv4 と IPv6 で同一ピーク性能の実現
- 10 ギガビット・イーサネットでフルワイヤレートの IPv6 ルーティングを実現
- 豊富な IPv6 ルーティングプロトコル（スタティック，RIPng，OSPFv3，BGP4+，PIM-SM，PM-SSM）によって、多様で柔軟な IPv6 ネットワークを実現可能
- IPv4/IPv6 デュアルスタック，IPv6-only 環境に対応したネットワーク管理（SNMP over IPv6）など充実した機能

充実した IPv4 ルーティングプロトコル

- 実績ある豊富な IPv4 ルーティングプロトコルをサポート（スタティック，RIP，OSPF，BGP4，PIM-SM/SSM，PIM-DM）

ポリシーベースルーティング

- 中継先の経路状態に合わせて最適な経路を選択できるポリシーベースルーティングをサポート

(6) ネットワーク・パーティション対応

ネットワークの水平統合・垂直統合によるコスト低減

- 論理的に分割された複数のスイッチを一つのスイッチ内に仮想的に収容する VRF 機能によって、従来物理的に分かれていた複数のネットワークを一つの物理ネットワーク内に統合
- センターにレイヤ 3 装置を集約，各オフィスや拠点にはレイヤ 2 装置を配置することで，ネットワーク設計や運用管理の容易なネットワークを実現

(7) ミッションクリティカル対応のネットワークを実現する高信頼性

高い装置品質

- 厳選した部品と厳しい設計・検査基準による装置の高い信頼性
- キャリア / ISP で実績あるソフトウェアを継承した安定したルーティング処理

冗長構成による単体装置としての高信頼化

- 電源，CPU 部，パケットスイッチング部の装置内冗長を採用

多様な冗長ネットワーク構築

- 高速な経路切り替え
高速スパニングツリープロトコル（IEEE 802.1w，IEEE 802.1s），GSRP，Autonomous Extensible Ring Protocol¹（以降，Ring Protocol と呼びます。），リンクアグリゲーション（IEEE 802.3ad），ホットスタンバイ（VRRP），スタティックポーリング²，VRRP ポーリング² など
- ロードバランス
OSPF イコールコストマルチパスによる IP レベルの均等トラフィック分散

注 1

Ring Protocol の詳細については、「22 Ring Protocol の解説」を参照してください。

注 2

指定経路上の到達性をポーリングによって確認し，動的に VRRP やスタティックルーティングと連動して経路を切り替えるための監視機能。

(8) 優れたネットワーク管理，保守・運用

- IPv4/v6 デュアルスタックや IPv6 環境に対応したネットワーク管理（SNMP over IPv6）など充実した機能
- 基本的な MIB-II に加え，IPv6 MIB，RMON などの豊富な MIB をサポート

- オンライン保守
モジュール・電源・ファンの増設 / 交換をコマンドレスでできます。
- SD メモリカード採用
コンフィグレーションのバックアップや障害情報採取が容易に実行できます。
- 全イーサネットポート，コンソールポート，メモリカードスロットを前面に配置
- AX3600S/AX2400S シリーズと共通なコマンド体系で，操作性の統一による SE，保守員の教育時間削減
- システム操作パネルの採用により，コンソール端末を使用せずに各種情報を表示し，動作指示を行うことが可能
- イーサネット網の保守管理機能の CFM (Connectivity Fault Management) をサポート

(9) OAN (Open Autonomic Networking) への対応

IT システムとの連携およびネットワーク運用・管理の自動化によって，運用効率向上や TCO 削減を実現

- AX-Config-Master
各装置のコンフィグレーションが不要になる自動コンフィグレーション。
ネットワーク全体でのコンフィグレーションの整合性チェック。
装置のコンフィグレーションの収集および配信のセキュリティ確保。
- AX-ON-API
CLI，SNMP に代わる新しい装置制御手段。
XML(eXtensible Markup Language)，SOAP(Simple Object Access Protocol)，Netconf など，IT システムの標準技術をエンタプライズ向けネットワーク装置に導入。
VLAN，インタフェース，リンクアグリゲーションなどの設定が可能。

注

詳細は，マニュアル「OAN ユーザーズガイド AX-Config-Master 編」を参照してください。

(10) 省電力対応

集中エンジン方式の採用によって，装置全体の消費電力を低減

装置の電力状態として通常か省電力かを設定によって選択可能

アイドル消費電力を低減

通信を継続したまま装置を省電力状態へ移行可能 **【AX6700S】【AX6600S】**

設定したスケジュールに従って装置を省電力状態へ自動で移行 **【AX6700S】【AX6600S】**

コールドスタンバイ方式によって待機系スイッチング機構の消費電力を削減 **【AX6700S】【AX6600S】**

2

装置構成

この章では，本装置の外観や構成要素などについて説明します。

2.1 本装置のモデル

2.2 装置の構成要素

2.1 本装置のモデル

AX6700S シリーズには、次に示すモデルがあります。

- AX6708S

AX6600S シリーズには、次に示すモデルがあります。

- AX6604S
- AX6608S

AX6300S シリーズには、次に示すモデルがあります。

- AX6304S
- AX6308S

本装置はイーサネットポートを最大 192 ポート装備し (AX6708S, AX6608S, および AX6308S モデル), レイヤ 2 スイッチングとレイヤ 3 ルーティング機能を備えた高機能ギガビット・イーサネットスイッチです。

AX6708S は基本制御部 (BCU), スイッチング部 (BSU), 電源 (PS) を冗長化し, NIF を 8 スロット収容可能なモデルです。

AX6604S は共通部 (CSU), 電源 (PS) を冗長化し, NIF を 4 スロット収容可能なモデルです。

AX6608S は共通部 (CSU), 電源 (PS) を冗長化し, NIF を 8 スロット収容可能なモデルです。

AX6304S は共通部 (MSU), 電源 (PS) を冗長化し, NIF を 4 スロット収容可能なモデルです。

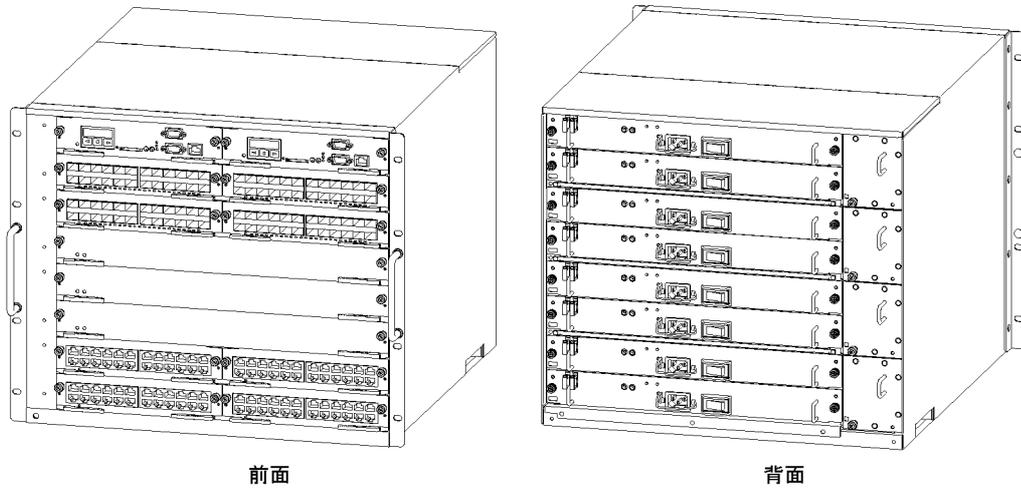
AX6308S は共通部 (MSU), 電源 (PS) を冗長化し, NIF を 8 スロット収容可能なモデルです。

2.1.1 装置の外観

各モデルの装置外観図を次に示します。

(1) AX6700S シリーズ

図 2-1 AX6708S モデル (AC 電源)



前面

背面

・モジュール実装位置

BCU1	BCU2
NIF1	NIF2
NIF3	NIF4
BSU1	
BSU2	
BSU3	
NIF5	NIF6
NIF7	NIF8

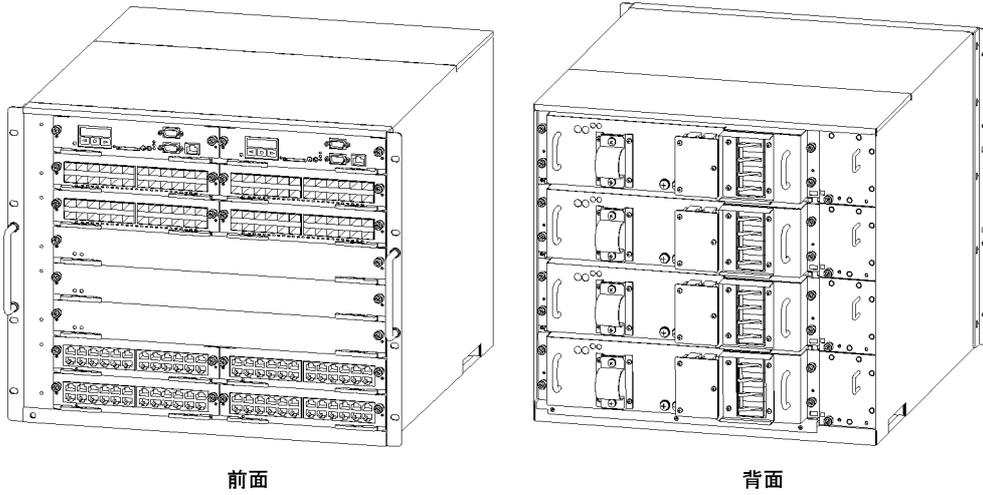
前面

PS1	FAN1
PS2	
PS3	FAN2
PS4	
PS5	FAN3
PS6	
PS7	FAN4
PS8	

背面

2. 装置構成

図 2-2 AX6708S モデル (DC 電源)



・モジュール実装位置

BCU1	BCU2
NIF1	NIF2
NIF3	NIF4
BSU1	
BSU2	
BSU3	
NIF5	NIF6
NIF7	NIF8

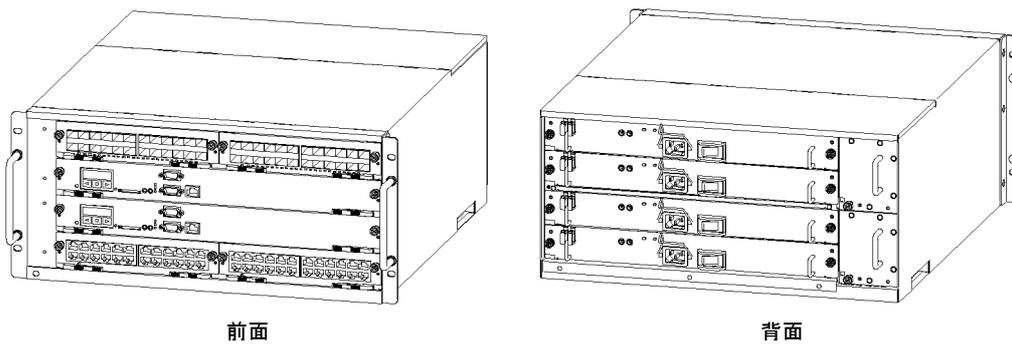
前面

PS1	FAN1
PS2	FAN2
PS3	FAN3
PS4	FAN4

背面

(2) AX6600S シリーズ

図 2-3 AX6604S モデル (AC 電源)



・モジュール実装位置

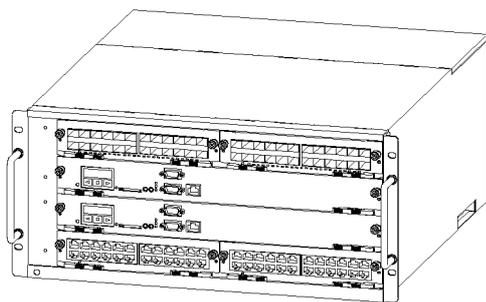
NIF1	NIF2
CSU1	
CSU2	
NIF3	NIF4

前面

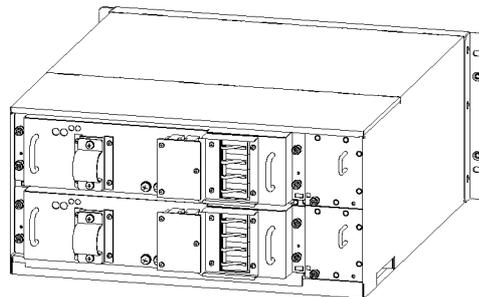
PS1	FAN1
PS2	
PS3	FAN2
PS4	

背面

図 2-4 AX6604S モデル (DC 電源)



前面



背面

・モジュール実装位置

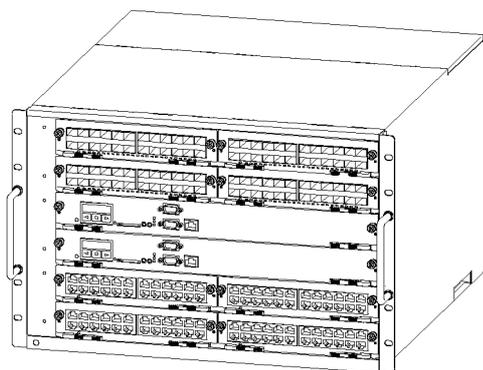
	NIF1	NIF2
	CSU1	
	CSU2	
	NIF3	NIF4

前面

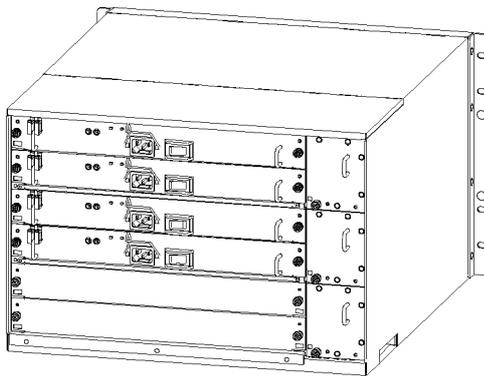
PS1	FAN1
PS2	FAN2

背面

図 2-5 AX6608S モデル (AC 電源)



前面



背面

・モジュール実装位置

	NIF1	NIF2
	NIF3	NIF4
	CSU1	
	CSU2	
	NIF5	NIF6
	NIF7	NIF8

前面

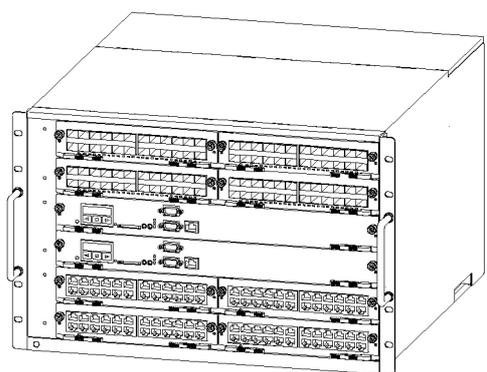
PS1	FAN1
PS2	
PS3	FAN2
PS4	
PS5※	FAN3
PS6※	

背面

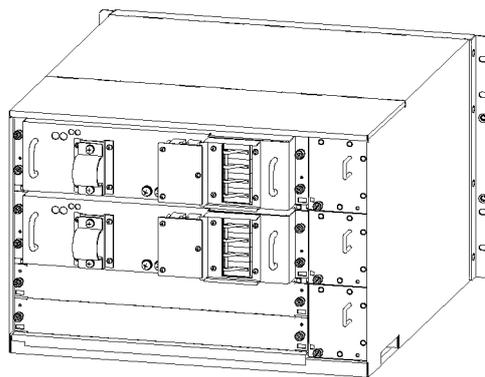
注※ PS5, PS6は将来の拡張用スロット

2. 装置構成

図 2-6 AX6608S モデル (DC 電源)



前面



背面

・モジュール実装位置

	NIF1	NIF2
	NIF3	NIF4
	CSU1	
	CSU2	
	NIF5	NIF6
	NIF7	NIF8

前面

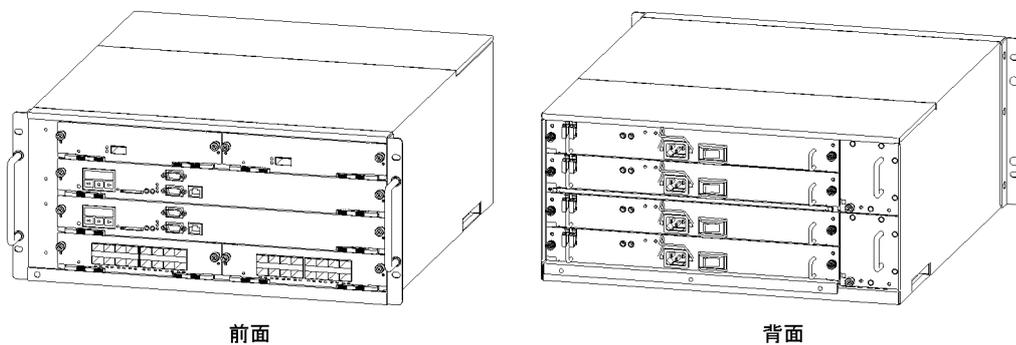
PS1	FAN1
PS2	FAN2
PS3※	FAN3

背面

注※ PS3は将来の拡張用スロット

(3) AX6300S シリーズ

図 2-7 AX6304S モデル (AC 電源)



前面

背面

・モジュール実装位置

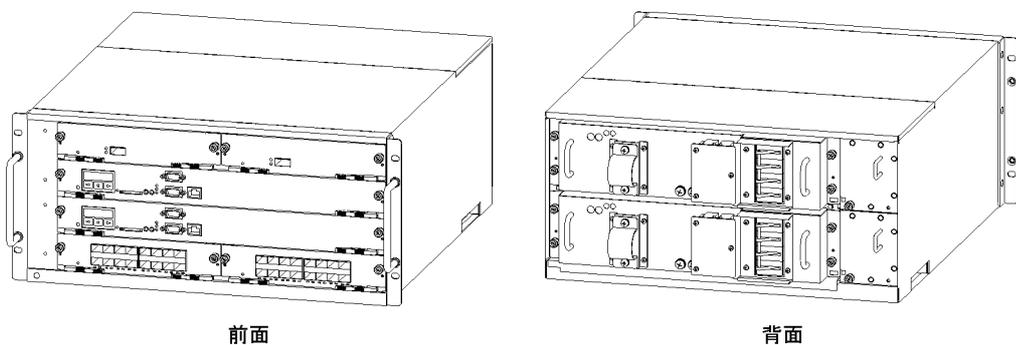
	NIF1	NIF2
	MSU1	
	MSU2	
	NIF3	NIF4

前面

	PS1	FAN1
	PS2	
	PS3	FAN2
	PS4	

背面

図 2-8 AX6304S モデル (DC 電源)



前面

背面

・モジュール実装位置

	NIF1	NIF2
	MSU1	
	MSU2	
	NIF3	NIF4

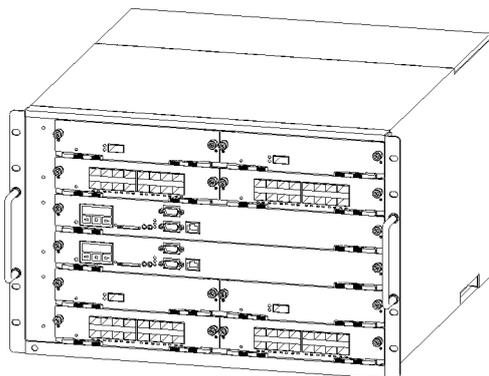
前面

	PS1	FAN1
	PS2	FAN2

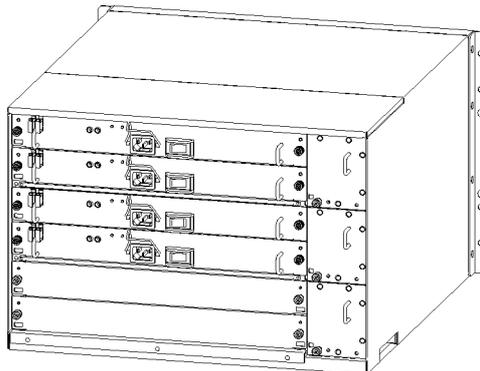
背面

2. 装置構成

図 2-9 AX6308S モデル (AC 電源)



前面



背面

・モジュール実装位置

	NIF1	NIF2
	NIF3	NIF4
	MSU1	
	MSU2	
	NIF5	NIF6
	NIF7	NIF8

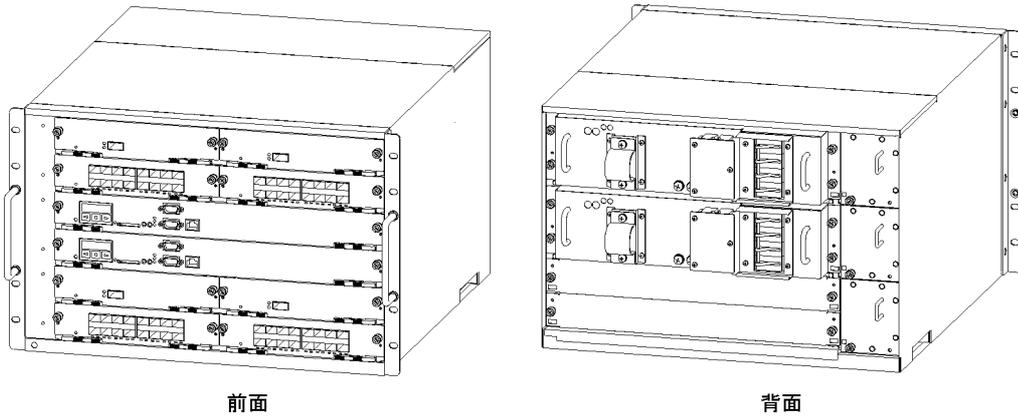
前面

PS1	FAN1
PS2	
PS3	FAN2
PS4	
PS5※	FAN3
PS6※	

背面

注※ PS5, PS6は将来の拡張用スロット

図 2-10 AX6308S モデル (DC 電源)



・ モジュール実装位置

	NIF1	NIF2
	NIF3	NIF4
	MSU1	
	MSU2	
	NIF5	NIF6
	NIF7	NIF8

前面

PS1	FAN1
PS2	FAN2
PS3※	FAN3

背面

注※ PS3は将来の拡張用スロット

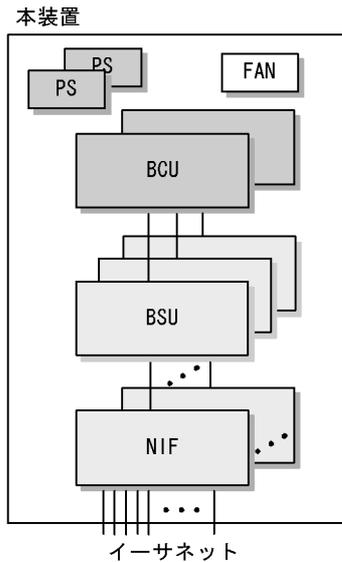
2.2 装置の構成要素

2.2.1 AX6700S ハードウェアの構成【AX6700S】

本装置は、PS、FAN、BCU、BSU および NIF で構成されています。

ハードウェアの構成を次の図に示します。

図 2-11 ハードウェアの構成



(凡例) BCU : Basic Control Unit
 BSU : Basic Switching Unit
 NIF : Network Interface
 PS : Power Supply
 FAN : Fan Unit

(1) PS (電源機構)

PS は外部供給電源から本装置内で使用する直流電源を生成し、冗長化構成をとれます。冗長化構成時は本装置の運用中に PS が故障しても装置を停止させることなく運用できます。

電源の冗長構成の詳細は、「コンフィグレーションガイド Vol.2 16. 電源機構 (PS) の冗長化」を参照してください。

表 2-1 AX6700S シリーズ用 PS 機器一覧

略称	概略仕様
PS-A11	AC 電源 AC100V/200V 系
PS-D11	DC 電源 DC-48V 系

(2) FAN

FAN は装置内部を冷却するファンユニットです。

表 2-2 AX6700S シリーズ用ファンユニット一覧

略称	概略仕様
FAN-11	AX6708S 用ファンユニット

(3) BCU (基本制御機構)

BCU は CPU を搭載し、装置全体の管理、スパンニングツリープロトコル処理、ルーティングプロトコル処理および BSU、NIF の制御を行います。BCU-S1 は 2048MB のメモリと、256MB の内蔵フラッシュメモリを搭載しています。BCU-S11 は 2048MB のメモリと、1024MB の大容量内蔵フラッシュメモリを搭載しています。また、それぞれ MC スロットを一つ搭載しています。そのほかに、RS232C ポート（コンソールポート、AUX ポート）と 10BASE-T/100BASE-TX ポート（マネージメントポート）があります。筐体に BCU を 2 枚実装することで、装置単体として冗長化構成が取れます。冗長化構成によって、本装置の運用中に BCU が故障しても装置を停止させることなく運用できます。

表 2-3 BCU 機器一覧

略称	概略仕様
BCU-S1	AX6708S 用基本制御部
BCU-S11	AX6708S 用基本制御部 (大容量内蔵フラッシュメモリ搭載版)

(4) BSU (基本スイッチング機構)

BSU は、搭載された二つの転送エンジンによって、MAC アドレステーブルやルーティングテーブルに基づきパケットを NIF にスイッチングします。筐体に BSU を最大 3 枚実装することで、装置単体として冗長化構成がとれます。冗長化構成によって、本装置の運用中に BSU が故障しても装置を停止させることなく運用できます。また、3 枚すべての BSU を運用系として使用すればスイッチング容量を拡張できます。なお、1 枚の BSU を運用系とすることを BSU シングルアクト運転、2 枚の BSU を運用系とすることを BSU ダブルアクト運転、3 枚の BSU を運用系とすることを BSU トリプルアクト運転とも呼びます。

表 2-4 BSU 機器一覧

略称	概略仕様
BSU-LA	AX6708S 用基本スイッチング部テーブルサイズ標準版
BSU-LB	AX6708S 用基本スイッチング部テーブルサイズ拡張版

(5) NIF (ネットワークインタフェース機構)

NIF は各種メディア対応のインタフェース制御部で、複数の種類があり、物理レイヤの処理を行います。

表 2-5 AX6700S シリーズ用 NIF 機器一覧

略称	概略仕様
NK1G-24T	10/100/1000Mbit/s イーサネット 24 回線
NK1G-24S	1Gbit/s イーサネット 24 回線 SFP
NK1GS-8M	10/100/1000Mbit/s イーサネットまたは 1Gbit/s イーサネット SFP 選択型 4 回線 階層化シェーバ機能付き + 1Gbit/s イーサネット SFP 4 回線 階層化シェーバ機能付き

2. 装置構成

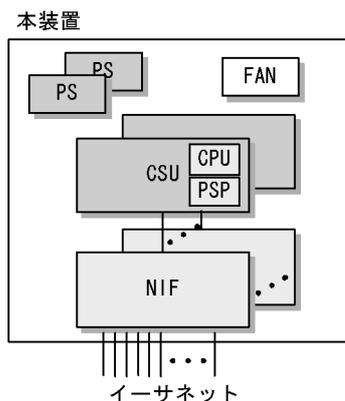
略称	概略仕様
NK10G-4RX	10Gbit/s イーサネット 4 回線 XFP
NK10G-8RX	10Gbit/s イーサネット 8 回線 XFP

2.2.2 AX6600S ハードウェアの構成【AX6600S】

本装置は、PS、FAN、CSU、およびNIFで構成されています。

ハードウェアの構成を次の図に示します。

図 2-12 ハードウェアの構成



(凡例) CSU : Control and Switching Unit
 CPU : Central Processing Unit
 PSP : Packet Switching Processor
 NIF : Network Interface
 PS : Power Supply
 FAN : Fan Unit

(1) PS (電源機構)

PS は外部供給電源から本装置内で使用する直流電源を生成し、冗長化構成をとれます。冗長化構成時は、本装置の運用中に PS が故障しても装置を停止させることなく運用できます。

電源の冗長構成の詳細は、「コンフィグレーションガイド Vol.2 16. 電源機構 (PS) の冗長化」を参照してください。

表 2-6 AX6600S シリーズ用 PS 機器一覧

略称	概略仕様
PS-A11	AC 電源 AC100V/200V 系
PS-D11	DC 電源 DC-48V 系

(2) FAN

FAN は装置内部を冷却するファンユニットです。

表 2-7 AX6600S シリーズ用ファンユニット一覧

略称	概略仕様
FAN-11	AX6604S, AX6608S 用ファンユニット

(3) CSU (制御スイッチング機構)

CSU は CPU 部と PSP 部から成ります。CPU 部は CPU を搭載し、装置全体の制御、スパンニングツリープロトコル処理、ルーティングプロトコル処理および NIF の制御を行います。PSP 部は搭載された一つの転送エンジンによって、MAC アドレステーブルやルーティングテーブルに基づきパケットを NIF にスイッチングします。CSU-1A は 1024MB のメモリ、CSU-1B は 2048MB のメモリと、それぞれ 1024MB の大容量内蔵フラッシュメモリを搭載しています。また、MC スロットを一つ搭載しています。そのほかに、RS232C ポート (コンソールポート、AUX ポート) と 10BASE-T/100BASE-TX ポート (マネージメントポート) があります。筐体に CSU を 2 枚実装することで、装置単体として冗長化構成が取れます。冗長化構成によって、本装置の運用中に CSU が故障しても装置を停止させることなく運用できます。また、冗長化構成時、待機系 CSU の PSP 部を運用系で使用すればスイッチング容量を拡張できます。なお、運用系 CSU の PSP 部だけを使用することを PSP シングルアクト運転、また待機系 CSU の PSP 部を運用系で使用することを PSP ダブルアクト運転とも呼びます。

表 2-8 CSU 機器一覧

略称	概略仕様
CSU-1A	AX6604S/AX6608S 用制御スイッチング部 テーブルサイズ標準版 (大容量内蔵フラッシュメモリ搭載版)
CSU-1B	AX6604S/AX6608S 用制御スイッチング部 テーブルサイズ拡張版 (大容量内蔵フラッシュメモリ搭載版)

(4) NIF (ネットワークインタフェース機構)

NIF は各種メディア対応のインタフェース制御部で、複数の種類があり、物理レイヤの処理を行います。

表 2-9 AX6600S シリーズ用 NIF 機器一覧

略称	概略仕様
NK1G-24T	10/100/1000Mbit/s イーサネット 24 回線
NK1G-24S	1Gbit/s イーサネット 24 回線 SFP
NK1GS-8M	10/100/1000Mbit/s イーサネットまたは 1Gbit/s イーサネット SFP 選択型 4 回線 階層化シェーパ機能付き + 1Gbit/s イーサネット SFP 4 回線 階層化シェーパ機能付き
NK10G-4RX	10Gbit/s イーサネット 4 回線 XFP
NK10G-8RX	10Gbit/s イーサネット 8 回線 XFP

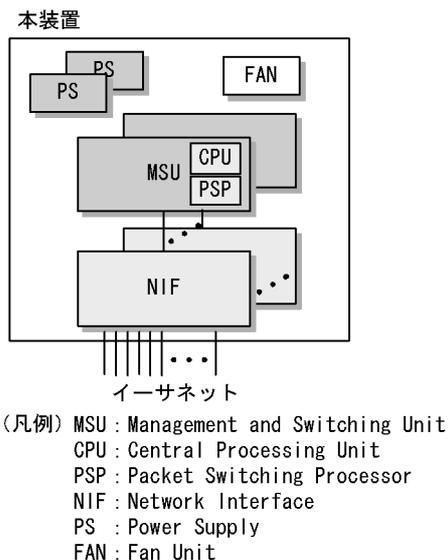
2.2.3 AX6300S ハードウェアの構成【AX6300S】

本装置は、PS、FAN、MSU、および NIF で構成されています。

ハードウェアの構成を次の図に示します。

2. 装置構成

図 2-13 ハードウェアの構成



(1) PS (電源機構)

PS は外部供給電源から本装置内で使用する直流電源を生成し、冗長化構成をとれます。冗長化構成時は、本装置の運用中に PS が故障しても装置を停止させることなく運用できます。

電源の冗長構成の詳細は、「コンフィグレーションガイド Vol.2 16. 電源機構 (PS) の冗長化」を参照してください。

表 2-10 AX6300S シリーズ用 PS 機器一覧

略称	概略仕様
PS-A11	AC 電源 AC100V/200V 系
PS-D11	DC 電源 DC-48V 系

(2) FAN

FAN は装置内部を冷却するファンユニットです。

表 2-11 AX6300S シリーズ用ファンユニット一覧

略称	概略仕様
FAN-11	AX6304S, AX6308S 用ファンユニット

(3) MSU (管理スイッチング機構)

MSU は CPU 部と PSP 部から成ります。CPU 部は CPU を搭載し、装置全体の制御、スパニングツリープロトコル処理、ルーティングプロトコル処理および NIF の制御を行います。PSP 部は搭載された一つの転送エンジンによって、MAC アドレステーブルやルーティングテーブルに基づきパケットを NIF にスイッチングします。MSU-1A および MSU-1A1 は 1024MB のメモリ、MSU-1B および MSU-1B1 は 2048MB のメモリを搭載しています。MSU-1A および MSU-1B は 256MB の内蔵フラッシュメモリ、

MSU-1A1 および MSU-1B1 は 1024MB の大容量内蔵フラッシュメモリを搭載しています。また、MC スロットを一つ搭載しています。そのほかに、RS232C ポート（コンソールポート、AUX ポート）と 10BASE-T/100BASE-TX ポート（マネージメントポート）があります。筐体に MSU を 2 枚実装することで、装置単体として冗長化構成が取れます。冗長化構成によって、本装置の運用中に MSU が故障しても装置を停止させることなく運用できます。

表 2-12 MSU 機器一覧

略称	概略仕様
MSU-1A	AX6304S/AX6308S 用管理スイッチング部テーブルサイズ標準版
MSU-1A1	AX6304S/AX6308S 用管理スイッチング部テーブルサイズ標準版 (大容量内蔵フラッシュメモリ搭載版)
MSU-1B	AX6304S/AX6308S 用管理スイッチング部テーブルサイズ拡張版
MSU-1B1	AX6304S/AX6308S 用管理スイッチング部テーブルサイズ拡張版 (大容量内蔵フラッシュメモリ搭載版)

(4) NIF（ネットワークインタフェース機構）

NIF は各種メディア対応のインタフェース制御部で、複数の種類があり、物理レイヤの処理を行います。

表 2-13 AX6300S シリーズ用 NIF 機器一覧

略称	概略仕様
NH1G-16S	1Gbit/s イーサネット 16 回線 SFP
NH1G-24T	10/100/1000Mbit/s イーサネット 24 回線
NH1G-24S	1Gbit/s イーサネット 24 回線 SFP
NH1G-48T	10/100/1000Mbit/s イーサネット 48 回線
NH1GS-6M	10/100/1000Mbit/s イーサネット 4 回線 階層化シェーバ機能付き + 1Gbit/s イーサネット SFP 2 回線 階層化シェーバ機能付き
NH10G-1RX	10Gbit/s イーサネット 1 回線 XFP
NH10G-4RX	10Gbit/s イーサネット 4 回線 XFP
NH10G-8RX	10Gbit/s イーサネット 8 回線 XFP

2.2.4 ソフトウェア

本装置のソフトウェアは基本ソフトとオプションライセンスから構成されています。BGP、BGP+、認証 VLAN、および VRF を使う場合はオプションライセンスが必要です。

本装置のソフトウェア一覧を次の表に示します。

表 2-14 ソフトウェア一覧（基本ソフト）

略称	機能概要
OS-SE	VLAN、スパニングツリー、GSRP、Ring Protocol、IP パケット中継、スタティックルーティング、RIP、RIPng、OSPF、OSPFv3、PIM-SM、PIM-SSM、SSH、https ほか

注

SSH は別冊マニュアル「Secure Shell(SSH) ソフトウェアマニュアル」を参照してください。

2. 装置構成

表 2-15 ソフトウェア一覧（オプションライセンス）

略称	機能概要
OP-BGP	BGP4 , BGP4+
OP-DH6R	IPv6 DHCP リレー
OP-MBSE	IPv4 マルチキャスト BSR 拡張機能（ブートストラップメッセージ受信抑止機能）
OP-NPAR	VRF
OP-VAA	認証 VLAN

注

AX6600S シリーズの場合，CSU-1A では未サポートです。

AX6300S シリーズの場合，MSU-1A および MSU-1A1 では未サポートです。

3

収容条件

この章では、収容条件について説明します。

3.1 AX6700S の搭載条件【AX6700S】

3.2 AX6700S の収容条件【AX6700S】

3.3 AX6600S の搭載条件【AX6600S】

3.4 AX6600S の収容条件【AX6600S】

3.5 AX6300S の搭載条件【AX6300S】

3.6 AX6300S の収容条件【AX6300S】

3.1 AX6700S の搭載条件【AX6700S】

3.1.1 最大収容ポート数

各モデルの最大収容可能ポート数を次の表に示します。

表 3-1 最大収容可能ポート数

モデル名	イーサネット		
	10GBASE-R	1000BASE-X	10/100/1000BASE-T
AX6708S	64	192	192

3.1.2 最大搭載数

(1) 機器搭載数

各モデルへの冗長化構成を含めた機器最大搭載数を次の表に示します。

表 3-2 機器最大搭載数

機器	AX6708S
BCU	2 (冗長化構成時)
BSU	3 (冗長化構成時)
NIF	8
PS (AC 電源)	8 (冗長化構成時)
PS (DC 電源)	4 (冗長化構成時)

(2) 電源機構の搭載数

電源機構の最大搭載数は「表 3-2 機器最大搭載数」を参照してください。また、電源機構搭載条件については、マニュアル「コンフィグレーションガイド Vol.2 16. 電源機構 (PS) の冗長化」を参照してください。

(3) NIF 最大搭載数

NIF の種別によって最大搭載数が異なります。NIF 種別ごとの最大搭載数を次に示します。

表 3-3 NIF 種別ごとの最大搭載数

NIF 種別	サイズ	AX6708S
		装置当たり
NK1G-24T	シングル	8
NK1G-24S	シングル	8
NK1GS-8M	シングル	8
NK10G-4RX	シングル	8
NK10G-8RX	シングル	8

3.2 AX6700S の収容条件【AX6700S】

本節で使用する VLAN ポート数とは各 VLAN に所属するポート数の延べ数の合計です。

例えば、VLAN 1 ~ 100 を設定し、それぞれの VLAN に 2 回線が所属している場合、VLAN ポート数は $100 \times 2 = 200$ となります。

3.2.1 テーブルエントリ数

(1) 概要

本項で使用するテーブルエントリ数とは、経路数やフィルタ・QoS のエントリ数を意味します。

本装置では、ネットワーク構成に合わせ、適切なテーブルエントリ数の配分パターンを選ぶことができます。配分パターンはコンフィグレーションコマンドによって変更できます。

エントリの配分パターンは経路系、フロー系をそれぞれ用意しています。経路系テーブルエントリ、フロー系テーブルエントリ定義を次の表に示します。

表 3-4 経路系テーブルエントリ、フロー系テーブルエントリ内容定義

項目	内容
経路系エントリ	IPv4 ユニキャスト経路 IPv4 マルチキャスト経路 IPv6 ユニキャスト経路 IPv6 マルチキャスト経路 MAC アドレスエントリ ARP NDP
フロー系エントリ	フィルタエントリ (ポリシーベースルーティングおよびポリシーベーススイッチングを含む) QoS エントリ

(2) テーブル容量種別

テーブル容量に対応した名称を次の表に示します。

表 3-5 経路系テーブル容量名称

テーブル容量	対応 BSU
standard	BSU-LA
extended	BSU-LB

表 3-6 フロー系テーブル容量名称

テーブル容量	対応 BSU
standard ¹	BSU-LA
standard-advance ²	
extended ³	BSU-LB
extended-advance ²	

3. 収容条件

- 注 1 BSU-LA でのデフォルトのテーブル容量です。
 注 2 フロー検出拡張モードを使用する場合に指定します。
 注 3 BSU-LB でのデフォルトのテーブル容量です。

(3) 配分パターン

配分パターンを次の表に示します。

表 3-7 経路系テーブルエントリ配分パターン

パターン名称	意味
default	全エントリ混在
ipv4-uni	IPv4 ユニキャスト主体, マルチキャスト, IPv6 無し
ipv4-ipv6-uni	IPv4 ユニキャスト / IPv6 ユニキャスト主体, マルチキャスト無し
vlan	L2 主体, マルチキャスト無し

注 デフォルトのパターン

表 3-8 standard および standard-advance のフロー系テーブルエントリ配分パターン

パターン名称	意味
default	フィルタ, QoS 均等

注 デフォルトのパターン

表 3-9 extended および extended-advance のフロー系テーブルエントリ配分パターン

パターン名称	意味
default	フィルタ, QoS 均等
filter-only	フィルタ専用
qos-only	QoS 専用
filter	フィルタ主体
qos	QoS 主体

注 デフォルトのパターン

経路系テーブルエントリ数とフロー系テーブルエントリ数を次の表に示します。

VRF 機能使用時の最大エントリ数は, 全 VRF のエントリ数の合計です。

本項表中の「k」の単位は 1024 です。例えば, 24k は $24 \times 1024 = 24576$ であることを表しています。

表 3-10 standard の経路系テーブルエントリ数

パターン名	IPv4 ユニ キャスト 経路 ¹	IPv4 マル チキャス ト経路	IPv6 ユニ キャスト 経路 ²	IPv6 マル チキャス ト経路	MAC ア ドレス	ARP	NDP
default	32768 (32k)	4000	16384 (16k)	1000	24576 (24k)	12288 (12k)	12288 (12k)
ipv4-uni	65536 (64k)	-	-	-	24576 (24k)	12288 (12k)	-

パターン名	IPv4 ユニキャスト経路 ¹	IPv4 マルチキャスト経路	IPv6 ユニキャスト経路 ²	IPv6 マルチキャスト経路	MAC アドレス	ARP	NDP
ipv4-ipv6-uni	32768 (32k)	-	32768 (32k)	-	24576 (24k)	12288 (12k)	12288 (12k)
vlan	8192 (8k)	-	8192 (8k)	-	49152 (48k)	8192 (8k)	8192 (8k)

(凡例) - : 該当なし

注 注 は次表を参照してください

表 3-11 extended の経路系テーブルエントリ数

パターン名	IPv4 ユニキャスト経路 ¹	IPv4 マルチキャスト経路	IPv6 ユニキャスト経路 ²	IPv6 マルチキャスト経路	MAC アドレス	ARP	NDP
default	65536 (64k)	8000	32768 (32k)	8000	65536 (64k)	24576 (24k)	24576 (24k)
ipv4-uni	212992 (208k)	-	-	-	24576 (24k)	24576 (24k)	-
ipv4-ipv6-uni	106496 (104k)	-	106496 (104k)	-	24576 (24k)	24576 (24k)	24576 (24k)
vlan	8192 (8k)	-	8192 (8k)	-	122880 (120k)	8192 (8k)	8192 (8k)

(凡例) - : 該当なし

注 1 IPv4 ユニキャスト経路数には次の情報が含まれます。

- RIP, OSPF, BGP4, スタティックを合わせたアクティブ経路
- 他 VRF (グローバルネットワークを含む) からインポートされた, アクティブ状態のエクストラネット経路
- IPv4 インタフェース数 × 4 : 直結経路のホスト経路, サブネット経路, ブロードキャスト経路 (ホストアドレスの全情報が 0 と 1 の 2 経路)
- ARP エントリ数
- ループバックインタフェースを指定の場合は 1 経路が加算されます。
VRF でループバックインタフェースを使用する場合は, VRF ごとに 1 経路が加算されます。
- RIP バージョン 2 を使用する場合は 1 経路が加算されます。
VRF で RIP バージョン 2 を使用する場合は, VRF ごとに 1 経路が加算されます。
- OSPF を使用する場合は 2 経路が加算されます。
VRF で OSPF を使用する場合は, VRF ごとに 2 経路が加算されます。
- vrrp でアクセプトモードを設定して, マスタ状態になっている場合は 1 経路が加算されます。
- ここに示した以外に 4 経路を装置固定情報として使用します。
VRF を使用する場合は, VRF ごとに 1 経路を装置固定情報として使用します。

注 2 IPv6 ユニキャスト経路数には次の情報が含まれます。

- RIPng, OSPFv3, BGP4+, スタティックを合わせたアクティブ経路数
- IPv6 インタフェース数 × 5 : 直結経路のグローバルアドレス, リンクローカルアドレスそれぞれのホスト経路およびサブネット経路, 直結経路のリンクローカルマルチキャストアドレス
- NDP エントリ数
- ループバックインタフェースを指定の場合は 1 経路が加算されます。
VRF でループバックインタフェースを使用する場合は, VRF ごとに 1 経路が加算されます。
- vrrp でアクセプトモードを設定して, マスタ状態になっている場合は 1 経路が加算されます。
- ここに示した以外に 1 経路を装置固定情報として使用します。
VRF を使用する場合は, VRF ごとに 1 経路を装置固定情報として使用します。

表 3-12 standard のフロー系エントリ数

パターン名	フィルタ	QoS
default (フィルタ, QoS 均等)	4000	4000

表 3-13 standard-advance のフロー系エントリ数

パターン名	フィルタ	QoS
default (フィルタ, QoS 均等)	2000 (300)	2000

注

括弧内の値は DHCP snooping が有効な場合のフィルタエントリ数です。

表 3-14 extended および extended-advance のフロー系エントリ数

パターン名	フィルタ	QoS
default (フィルタ, QoS 均等)	16000 (6000)	16000
filter-only (フィルタ専用)	32000 (22000)	-
qos-only (QoS 専用)	-	32000
filter (フィルタ主体)	24000 (14000)	8000
qos (QoS 主体)	8000 (4000)	24000

(凡例) - : 該当なし

注

括弧内の値は, extended-advance で DHCP snooping が有効な場合のフィルタエントリ数です。

3.2.2 BSU 経路配分パターン

BSU 経路配分パターンに応じた収容可能な IP ユニキャスト, IP マルチキャストの経路エントリ数, MAC アドレスエントリ数, および IP インタフェース数を次の表に示します。表中の「k」の単位は 1024 です。

(1) BSU-LA (standard) の経路配分パターン

表 3-15 BSU-LA 経路配分パターンと収容経路エントリ数 (その1)

経路配分パターン	IPv4 ユニキャスト					IPv4 マルチキャスト		IPv4 インタフェース数	MAC アドレスエントリ数
	最大経路エントリ数		プロトコル別最大経路エントリ数			PIM-SM/SSM PIM-DM			
	アクティブ/非アクティブの合計	アクティブ	RIP+OS PF	BGP	スタティック	(S,G) エントリ数	インタフェース数		
default	131072 (128k)	32768 (32k)	10000	131072 (128k)	4096	1	1	4096	24576 (24k)
ipv4-uni	262144 (256k)	65536 (64k)	10000	262144 (256k)	4096	-	-	4096	24576 (24k)
ipv4-ipv6-uni	131072 (128k)	32768 (32k)	10000	131072 (128k)	4096	-	-	4096	24576 (24k)
vlan	32768 (32k)	8192	10000	32768 (32k)	4096	-	-	4096	49152 (48k)

(凡例) - : 該当なし

注 注 は次表を参照してください。

表 3-16 BSU-LA 経路配分パターンと収容経路エントリ数 (その2)

経路配分パターン	IPv6 ユニキャスト					IPv6 マルチキャスト		IPv6 インタフェース数
	最大経路エントリ数		プロトコル別最大経路エントリ数			PIM-SM/SSM		
	アクティブ/非アクティブの合計	アクティブ	RIPng+OS PFv3	BGP4+	スタティック	(S,G) エントリ数	インタフェース数	
default	65536 (64k)	16384 (16k)	10000	65536 (64k)	4096	2	2	4096
ipv4-uni	-	-	-	-	-	-	-	-
ipv4-ipv6-uni	131072 (128k)	32768 (32k)	10000	131072 (128k)	4096	-	-	4096
vlan	32768 (32k)	8192	10000	32768 (32k)	4096	-	-	4096

(凡例) - : 該当なし

注 1,2

(S,G) エントリ数とインタフェース数の組み合わせは、次のどれかの組み合わせとなります。IPv4 と IPv6 のマルチキャストに関しては、IPv4 マルチキャストと IPv6 マルチキャストを混在で使用する場合、(S,G) エントリ数とインタフェース数は、IPv4 と IPv6 の合計値が次の表のエントリ数以内となるようにしてください。

注 1 の場合の組み合わせを次の表に示します。

3. 収容条件

表 3-17 IPv4 マルチキャスト単独使用の場合の (S,G) エントリ数とインタフェース数の組み合わせ

(S,G) エントリ数	インタフェース数
4000	31
2000	63
1000	127

注 2 の場合の組み合わせを次の表に示します。

表 3-18 IPv6 マルチキャスト単独使用, または IPv4/IPv6 マルチキャスト混在使用の場合の (S,G) エントリ数とインタフェース数の組み合わせ

(S,G) エントリ数	インタフェース数
1000	31
500	63
250	127

(2) BSU-LB (extended) の経路配分パターン

表 3-19 BSU-LB 経路配分パターンと収容経路エントリ数 (その1)

経路配分パターン	IPv4 ユニキャスト					IPv4 マルチキャスト		IPv4 インタフェース数	MAC アドレスエントリ数
	最大経路エントリ数		プロトコル別最大経路エントリ数			PIM-SM/SSM PIM-DM			
	アクティブ/非アクティブの合計	アクティブ	RIP+OS PF	BGP	スタティック	(S,G) エントリ数	インタフェース数		
default	262144 (256k)	65536 (64k)	10000	262144 (256k)	4096			4096	65536 (64k)
ipv4-uni	851968 (832k)	212992 (208k)	10000	851968 (832k)	4096	-	-	4096	24576 (24k)
ipv4-ipv6-uni	425984 (416k)	106496 (104k)	10000	425984 (416k)	4096	-	-	4096	24576 (24k)
vlan	32768 (32k)	8192	10000	32768 (32k)	4096	-	-	4096	122880 (120k)

(凡例) - : 該当なし

注 は次表を参照してください。

表 3-20 BSU-LB 経路配分パターンと収容経路エントリ数 (その 2)

経路配分パターン	IPv6 ユニキャスト					IPv6 マルチキャスト		IPv6 インタフェース数
	最大経路エントリ数		プロトコル別最大経路エントリ数			PIM-SM/SSM		
	アクティブ/非アクティブの合計	アクティブ	RIPng+OS PFv3	BGP4+	スタティック	(S,G) エントリ数	インタフェース数	
default	131072 (128k)	32768 (32k)	10000	131072 (128k)	4096			4096
ipv4-uni	-	-	-	-	-	-	-	-
ipv4-ipv6-uni	425984 (416k)	106496 (104k)	10000	425984 (416k)	4096	-	-	4096
vlan	32768 (32k)	8192	10000	32768 (32k)	4096	-	-	4096

(凡例) - : 該当なし

注

(S,G) エントリ数とインタフェース数の組み合わせは、次のどれかの組み合わせとなります。IPv4 と IPv6 のマルチキャストに関しては、IPv4 マルチキャストと IPv6 マルチキャストを混在で使用する場合、(S,G) エントリ数とインタフェース数は、IPv4 と IPv6 の合計値が次の表のエントリ数以内となるようにしてください。

組み合わせを次の表に示します。

表 3-21 (S,G) エントリ数とインタフェース数の組み合わせ

(S,G) エントリ数	インタフェース数
8000	31
4000	63
2000	127
1000	255

3.2.3 リンクアグリゲーション

コンフィグレーションによって設定できるリンクアグリゲーションの収容条件を次の表に示します。

表 3-22 リンクアグリゲーションの収容条件

モデル	装置当たりの最大チャンネルグループ数	チャンネルグループ当たりの最大ポート数
AX6700S シリーズ共通	63	16

3.2.4 レイヤ 2 スイッチ

(1) MAC アドレステーブル

L2 スイッチ機能では、複数の機能で MAC アドレステーブルを使用しています。例えば、MAC アドレスの学習機能では、接続された端末の MAC アドレスをダイナミックに学習して MAC アドレステーブルへ

3. 収容条件

登録します。

MAC アドレステーブルの最大エン트리数については、次の表を参照してください。

- 表 3-15 BSU-LA 経路配分パターンと収容経路エン트리数 (その 1)
- 表 3-19 BSU-LB 経路配分パターンと収容経路エン트리数 (その 1)

MAC アドレステーブルを使用する機能と、その機能による MAC アドレステーブルの使用量を次の表に示します。

表 3-23 MAC アドレステーブルを使用する機能

機能名	使用量
MAC アドレス学習抑止機能	設定した VLAN ごとに 1 エン트리
スタティック MAC アドレス登録機能	登録した MAC アドレスごとに 1 エン트리
スタティック ARP/NDP 登録機能	登録した ARP/NDP エン트리ごとに 1 エン트리
MAC アドレス学習機能 ARP/NDP 学習機能	学習したアドレスごとに 1 エン트리
Ring Protocol 機能	[マスタノード時] リング ID ごとに 2 エン트리 [共有ノード時] リング ID ごとに 1 エン트리
IGMP/MLD snooping 機能 (学習)	学習した MAC アドレスごとに 1 エン트리
IGMP snooping 機能	設定した VLAN ごとに 2 エン트리
MLD snooping 機能	設定した VLAN ごとに 8 エン트리
IEEE802.1X	認証済み端末ごとに 1 エン트리
Web 認証機能	認証済み端末ごとに 1 エン트리
MAC 認証機能	認証済み端末ごとに 1 エン트리

注 MAC アドレスと対応する ARP/NDP を学習した場合は合わせて 1 エン트리となります

MAC アドレステーブルのエン트리数が最大エン트리数に達した場合、新たなエントリを登録できなくなるため、上記の収容条件内で運用してください。

運用中は、運用コマンド show system で MAC アドレステーブルの使用状況を確認できます。

(2) MAC アドレス学習

MAC アドレス学習数の収容条件は、「表 3-15 BSU-LA 経路配分パターンと収容経路エン트리数 (その 1)」、「表 3-19 BSU-LB 経路配分パターンと収容経路エン트리数 (その 1)」で示した MAC アドレステーブルの最大エン트리数となります。「表 3-23 MAC アドレステーブルを使用する機能」に示したほかの機能を使用した場合は、ほかの機能で使用した分だけ MAC アドレス学習数の最大数が減少します。

(3) スタティック MAC アドレス登録

スタティック MAC アドレス登録機能の収容条件を次の表に示します。

表 3-24 スタティック MAC アドレスの登録数

モデル	装置当たり
AX6700S シリーズ共通	1000

MAC アドレステーブルに空きがない場合は、スタティック MAC アドレス登録機能の最大数まで登録できないことがあります。

(4) VLAN

コンフィグレーションによって設定できる VLAN の数を次の表に示します。

表 3-25 VLAN 数

モデル	装置当たり VLAN	ポート当たり VLAN	VLAN ポート数
AX6700S シリーズ共通	4095	4095	100000

VLAN ポート数が収容条件を超えた場合、CPU の利用率が高くなり、コンフィグレーションコマンドや運用コマンドのレスポンスが遅くなったり、実行できなくなったりすることがあります。

(a) プロトコル VLAN

プロトコル VLAN では、イーサネットフレーム内の Ethernet-Type, LLC SAP, および SNAP type フィールドの値を基にプロトコルの識別を行います。コンフィグレーションによって設定できるプロトコル VLAN の収容条件を次の表に示します。

表 3-26 プロトコル VLAN のプロトコルの種類数

モデル	装置当たり	ポート当たり
AX6700S シリーズ共通	16	16

表 3-27 プロトコル VLAN 数

モデル	装置当たり
AX6700S シリーズ共通	96

表 3-28 プロトコルポート数

モデル	装置当たり
AX6700S シリーズ共通	96

(b) MAC VLAN

MAC VLAN の収容条件を次の表に示します。

表 3-29 MAC VLAN の登録 MAC アドレス数

モデル	コンフィグレーションによる最大登録 MAC アドレス数	L2 認証機能による最大登録 MAC アドレス数	コンフィグレーションによる登録数と L2 認証機能による登録数の同時登録最大 MAC アドレス数
AX6700S シリーズ共通	4096	4096	4096

(c) Tag 変換

コンフィグレーションによって設定できる Tag 変換情報エントリ数を次の表に示します。

3. 収容条件

表 3-30 Tag 変換情報エントリ数

モデル	装置当たり
AX6700S シリーズ共通	4096

注 Tag 変換情報エントリをポートチャンネルインタフェースに設定する場合、Tag 変換情報エントリ数は該当チャンネルグループのポート数で計算します。

(d) VLAN トンネリング

コンフィグレーションによって設定できる VLAN トンネリングの数を次の表に示します。

表 3-31 VLAN トンネリングの数

モデル	装置当たり
AX6700S シリーズ共通	4095

(e) VLAN 識別テーブル

VLAN 識別テーブルは、フレーム受信時に VLAN を識別するためのテーブルです。プロトコル VLAN、MAC VLAN、および Tag 変換では、VLAN 識別テーブルを使用します。これらの機能を同時に使用する場合は、次の収容条件となります。

ポートごとのプロトコル数 + 登録 MAC アドレス数 + Tag 変換情報エントリ数 4096

ポートごとのプロトコル数

装置内の各プロトコルポートに設定するプロトコル数の合計。リンクアグリゲーションを使用する場合は、ポートチャンネルインタフェースに設定するプロトコル数で計算するため、チャンネルグループの収容ポート数は無関係です。

登録 MAC アドレス数

コンフィグレーションによる MAC アドレス登録数と L2 認証機能による MAC アドレス登録数の合計。

Tag 変換情報エントリ数

コンフィグレーションで設定する Tag 変換情報エントリの数。リンクアグリゲーションを使用する場合は、ポートチャンネルインタフェースに設定する Tag 変換情報エントリ数で計算するため、チャンネルグループの収容ポート数は無関係です。

(5) スパニングツリー

スパニングツリーの収容条件を種類ごとに次の表に示します。

なお、スパニングツリーの VLAN ポート数は、スパニングツリーが動作する VLAN に所属するポート数の延べ数です。チャンネルグループの場合、チャンネルグループ当たりの物理ポート数を数えます。ただし、次の VLAN やポートは、VLAN ポート数に含めません。

- コンフィグレーションコマンド state で suspend パラメータが設定されている VLAN
- VLAN トンネリングを設定しているポート
- BPDU ガード機能を設定しているが、BPDU フィルタ機能を設定していないポート
- PortFast 機能と BPDU フィルタ機能を設定しているアクセスポート

表 3-32 PVST+ の収容条件

モデル	Ring Protocol 共存有無	対象 VLAN 数	VLAN ポート数
AX6700S シリーズ共通	共存なし	250	1000
	共存あり	128	900

表 3-33 シングルスパニングツリーの収容条件

モデル	Ring Protocol 共存有無	対象 VLAN 数	VLAN ポート数	
AX6700S シリーズ 共通	共存なし	4095	シングルだけ	10000
			PVST+ 併用時	5000
	共存あり		シングルだけ	9000
			PVST+ 併用時	4500

注

PVST+ 併用時、PVST+ の VLAN ポート数とシングルスパニングツリーの VLAN ポート数との合計が最大値となります。

表 3-34 マルチプルスパニングツリーの収容条件

モデル	Ring Protocol 共存有無	MST インスタンス数	MST インスタンスごとの対象 VLAN 数	VLAN ポート数
AX6700S シリーズ 共通	共存なし	16	200	10000
	共存あり	16	200	9000

注

MST インスタンス 0 は除きます。MST インスタンス 0 の対象 VLAN 数は 4095 となります。なお、運用中は運用コマンド `show spanning-tree port-count` で対象 VLAN 数と VLAN ポート数を確認できます。

(6) Ring Protocol

(a) Ring Protocol

Ring Protocol の収容条件を次の表に示します。

表 3-35 Ring Protocol 収容条件

項目	リング当たり	装置当たり
リング数	-	16 ¹
VLAN マッピング数	-	128 ²
VLAN グループ数	2	32
VLAN グループの VLAN 数	4094 ³	4094 ³
リングポート数 ⁴	2	32

(凡例) - : 該当なし

注 1

リングネットワークの構成によっては、最大数の 16 個まで設定できない場合があります。

3. 収容条件

注 2

Ring Protocol と VRF 機能を併用する（コンフィギュレーションコマンド `vrf mode` の `axrp-enable` パラメータ、または `axrp-enable-ipv4-ipv6` パラメータを設定している）場合、装置当たりの VLAN マッピング数は 64 となります。

【OP-NPAR】

注 3

制御 VLAN 用に VLAN を一つ消費するため、VLAN グループに使用できる VLAN 最大数は 4094 となります。

注 4

チャンネルグループの場合は、チャンネルグループ単位で 1 ポートと数えます。

(b) 仮想リンク

仮想リンクの収容条件を次の表に示します。

表 3-36 仮想リンクの収容条件

項目	最大数
装置当たりの仮想リンク ID 数	1
仮想リンク当たりの VLAN 数	1
拠点当たりのリングノード数	2
ネットワーク全体での仮想リンクの拠点数	250

(c) Ring Protocol とスパニングツリーまたは GSRP 併用時の物理ポート数

Ring Protocol とスパニングツリー、または Ring Protocol と GSRP の併用時の収容条件を次の表に示します。なお、リングポートを収容している NIF が対象となります。

表 3-37 Ring Protocol とスパニングツリーまたは GSRP 併用時の収容条件

NIF 略称	使用可能な物理ポート数 ^{1 2}
NK1G-24T	すべてのポート
NK1G-24S	すべてのポート
NK1GS-8M	すべてのポート
NK10G-4RX	BSU シングルアクト運転の場合、2 ポートまで
	BSU ダブルアクト運転または BSU トリプルアクト運転の場合、すべてのポート ³
NK10G-8RX	BSU シングルアクト運転の場合、2 ポートまで
	BSU ダブルアクト運転の場合、4 ポートまで ⁴
	BSU トリプルアクト運転の場合、6 ポートまで ^{5 6}

注 1

収容条件を超える物理ポートを使用した場合、常時または一時的にリングポートに高負荷のトラフィックが流れると、仮想リンクの制御フレームが廃棄されるおそれがあります。

注 2

収容条件は、対象 NIF でリングポートを収容した場合に、その NIF で使用可能な物理ポート数の最大となります。

注 3

BSU の冗長性を確保したい場合は、BSU トリプルアクト運転で使用してください。

注 4

ポート番号が 1 ~ 4, 3 ~ 6, または 5 ~ 8 のどれかの範囲で使用してください。

注 5

ポート番号が 1 ~ 6, または 3 ~ 8 のどちらかの範囲で使用してください。

注 6

BSU の冗長性を確保したい場合は, 使用する物理ポートを 4 ポートまでで運用してください。ただし, ポート番号が 1 ~ 4, 3 ~ 6, または 5 ~ 8 のどれかの範囲で使用してください。

(7) ポリシーベーススイッチング

ポリシーベーススイッチングでは, フィルタのフロー検出を使用して, ポリシーベーススイッチングの対象にするフローを検出します。なお, ポリシーベーススイッチングは, フロー系エントリの配分パターンが qos-only 以外, かつ経路系テーブル容量が extended のときだけ使用できます。

装置当たりのポリシーベーススイッチンググループのエントリ数を次の表に示します。

表 3-38 装置当たりのポリシーベーススイッチンググループのエントリ数

項目	エントリ数
アクセスリストエントリ数	「表 3-41 フィルタ・QoS エントリ数」を参照 ¹
ポリシーベーススイッチングリスト数	1000 ²
ポリシーベーススイッチングリスト情報内に設定できる経路数	8

注 1

エントリ数の算出方法は, 「3.2.5 フィルタ・QoS」と同じです。

注 2

1 ポリシーベーススイッチングリスト情報を 1 リストとして登録します。このため, 複数のアクセスリストで同一のポリシーベーススイッチングリスト情報を設定した場合, 使用するリスト数は 1 リストと計算します。

(8) IGMP snooping / MLD snooping

IGMP snooping の収容条件を次の表に示します。IGMP snooping で学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。登録可能なマルチキャスト MAC アドレス数を次の表に示します。

表 3-39 IGMP snooping 収容条件

モデル	マルチキャスト同時使用	最大数		
		設定 VLAN 数 ¹	収容ポート数 ²	登録エントリ数
AX6700S シリーズ共通 (BSU-LA 搭載時)		256	16	1000
			32	500
			64	250
	x	256	16	2000
			32	1000
			64	500
AX6700S シリーズ共通 (BSU-LB 搭載時)		256	32	2000
			64	1000
	x	256	32	4000
			64	2000

3. 収容条件

モデル	マルチキャスト同時使用	最大数		
		設定 VLAN 数 ¹	収容ポート数 ²	登録エントリ数
			128	1000

(凡例)

：IPv4 マルチキャスト，または IPv6 マルチキャストを同時使用する

×：IPv4 マルチキャスト，または IPv6 マルチキャストを同時使用しない

注 1

snooping が動作するポート数 (snooping 設定 VLAN に収容されるポートの総和) は装置全体で最大 4096 です。例えば，おのおの 10 ポート収容している 128 個の VLAN で snooping を動作させる場合，snooping 動作ポート数は 1280 となります。

注 2

リンクアグリゲーションポートは 1 ポートと数えます。

MLD snooping の収容条件を次の表に示します。MLD snooping で学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。登録可能なマルチキャスト MAC アドレス数を次の表に示します。

表 3-40 MLD snooping 収容条件

モデル	マルチキャスト同時使用	最大数		
		設定 VLAN 数 ¹	収容ポート数 ²	登録エントリ数
AX6700S シリーズ共通 (BSU-LA 搭載時)		256	16	1000
			32	500
			64	250
	×	256	16	2000
			32	1000
			64	500
			128	250
	AX6700S シリーズ共通 (BSU-LB 搭載時)		256	32
64				1000
×		256	32	4000
			64	2000
			128	1000

(凡例)

：IPv4 マルチキャスト，または IPv6 マルチキャストを同時使用する

×：IPv4 マルチキャスト，または IPv6 マルチキャストを同時使用しない

注 1

snooping が動作するポート数 (snooping 設定 VLAN に収容されるポートの総和) は装置全体で最大 4096 です。例えば，おのおの 10 ポート収容している 128 個の VLAN で snooping を動作させる場合，snooping 動作ポート数は 1280 となります。

注 2

リンクアグリゲーションポートは 1 ポートと数えます。

3.2.5 フィルタ・QoS

(1) フィルタ・QoS

フィルタおよび QoS の収容条件を示します。ここでのエン트리数とは、コンフィグレーション (access-list, qos-flow-list) で設定したリストを装置内部で使用する形式 (エン트리) に変換したあとの数です。

(a) フィルタ・QoS エン트리数

フィルタ, および QoS の最大エン트리数を次の表に示します。

表 3-41 フィルタ・QoS エン트리数

モデル	フィルタの最大エン트리数		QoS の最大エン트리数	
	入出力インタフェース当たり	装置当たり	入出力インタフェース当たり	装置当たり
AX6700S シリーズ共通 (BSU-LA 搭載時)	4000	4000	4000	4000
AX6700S シリーズ共通 (BSU-LB 搭載時)	32000	32000	32000	32000

フロー制御はフローコンフィグレーションで設定しますが、リストに設定するフロー検出条件パラメータによって使用するエン트리数が異なります。複数エントリを使用するフロー検出条件のパラメータを次の表に示します。

表 3-42 複数エントリを使用するフロー検出条件

複数エントリを使用する フロー検出条件のパラメータ	使用エントリ数算出例
宛先 IPv4 アドレス, 送信元 IPv4 アドレス, 宛先 IPv6 アドレスを範囲指定	指定された IP アドレスが幾つのサブネットに区切られるかによってエン트리数が決定。 例えば, 宛先 IPv4 アドレスに 192.168.0.1 - 192.168.0.4 と指定した場合, 192.168.0.1/32, 192.168.0.2/31, 192.168.0.4/32 の三つのサブネットに区切られるため, 3 エントリとなります。
宛先ポート番号を範囲指定, 送信元ポート番号を範囲指定	指定された値が最大 16 ビットのマスクで区切ったときに幾つに分けられるかによってエン트리数が決定。 例えば, 宛先ポート番号に 135 - 140 と指定した場合, <ul style="list-style-type: none"> 135/16 = 0000 0000 1000 0111 (2 進表記) 136/14 = 0000 0000 1000 10xx (2 進表記) 140/16 = 0000 0000 1000 1100 (2 進表記) の三つの領域に区切られるため, 3 エントリとなります。
VLAN ID を複数指定	指定された VLAN ID 複数指定の中で, 次に示す総和をエン트리数とします。 <ul style="list-style-type: none"> 各単数指定部分: 1 エントリ。 各範囲指定部分: 前項と同様の方式で最大 12 ビットとして算出したエン트리数。 例えば, 1, 4-7, 16-18 と指定した場合, 1:1/12 = 0000 0000 0001(2 進表記) 4-7:4/10 = 0000 0000 01xx(2 進表記) 16-18:16/11 = 0000 0001 000x(2 進表記) 18/12 = 0000 0001 0010(2 進表記) のエントリとなります。

3. 収容条件

複数エントリを使用する フロー検出条件のパラメータ	使用エントリ数算出例
TCP セッション維持 (ack フラグが ON, または rst フラグが ON のパケット検出)	2 エントリ使用します。

1 リストに上記のフロー検出条件を複数指定した場合、おのこのフロー検出条件で使用するエントリ数を掛け合わせた値が、1 リストで使用するエントリ数となります。

1 リストに上記のフロー検出条件を一つ指定した場合は、指定したフロー検出条件にて使用するエントリ数が 1 リストで使用するエントリ数となります。

二つ以上指定した場合は、おのこのフロー検出条件で使用するエントリ数を掛け合わせた値が、1 リストで使用するエントリ数となります。

上記のフロー検出条件を指定していない場合は、1 リストで使用するエントリ数は 1 エントリとなります。

(b) 帯域監視機能でのエントリ数

帯域監視機能の収容条件エントリ数は、ストームコントロール機能と併用です。帯域監視モードと動作概要を次の表に示します。

表 3-43 帯域監視モードと動作概要

帯域監視モード	モード指定時の帯域監視機能の動作概要
upc-in-and-storm-control	<ul style="list-style-type: none"> 帯域監視は受信側にだけ設定可 一つのフローエントリごとに、最大帯域制御または最低帯域監視のどちらかを設定可 ストームコントロール機能が使用可能
upc-in-in	<ul style="list-style-type: none"> 帯域監視は受信側にだけ設定可 一つのフローエントリで最大帯域制御と最低帯域監視の同時監視可 ストームコントロール機能は使用不可

各モードの帯域監視機能の収容条件を次の表に示します。

表 3-44 装置当たりの帯域機能エントリ数

帯域監視モード	帯域監視機能でのエントリ数	ストームコントロール機能
upc-in-and-storm-control	744	
upc-in-in	1000	×

(凡例) : 有効 × : 無効

1 リストに指定した帯域監視機能の内容によって、1 リストで使用するエントリ数が異なります。その内容を次の表に示します。

表 3-45 1 リストで使用する帯域監視機能のエントリ数

1 リストに指定した帯域監視機能	使用エントリ数
最大帯域制御だけ	1
最低帯域監視だけ	1
最大帯域制御と最低帯域監視の両方を指定	2

(c) 階層化シェーパ

階層化シェーパのユーザ数の収容条件を次の表に示します。

表 3-46 階層化シェーパの最大ユーザ数

モデル	回線当たりの最大ユーザ数	装置当たりの最大ユーザ数
AX6700S シリーズ共通	1024	32768

注 デフォルトユーザを含む数です。

(2) アクセスリストロギング

アクセスリストロギングの収容条件を示します。

アクセスリストロギングの最大アクセスリストログ情報数を次の表に示します。

表 3-47 最大アクセスリストログ情報数

モデル	最大アクセスリストログ情報数
AX6700S シリーズ共通 (BSU-LA 搭載時)	2000
AX6700S シリーズ共通 (BSU-LB 搭載時)	4000

3.2.6 レイヤ 2 認証

(1) レイヤ 2 認証

レイヤ 2 認証共通の収容条件を次の表に示します。

表 3-48 認証専用 IPv4 アクセスリストに設定できるフィルタ条件数

モデル	認証専用 IPv4 アクセスリストに設定できるフィルタ条件数
AX6700S シリーズ共通	10

(2) IEEE802.1X

IEEE802.1X の収容条件を次に示します。

本装置の IEEE802.1X では、三つの認証モードをサポートしています。

- ポート単位認証
- VLAN 単位認証 (静的)
- VLAN 単位認証 (動的)

VLAN 単位認証を使用する場合の、IEEE802.1X を設定可能な装置当たりの総ポート数を次の表に示します。

表 3-49 IEEE802.1X を設定可能な装置当たりの総ポート数

モデル	IEEE802.1X を設定可能な装置当たりの総ポート数
AX6700S シリーズ共通	1024

3. 収容条件

注

IEEE802.1X を設定可能な装置当たりの総ポート数とは、VLAN 単位認証を設定した VLAN での VLAN ポート数の総和の最大値を指します。VLAN 内にチャンネルグループが含まれている場合は、チャンネルグループを構成する物理ポート数に関係なく、チャンネルグループを 1 ポートとして計算します。また、1 ポートに VLAN が Tag で多重化されている場合も個別に数えます。例えば、一つのポートに Tag で多重化された 10 個の VLAN が設定されていた場合、その 10 個の VLAN で VLAN 単位認証を動作させると、総ポート数は 10 ポートになります。

各認証モードでの単位当たりの最大認証端末数を次の表に示します。

表 3-50 各認証モードでの単位当たりの最大認証端末数

モデル	認証モード		
	ポート単位認証	VLAN 単位認証 (静的)	VLAN 単位認証 (動的)
AX6700S シリーズ共通	256 / ポート	256 / VLAN	4096 / 装置

注

IEEE802.1X (VLAN 単位認証 (動的)), Web 認証 (ダイナミック VLAN モード) および MAC 認証 (ダイナミック VLAN モード) を同時に動作させた場合は、それぞれの認証端末数の合計で装置当たり 4096 までとなります。

本装置の最大認証端末数を次の表に示します。

表 3-51 本装置の最大認証端末数

モデル	3 モード合計での最大認証端末数
AX6700S シリーズ共通	4096 / 装置

注

IEEE802.1X (ポート単位認証および VLAN 単位認証 (静的)), Web 認証 (固定 VLAN モード) および MAC 認証 (固定 VLAN モード) を同時に動作させた場合は、それぞれの認証端末数の合計で装置当たり 4096 までとなります。

(3) Web 認証

Web 認証の収容条件を次の表に示します。

表 3-52 Web 認証 (固定 VLAN モード) の最大認証端末数

モデル	装置当たりの最大認証端末数
AX6700S シリーズ共通	4096

注

Web 認証 (固定 VLAN モード), IEEE802.1X (ポート単位認証および VLAN 単位認証 (静的)) および MAC 認証 (固定 VLAN モード) を同時に動作させた場合は、それぞれの認証端末数の合計で装置当たり 4096 までとなります。

表 3-53 Web 認証 (ダイナミック VLAN モード) の最大認証端末数

モデル	装置当たりの最大認証端末数
AX6700S シリーズ共通	4096

注

Web 認証 (ダイナミック VLAN モード), IEEE802.1X (VLAN 単位認証 (動的)) および MAC 認証 (ダイナミック VLAN モード) を同時に動作させた場合は, それぞれの認証端末数の合計で装置当たり 4096 までとなります。

表 3-54 Web 認証 (レガシーモード) の最大認証端末数

モデル	装置当たりの最大認証端末数
AX6700S シリーズ共通	4096

注

Web 認証 (レガシーモード) および IEEE802.1X (VLAN 単位認証 (動的)) を同時に動作させた場合は, それぞれの認証端末数の合計で装置当たり 4096 までとなります。

表 3-55 Web 認証の装置当たりの内蔵 Web 認証 DB 登録ユーザ数

モデル	装置当たりの内蔵 Web 認証 DB 登録ユーザ数
AX6700S シリーズ共通	300

注

内蔵 Web 認証 DB に登録したユーザ ID を複数の端末で使用すると, 最大認証端末数まで端末を認証できます。ただし, 認証対象となるユーザ ID の数が内蔵 Web 認証 DB の最大登録数より多い場合は, RADIUS サーバを用いた RADIUS 認証方式を使用してください。

表 3-56 Web 認証の画面入れ替えで指定できる認証画面ファイル合計サイズ

モデル	装置当たりの指定できる認証画面ファイルの合計サイズ
AX6700S シリーズ共通	1024K バイト

表 3-57 Web 認証の画面入れ替えで指定できる認証画面ファイル数

モデル	装置当たりの指定できる認証画面ファイル数
AX6700S シリーズ共通	100

(4) MAC 認証

MAC 認証の収容条件を次の表に示します。

表 3-58 MAC 認証 (固定 VLAN モード) の最大認証端末数

モデル	装置当たりの最大認証端末数
AX6700S シリーズ共通	4096

注

MAC 認証 (固定 VLAN モード), IEEE802.1X (ポート単位認証および VLAN 単位認証 (静的)) および Web 認証 (固定 VLAN モード) を同時に動作させた場合は, それぞれの認証端末数の合計で 4096 までとなります。

表 3-59 MAC 認証 (ダイナミック VLAN モード) の最大認証端末数

モデル	装置当たりの最大認証端末数
AX6700S シリーズ共通	4096

3. 収容条件

注

MAC 認証 (ダイナミック VLAN モード), IEEE802.1X (VLAN 単位認証 (動的)) および Web 認証 (ダイナミック VLAN モード) を同時に動作させた場合は, それぞれの認証端末数の合計で 4096 までとなります。

表 3-60 MAC 認証の装置当たりの内蔵 MAC 認証 DB 登録ユーザ数

モデル	装置当たりの内蔵 MAC 認証 DB 登録ユーザ数
AX6700S シリーズ共通	1024

注

内蔵 MAC 認証 DB を使用した場合で VLAN ID をチェックしないときは, 認証対象となる MAC アドレスと VLAN ID 数 (Tag 使用時の VLAN ID 数も含む) の組み合わせ合計数が最大認証端末数に到達するまで端末を認証できます。ただし, 認証する端末 (MAC アドレス) と VLAN ID の組み合わせ合計数が内蔵 MAC 認証 DB の最大登録数より多い場合は, RADIUS サーバを用いた RADIUS 認証方式を使用してください。

(5) 認証 VLAN

認証 VLAN の収容条件を次の表に示します。

表 3-61 最大認証端末数

モデル	装置当たりの最大認証端末数
AX6700S シリーズ共通	4096

表 3-62 接続可能な認証サーバ数

モデル	装置当たりの接続可能な認証サーバ数
AX6700S シリーズ共通	10

表 3-63 設定可能な認証済み VLAN 数

モデル	装置当たりの設定可能な認証済み VLAN 数
AX6700S シリーズ共通	4094

3.2.7 DHCP snooping

DHCP snooping の収容条件を次の表に示します。

表 3-64 DHCP snooping の最大エントリ数

フロー系テーブル容量名称	フロー系テーブルエントリ配分パターン	バインディングデータベースエントリ数 ¹		端末フィルタエントリ数 ²
		ダイナミック / スタティックの合計	スタティック	
standard	default (フィルタ, QoS 均等)	-	-	-
standard-advance	default (フィルタ, QoS 均等)	1100	256	1100
extended	default (フィルタ, QoS 均等)	-	-	-
	filter-only (フィルタ専用)	-	-	-

フロー系テーブル容量名称	フロー系テーブルエントリ配分パターン	バインディングデータベースエントリ数 ¹		端末フィルタエントリ数 ²
		ダイナミック / スタティックの合計	スタティック	
	qos-only (QoS 専用)	-	-	-
	filter (フィルタ主体)	-	-	-
	qos (QoS 主体)	-	-	-
extended-advance	default (フィルタ, QoS 均等)	8000	1024	8000
	filter-only (フィルタ専用)	8000	1024	8000
	qos-only (QoS 専用)	-	-	-
	filter (フィルタ主体)	8000	1024	8000
	qos (QoS 主体)	2000	1024	2000

(凡例) - : DHCP snooping は使用できない

注 1

untrust ポート配下の端末当たり 1 エントリを消費します。

注 2

バインディングデータベースエントリ配下のポート当たり 1 エントリを消費します。
チャンネルグループの場合、チャンネルグループ当たりのポート数を数えます。

表 3-65 DHCP snooping の最大 VLAN 数

フロー系テーブル容量名称	最大 VLAN 数
standard	-
standard-advance	512
extended	-
extended-advance	2048

(凡例) - : DHCP snooping は使用できない

3.2.8 冗長化構成による高信頼化

(1) GSRP

GSRP の収容条件を次の表に示します。

GSRP の VLAN ポート数は、チャンネルグループの場合、チャンネルグループ当たりの物理ポート数を数えます。

表 3-66 GSRP 収容条件

モデル	レイヤ 3 冗長機能	VLAN ポート数の合計	VLAN グループ最大数	VLAN グループ当たりの VLAN 最大数
AX6700S シリーズ 共通	あり	10000	128	4095
	なし	100000	128	4095

3. 収容条件

注

GSRP と VRF 機能を併用する（コンフィギュレーションコマンド `vrf mode` の `gsrp-enable-ipv4-ipv6` パラメータを設定している）場合、VLAN グループ当たりの VLAN 最大数は 250 となります。【OP-NPAR】

(2) VRRP

VRRP に関する収容条件を次の表に示します。

表 3-67 VRRP 収容条件

モデル	仮想ルータ最大数		track 設定最大数	track 割り当て最大数	
	インタフェース当たり	装置当たり		仮想ルータ当たり	装置当たり
AX6700S シリーズ共通	255 ¹	255 ¹	255	16 ²	255 ²

注 1 IPv4/IPv6 の仮想ルータの合計数です。

注 2 障害監視インタフェースと VRRP ボーリングの合計数です。

表 3-68 VRRP 収容条件（グループ切替機能使用時）

モデル	仮想ルータ最大数		最大グループ数	1グループ当たりの最大フォロ-仮想ルータ数	track 設定最大数	track 割り当て最大数	
	インタフェース当たり	装置当たり				仮想ルータ当たり	装置当たり
AX6700S シリーズ共通	255 ¹	4095 ¹	255	4094	255	16 ²	255 ²

注 1 IPv4/IPv6 の仮想ルータの合計数は 255 までです。ただし、グループ切替機能を利用し、フォロ-仮想ルータを作成することで、最大 4095 の仮想ルータが動作できます。

注 2 障害監視インタフェースと VRRP ボーリングの合計数です。

3.2.9 ネットワークの障害検出による高信頼化機能

(1) IEEE802.3ah/UDLD

IEEE802.3ah/UDLD の収容条件を次の表に示します。

表 3-69 設定可能ポート数

モデル	設定可能ポート数
AX6708S	192

(2) L2 ループ検知

(a) L2 ループ検知フレーム送信レート

L2 ループ検知の L2 ループ検知フレーム送信レートを次の表に示します。

表 3-70 L2 ループ検知フレーム送信レート

モデル	L2 ループ検知フレームの送信レート（装置当たり） ¹	
	スパニングツリー，GSRP，Ring Protocol のどれかを使用している場合	スパニングツリー，GSRP，Ring Protocol のどれも使用していない場合
AX6700S シリーズ共通	90pps（推奨値） ²	600pps（最大値） ³

- L2 ループ検知フレーム送信レート算出式

L2 ループ検知フレーム送信対象の VLAN ポート数 ÷ L2 ループ検知フレームの送信レート（pps） 送信間隔（秒）

注 1

送信レートは上記の条件式に従って、自動的に 600pps 以内で変動します。

注 2

スパニングツリー，GSRP，Ring Protocol のどれかを使用している場合は、90pps 以下に設定してください。90pps より大きい場合、スパニングツリー，GSRP，Ring Protocol の正常動作を保障できません。

注 3

600pps を超えるフレームは送信しません。送信できなかったフレームに該当するポートや VLAN ではループ障害を検知できなくなります。必ず 600pps 以下に設定してください。

(b) ネットワーク全体での動作可能装置数

ネットワーク全体で本機能が動作可能な装置台数は、AX6700S シリーズ，AX6600S シリーズ，AX6300S シリーズの合計で 64 台までです。

(c) 物理ポート数

L2 ループ検知を運用時の物理ポート数の収容条件を次の表に示します。

表 3-71 物理ポートの収容条件

NIF 略称	使用可能な物理ポート数 ¹
NK1G-24T	すべてのポート
NK1G-24S	すべてのポート
NK1GS-8M	すべてのポート
NK10G-4RX	BSU シングルアクト運転の場合，2 ポートまで
	BSU ダブルアクト運転または BSU トリプルアクト運転の場合，すべてのポート ²
NK10G-8RX	BSU シングルアクト運転の場合，2 ポートまで
	BSU ダブルアクト運転の場合，4 ポートまで ³
	BSU トリプルアクト運転の場合，6 ポートまで ^{4 5}

注 1

収容条件を超える物理ポートを使用した場合、常時または一時的に高負荷のトラフィックが流れると、L2 ループ検知フレームが廃棄されるおそれがあります。廃棄されることでループ障害の検知が遅れる場合があります。

注 2

BSU の冗長性を確保したい場合は、BSU トリプルアクト運転で使用してください。

注 3

ポート番号が 1 ~ 4，3 ~ 6，または 5 ~ 8 のどれかの範囲で使用してください。

注 4

3. 収容条件

ポート番号が 1 ~ 6, または 3 ~ 8 のどちらかの範囲で使用してください。

注 5

BSU の冗長性を確保したい場合は, 使用する物理ポートを 4 ポートまでで運用してください。ただし, ポート番号が 1 ~ 4, 3 ~ 6, または 5 ~ 8 のどれかの範囲で使用してください。

(3) CFM

CFM の収容条件を次の表に示します。

表 3-72 CFM の収容条件

モデル	ドメイン数	MA 数	MEP 数	MIP 数	CFM ポート 総数 ^{1 2}	リモート MEP 総数 ^{2 3}
AX6700S シ リーズ共通	8 / 装置	192 / 装置	192 / 装置	192 / 装置	1024 / 装 置	8064 / 装置

注 1

CFM ポート総数とは, MA のプライマリ VLAN のうち, CFM のフレームを送信する VLAN ポートの総数です。

Down MEP だけの MA の場合

Down MEP の VLAN ポートの総数

Up MEP を含む MA の場合

プライマリ VLAN の全 VLAN ポートの総数

なお, CFM ポート総数は運用コマンド `show cfm summary` で確認できます。

注 2

CFM ポート総数およびリモート MEP 総数は, CCM 送信間隔がデフォルト値のときの収容条件です。CCM 送信間隔を変更すると, CFM ポート総数およびリモート MEP 総数の収容条件が変わります。CCM 送信間隔による CFM ポート総数およびリモート MEP 総数の収容条件を次の表に示します。

表 3-73 CCM 送信間隔による収容条件

モデル	CCM 送信間隔	CFM ポート総数	リモート MEP 総数
AX6700S シリーズ共通	1 分以上	1024 / 装置	8064 / 装置
	10 秒	256 / 装置	4032 / 装置
	1 秒	192 / 装置	400 / 装置

注 3

リモート MEP 総数とは, 自装置以外の MEP の総数です。MEP からの CCM 受信性能に影響しません。リモート MEP 総数は運用コマンド `show cfm remote-mep` で確認できます。

表 3-74 CFM の物理ポートおよびチャネルグループの収容条件

モデル	MEP・MIP を設定可能な物理ポートおよびチャネルグループの総数
AX6700S シリーズ 共通	全ポート

注

MEP・MIP は同一ポートに対して複数設定できます。チャンネルグループの場合は、チャンネルグループ単位で1ポートと数えます。

表 3-75 CFM のデータベース収容条件

モデル	MEP CCM データベース エン트리数	MIP CCM データベース エン트리数	Linktrace データベース エン트리数
AX6700S シリーズ共通	63 / MEP	12288 / 装置	1024 / 装置

注

1 ルート当たり 256 装置の情報を保持する場合は、最大で 4 ルート分を保持します (1024 ÷ 256 装置 = 4 ルート)。

3.2.10 隣接装置情報の管理 (LLDP/OADP)

隣接装置情報 (LLDP/OADP) の収容条件を次の表に示します。

表 3-76 隣接装置情報 (LLDP/OADP) の収容条件

モデル	LLDP 隣接装置情報	OADP 隣接装置情報
AX6700S シリーズ共通	192	250

注

LLDP/OADP の隣接装置情報数とは、本装置に接続されている隣接装置から収集できる情報のことで、基本的に 1 隣接装置当たり 1 情報を収集できます。

3.2.11 IPv4・IPv6 パケット中継

(1) IP アドレスを設定できるインタフェース数

本装置では、次のインタフェースに IP アドレスを設定できます。

- VLAN インタフェース
- マネージメントポート

ここでは、IP アドレスを設定できるインタフェースの最大数について説明します。また、設定できる IP アドレスの最大数について説明します。

インタフェースに対してサポートする最大インタフェース数を次の表に示します。ここで示す値は、IPv4 と IPv6 との合計の値です。なお、IPv4 と IPv6 を同一のインタフェースに設定することも、個別に設定することもできます。

表 3-77 インタフェースに対する最大インタフェース数

モデル	VLAN インタフェース数 (装置当たり)	マネージメントポート (装置当たり)
AX6700S シリーズ共通	4095	1

(2) マルチホームの最大サブネット数

LAN のマルチホーム接続では一つのインタフェースに対して、複数の IPv4 アドレス、または IPv6 アド

3. 収容条件

レスを設定できます。

(a) IPv4 の場合

IPv4 でのマルチホームの最大サブネット数を次の表に示します。ただし、マネージメントポートは IPv4 のマルチホーム不可のため 1 になります。

表 3-78 マルチホームの最大サブネット数 (IPv4 の場合)

モデル	マルチホーム サブネット数 (インタフェース当たり)
AX6700S シリーズ共通	256

(b) IPv6 の場合

IPv6 でのマルチホームの最大サブネット数を次の表に示します。なお、ここで示す値にはリンクローカルアドレスを含みます。一つのインタフェースには必ず一つのリンクローカルアドレスが設定されます。このため、すべてのインタフェースで IPv6 グローバルアドレスだけを設定した場合、実際に装置に設定される IPv6 アドレス数は、表の数値に自动生成される IPv6 リンクローカルアドレス数 1 を加算した 8 になります。

表 3-79 マルチホームの最大サブネット数 (IPv6 の場合)

モデル	マルチホーム サブネット数 (インタフェース当たり)
AX6700S シリーズ共通	7

(3) IP アドレス最大設定数

(a) IPv4 アドレス

コンフィグレーションで設定できる IPv4 アドレスの最大数を次の表に示します。なお、この表で示す値は、インタフェースに設定できる IPv4 アドレス数です。

表 3-80 コンフィグレーションで装置に設定できる IPv4 アドレスの最大数

モデル	VLAN インタフェースに設定できる IPv4 アドレス数 (装置当たり)	マネージメントポートに設定できる IPv4 アドレス数 (装置当たり)
AX6700S シリーズ共通	4096	1

(b) IPv6 アドレス

コンフィグレーションで設定できる装置当たりの IPv6 アドレスの最大数を次の表に示します。なお、ここで示す値はインタフェースに設定する IPv6 アドレスの数です。また、IPv6 リンクローカルアドレスの数も含みます。一つのインタフェースには必ず一つの IPv6 リンクローカルアドレスが設定されます。このため、すべてのインタフェースに IPv6 グローバルアドレスを設定した場合、インタフェースには自動で IPv6 リンクローカルアドレスが付与され、実際に装置に設定される IPv6 アドレスの数は次の表に示す値となります。

表 3-81 コンフィグレーションで装置に設定できる IPv6 アドレスの最大数

モデル	VLAN インタフェースに設定できる IPv6 アドレス数 (装置当たり)	マネージメントポートに設定できる IPv6 アドレス数 (装置当たり)
AX6700S シリーズ共通	4096	7

表 3-82 VLAN インタフェースに設定される IPv6 アドレス数

コンフィグレーションで VLAN インタフェースに設定する IPv6 アドレスの数		自動で設定する IPv6 リンクローカルアドレスの数	VLAN インタフェースに設定される IPv6 アドレス数
IPv6 リンクローカルアドレス	IPv6 グローバルアドレス		
4095	0	0	4095
0	4096	4095	8191

注 IPv6 グローバルアドレスは、マルチホームを使用することで 4096 まで設定できます。

表 3-83 マネージメントポートに設定される IPv6 アドレス数

コンフィグレーションでマネージメントポートに設定する IPv6 アドレスの数		自動で設定する IPv6 リンクローカルアドレスの数	マネージメントポートに設定される IPv6 アドレス数
IPv6 リンクローカルアドレス	IPv6 グローバルアドレス		
1	0	0	1
0	7	1	8

(4) 最大相手装置数

本装置が接続する通信可能な最大相手装置数を示します。この場合の相手装置はスイッチに限らず、端末も含まれます。

(a) ARP エントリ数

IPv4 の場合、ARP によって、送信しようとするパケットの宛先アドレスに対応するハードウェアアドレスを決定します。最大相手装置数は、ARP エントリ数によって決まります。ARP エントリはコンフィグレーションコマンドを使用することで、スタティックに 4096 エントリ登録できます。本装置でサポートする ARP エントリの最大数については、次の表を参照してください。最大エントリ数は、スタティックで登録したエントリ数を含みます。

- 表 3-10 standard の経路系テーブルエントリ数
- 表 3-11 extended の経路系テーブルエントリ数

(b) NDP エントリ数

IPv6 の場合、NDP でのアドレス解決によって、送信しようとするパケットの宛先アドレスに対応するハードウェアアドレスを決定します。最大相手装置数は NDP エントリ数によって決まります。NDP エントリは、コンフィグレーションコマンドを使用することで、スタティックに 4096 エントリ登録できます。本装置でサポートする NDP エントリの最大数については、次の表を参照してください。最大エントリ数は、スタティックで登録したエントリ数を含みます。

3. 収容条件

- 表 3-10 standard の経路系テーブルエントリ数
- 表 3-11 extended の経路系テーブルエントリ数

(c) RA の最大相手端末数

RA ではルータから通知される IPv6 アドレス情報を基に端末でアドレスを生成します。本装置での最大相手端末数を次の表に示します。

表 3-84 RA の最大相手端末数

モデル	RA の最大相手端末数	
	インタフェース当たり	装置当たり
AX6700S シリーズ共通	4096	4096

(5) ポリシーベースルーティング

ポリシーベースルーティングでは、フィルタのフロー検出を使用して、ポリシーベースルーティングの対象にするフローを検出します。なお、フロー系エントリの配分パターンが qos-only の場合、ポリシーベースルーティングは使用できません。

(a) ポリシーベースルーティングの収容条件

アクセスリストの動作に中継先の経路を指定

アクセスリストの動作に中継先の経路を指定する場合の収容条件を次の表に示します。

表 3-85 装置当たりのポリシーベースルーティングのエントリ数

項目	IPv4 ポリシーベースルーティング	IPv6 ポリシーベースルーティング
アクセスリストエントリ数	「表 3-41 フィルタ・QoS エントリ数」を参照 ¹	「表 3-41 フィルタ・QoS エントリ数」を参照 ¹
ネクストホップエントリ数	256 ²	256 ²

注 1

エントリ数の算出方法は、「3.2.5 フィルタ・QoS」と同じです。

注 2

1 ネクストホップを 1 エントリとして登録します。このため、複数のアクセスリストで同一のネクストホップを設定した場合、使用するエントリ数は 1 エントリと計算します。

アクセスリストの動作にポリシーベースルーティングリスト情報を指定

アクセスリストの動作にポリシーベースルーティングリスト情報を指定する場合の収容条件を次の表に示します。

表 3-86 装置当たりのポリシーベースルーティンググループのエントリ数

項目	IPv4 ポリシーベースルーティンググループ	IPv6 ポリシーベースルーティンググループ
アクセスリストエントリ数	「表 3-41 フィルタ・QoS エントリ数」を参照 ¹	-
ポリシーベースルーティングリスト数	256 ²	-
ポリシーベースルーティングリスト情報内に設定できる経路数	8	-

項目	IPv4 ポリシーベースルーティンググループ	IPv6 ポリシーベースルーティンググループ
ポリシーベースルーティングのトラッキング機能と連携できる経路数	1024 ³	-

(凡例) - : 該当なし

注 1

エン트리数の算出方法は、「3.2.5 フィルタ・QoS」と同じです。

注 2

1 ポリシーベースルーティングリスト情報を 1 リストとして登録します。このため、複数のアクセスリストで同一のポリシーベースルーティングリスト情報を設定した場合、使用するリスト数は 1 リストと計算します。

注 3

1 トラック ID を 1 エントリとして登録します。このため、複数の経路で同一のトラック ID を設定した場合、使用するエン트리数は 1 エントリと計算します。

(b) トラッキング機能の収容条件

ポリシーベースルーティングのトラッキング機能の収容条件を次の表に示します。

表 3-87 トラッキング機能の収容条件

項目	収容条件
トラックの数	1024
ポーリング監視トラックの数	1024

注 コンフィグレーションコマンド `type icmp` を設定したトラックの数です。

(6) DHCP/BOOTP リレー

DHCP/BOOTP リレーの収容条件を次の表に示します。

表 3-88 DHCP/BOOTP リレーの最大数

モデル	クライアント接続インタフェース数	サーバ台数 (グローバルネットワーク、 VRF ごと)	VRF 使用時の装置 当たりのサーバ台数
AX6700S シリーズ共通	2048	16	256

(7) IPv6 DHCP リレー

IPv6 DHCP リレーの収容条件を次の表に示します。

表 3-89 IPv6 DHCP リレーの最大数

モデル	装置当たりの最大数	
	配布プレフィックス数	インタフェース数
AX6700S シリーズ共通	1024	1024

注

クライアントを直接収容した場合に IPv6 DHCP サーバによって配布される PD プレフィックス数です。ほかのリレー経由のパケットや PD プレフィックス以外の情報は、この条件に関係なく中継できます。

3. 収容条件

(8) DHCP サーバ

DHCP サーバで設定できるインタフェース数および配布可能 IP アドレス数などを次の表に示します。

表 3-90 DHCP サーバの最大数

モデル	最大配布可能 IP アドレス数	最大固定 IP アドレス割り当て数	最大インタフェース数	最大管理サブネット数
AX6700S シリーズ共通	8192	320	2048	2048

(9) IPv6 DHCP サーバ

IPv6 DHCP サーバの収容条件を次の表に示します。

表 3-91 IPv6 DHCP サーバの最大数

モデル	装置当たりの最大数	
	インタフェース数	最大配布可能 Prefix
AX6700S シリーズ共通	1024	1024

3.2.12 IPv4・IPv6 ルーティングプロトコル

(1) 最大隣接ルータ数

最大隣接ルータ数の定義を次の表に示します。

表 3-92 最大隣接ルータ数の定義

ルーティングプロトコル別	最大隣接ルータ数の定義
スタティックルーティング	ネクストホップ・アドレスの数
RIP, RIPng	RIP/RIPng が動作するインタフェース数
OSPF, OSPFv3	本装置が OSPF/OSPFv3 指定ルータ (DR, BDR) になるネットワークの場合、そのネットワーク上のそのほかすべての OSPF/OSPFv3 ルータ数。本装置が OSPF/OSPFv3 指定ルータにならないネットワークの場合、そのネットワーク上の指定ルータ (DR, BDR) 数。
BGP4, BGP4+	BGP4/BGP4+ ピア数

最大隣接ルータ数を次の表に示します。

表 3-93 最大隣接ルータ数

ルーティングプロトコル	最大隣接ルータ数	
	ポリシーベースルーティングのトラッキング機能を使用しない	ポリシーベースルーティングのトラッキング機能を使用する
スタティックルーティング (IPv4, IPv6 の合計)	4096	4096
RIP	200	100
RIPng	200	100
OSPF	200	100

ルーティングプロトコル	最大隣接ルータ数	
	ポリシーベースルーティングのトラッキング機能を使用しない	ポリシーベースルーティングのトラッキング機能を使用する
OSPFv3	100	50
BGP4	200	100
BGP4+	200	100
RIP, OSPF, BGP4, RIPng, OSPFv3, BGP4+ の合計	256	128

注

動的監視機能を使用する隣接ルータは、ポーリング間隔によって数が制限されます。詳細は、次の表を参照してください。

表 3-94 スタティックの動的監視機能を使用できる最大隣接ルータ数

ポーリング周期	動的監視機能を使用できる最大隣接ルータ数
1 秒	60
5 秒	300
10 秒	600
20 秒	1200

(2) 経路エントリ数と最大隣接ルータ数の関係

最大経路エントリ数と最大隣接ルータ数の関係を次の表に示します。

表 3-95 経路エントリ数と最大隣接ルータ数の関係

ルーティングプロトコル	経路エントリ数 ¹	最大隣接ルータ数 ²	
		ポリシーベースルーティングのトラッキング機能を使用しない	ポリシーベースルーティングのトラッキング機能を使用する
RIP	1000	100	50
	2000	50	25
	10000	10	5
RIPng	1000	100	50
	2000	50	25
	10000	10	5
OSPF ^{3 4}	1000	200	100
	2000	100	50
	5000	40	20
	10000	20	10
OSPFv3 ^{3 5}	1000	100	50
	2000	50	25
	5000	20	10
	10000	10	5
BGP4	6	200	100

3. 収容条件

ルーティングプロトコル	経路エントリ数 ¹	最大隣接ルータ数 ²	
		ポリシーベースルーティングのトラッキング機能を使用しない	ポリシーベースルーティングのトラッキング機能を使用する
BGP4+	6	200	100

注 1

経路エントリ数は代替経路を含みます。

注 2

各ルーティングプロトコル (RIP, RIPng, OSPF, OSPFv3, BGP4, BGP4+) を併用して使用する場合の最大隣接ルータ数は、それぞれ $1/n$ (n : 使用ルーティングプロトコル数) です。例えば、BGP4, BGP4+ を使用しないで、OSPF (1000 経路) と OSPFv3 (1000 経路) を併用して使用する場合の最大隣接ルータ数は $1/2$ となり、OSPF では 100, OSPFv3 では 50 となります。

注 3

OSPF/OSPFv3 の最大経路エントリ数は LSA 数を意味します。

注 4

VRF で OSPF を使用している場合、装置全体の最大隣接ルータ数は 200 ですが、各 VRF で保持している LSA 数 × 各 VRF の隣接ルータ数の総計が 20 万を超えないようにしてください。

注 5

VRF で OSPFv3 を使用している場合、装置全体の最大隣接ルータ数は 100 ですが、各 VRF で保持している LSA 数 × 各 VRF の隣接ルータ数の総計が 10 万を超えないようにしてください。

注 6

「表 3-15 BSU-LA 経路配分パターンと収容経路エントリ数 (その 1)」、「表 3-16 BSU-LA 経路配分パターンと収容経路エントリ数 (その 2)」、「表 3-19 BSU-LB 経路配分パターンと収容経路エントリ数 (その 1)」、および「表 3-20 BSU-LB 経路配分パターンと収容経路エントリ数 (その 2)」を参照してください。

(3) 本装置で設定できるコンフィギュレーションの最大数

ルーティングプロトコルについて、設定できるコンフィギュレーションの最大数を次の表に示します。

なお、この表で示す値はコンフィギュレーションで設定できる最大数です。運用する際は本章にある収容条件をすべて満たすようにしてください。

表 3-96 コンフィギュレーションの最大設定数

分類	コンフィギュレーションコマンド	最大数の定義	最大設定数
IPv4 スタティック	ip route	テーブル容量が standard 時の設定行数	8192
		テーブル容量が extended 時の設定行数	16384
IPv6 スタティック	ipv6 route	テーブル容量が standard 時の設定行数	8192
		テーブル容量が extended 時の設定行数	16384
IPv4 集約経路	ip summary-address	設定行数	1024
IPv6 集約経路	ipv6 summary-address	設定行数	1024
RIP	network	設定行数	256
	ip rip authentication key	設定行数	512

分類	コンフィグレーション コマンド	最大数の定義	最大 設定数
OSPF	area range	設定行数	1024
	area virtual-link	authentication-key , message-digest-key パラメータを 設定した行数の総計	512
	ip ospf authentication-key ip ospf message-digest-key	各設定行数の総計	512
	network	設定行数	512
	router ospf	設定行数	256
BGP4	network	設定行数	1024
OSPFv3	area range	設定行数	1024
	ipv6 router ospf	設定行数	128
BGP4+	network	設定行数	1024
経路フィルタ	distribute-list in (RIP) distribute-list out (RIP) redistribute (RIP)	各設定行数の総計	2048
	distribute-list in (OSPF) distribute-list out (OSPF) redistribute (OSPF)	各設定行数の総計	2048
	distribute-list in (BGP4) distribute-list out (BGP4) redistribute (BGP4)	各設定行数の総計	2048
	distribute-list in (RIPng) distribute-list out (RIPng) redistribute (RIPng)	各設定行数の総計	2048
	distribute-list in (OSPFv3) distribute-list out (OSPFv3) redistribute (OSPFv3)	各設定行数の総計	1024
	distribute-list in (BGP4+) distribute-list out (BGP4+) redistribute (BGP4+)	各設定行数の総計	2048
	ip as-path access-list	設定 <Id> の種類数	1024
		設定行数	4096
	ip community-list	設定 <Id> の種類数	512
		standard 指定の設定行数	1024
		expanded 指定の設定行数	1024
	ip prefix-list	設定 <Id> の種類数	2048
		設定行数	8192
	ipv6 prefix-list	設定 <Id> の種類数	2048
		設定行数	8192
	neighbor in (BGP4) neighbor out (BGP4)	<IPv4-Address> の設定行数の総計	256
<Peer-Group> の設定行数の総計		256	
neighbor in (BGP4+) neighbor out (BGP4+)	<IPv6-Address> の設定行数の総計	256	

3. 収容条件

分類	コンフィギュレーション コマンド	最大数の定義	最大 設定数
		<Peer-Group> の設定行数の総計	256
	route-map	設定 <Id> の種類数	1024
		設定 <Id> と <Seq> の組み合わせ 種類数	4096
	match as-path	各設定行で指定したパラメータの 総計	4096
	match community	各設定行で指定したパラメータの 総計	4096
	match interface	各設定行で指定したパラメータの 総計	2048
	match ip address match ipv6 address	各設定行で指定したパラメータの 総計	4096
	match ip route-source match ipv6 route-source	各設定行で指定したパラメータの 総計	2048
	match origin	設定行数	2048
	match protocol	各設定行で指定したパラメータの 総計	4096
	match route-type	設定行数	2048
	match tag	各設定行で指定したパラメータの 総計	2048
	match vrf	各設定行で指定したパラメータの 総計	4096
	set as-path prepend count set distance set local-preference set metric set metric-type set origin set tag	どれか一つが設定された route-map の、<Id> と <Seq> の 組み合わせ種類数	4096
	set community	各設定行で指定したパラメータの 総計	2048
	set community-delete	各設定行で指定したパラメータの 総計	2048

3.2.13 IPv4・IPv6 マルチキャストルーティングプロトコル

(1) IPv4 マルチキャスト

IPv4 マルチキャストを設定できるインタフェース数およびルーティングテーブルのエントリ数を次の表に示します。

複数の VRF で IPv4 マルチキャストを使用する場合、グローバルネットワークとすべての VRF の合計を本収容条件内に収めてください。

なお、PIM-DM はグローバルネットワークでだけ動作します。また、本装置では、PIM-SM と PIM-DM は同時に動作できません。

表 3-97 IPv4 マルチキャストの最大数

項目	最大数	
	BSU-LA	BSU-LB
PIM-SM/SSM または PIM-DM マルチキャストインタフェース数 ¹	127 / 装置	255 / 装置
IGMP 動作インタフェース数	127 / 装置	255 / 装置
マルチキャスト送信元の数	256 / グループ 3000 / 装置	256 / グループ 3000 / 装置
PIM-SM/SSM マルチキャスト経路情報のエントリ ((S,G) エントリ, (*,G) エントリ, およびネガティブキャッシュ) 数, または PIM-DM マルチキャスト経路情報のエントリ ((S,G) エントリ) 数 ¹ S: 送信元 IP アドレス G: グループアドレス	4000 / 装置	8000 / 装置
IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連携動作させる設定数 (ソース, グループのペア数) ²	256 / 装置	256 / 装置
IGMPv3 で 1Report につき処理できる record 情報 ³	32record / メッセージ 32 ソース / record	32record / メッセージ 32 ソース / record
IGMP 加入グループ数 ^{4 5}	2000 / 装置	3000 / 装置
マルチキャストルータ隣接数 ¹	256 / 装置	256 / 装置
ランデブーポイント数	2 / グループ	2 / グループ
1 装置当たりランデブーポイントで設定できるグループ数 ⁶	128 / 装置	128 / 装置
1 ネットワーク (VPN) 当たりランデブーポイントに設定できる延べグループ数	128 / ネットワーク (VPN) 256 / 装置 ⁷	128 / ネットワーク (VPN) 256 / 装置 ⁷
1 ネットワーク (VPN) 当たりの BSR 候補数	16 / ネットワーク (VPN) 256 / 装置 ⁷	16 / ネットワーク (VPN) 256 / 装置 ⁷
静的加入グループ数 ⁸	256 / 装置	256 / 装置
静的ランデブーポイント (RP) ルータアドレス数	16 / 装置	16 / 装置
IGMP グループ当たりのソース数	256 / グループ	256 / グループ
マルチキャスト中継エントリの延べ下流インタフェース数 ^{9 10}	140000 / 装置	280000 / 装置
マルチキャストを設定できる VRF 数 ¹¹	127 / 装置	249 / 装置
エクストラネットのマルチキャストフィルタ数 ¹²	512 / 装置	512 / 装置
エクストラネットで使用する route-map 数	256 / 装置 256 / VRF	256 / 装置 256 / VRF
PIM-SM VRF ゲートウェイ動作マルチキャストアドレス数 ¹³	256 / 装置 256 / VRF	256 / 装置 256 / VRF

注 1

PIM-DM を使用する場合、隣接ルータ数によって使用できるマルチキャスト経路情報のエントリ数が異なります。「表 3-98 PIM-DM での隣接ルータ数に対するマルチキャスト経路情報のエントリ数」に示す範囲内で使用してください。

注 2

マルチキャストで使用するインタフェース数および加入グループ数によって設定できる数が変わります。「表 3-99

3. 収容条件

使用インタフェース数に対する IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数、および「表 3-100 加入グループ数に対する IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数」に示す範囲内で使用してください。加入グループ数は、動的および静的加入グループ数の総計です。同一グループアドレスが異なるインタフェースに加入している場合、加入グループ数は一つではなく、加入したインタフェースの数になります。

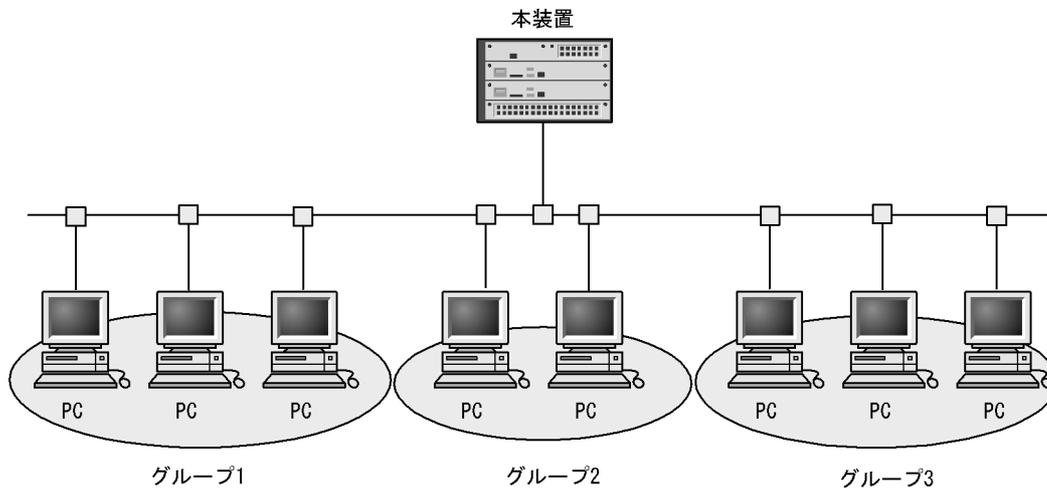
注 3

一つの Report メッセージで処理できるソース数は延べ 256 ソースまでです。ソース情報のない record も 1 ソースとして数えます。

IGMPv3 (EXCLUDE モード) で PIM-SSM を連携動作させる設定をした場合、その設定に一致した EXCLUDE record で定義されているソース数を数えます。また、受信した Report メッセージ内に EXCLUDE record が複数存在し、IGMPv3 (EXCLUDE モード) で PIM-SSM を連携動作させる設定で追加したソース数が延べ 256 を超えた場合、以降のそのメッセージ内の EXCLUDE record で、連携動作の対象となる EXCLUDE record についてマルチキャスト中継情報は作成しません。

注 4

本装置に直接接続しているグループの数を示します。IGMPv3 使用時に送信元を指定する場合のグループ数は、送信元とグループの組み合わせの数となります。次の図の例ではグループ数が 3 になります。



注 5

IPv4 でのインタフェース当たりの加入可能グループ数を「表 3-101 IPv4 でのインタフェース当たりの加入グループ数」に示します。

注 6

グループを指定しないでランデブーポイントを設定した場合、デフォルトグループが設定されます。グローバルネットワークおよび VRF でランデブーポイントを設定する場合、デフォルトグループも 1 グループとして、装置内またはネットワーク (VPN) 内の総グループ数が収容条件内になるように設定してください。

注 7

本装置のグローバルネットワークとすべての VRF に接続するネットワーク (VPN) 上の総数です。

注 8

静的加入グループ数とは、各マルチキャストインタフェースで静的加入するグループアドレスの総数です。同一グループアドレスを複数の異なるインタフェースに静的加入設定した場合、静的加入グループ数は一つではなく、静的加入設定したインタフェースの数になります。また、PIM-SM VRF ゲートウェイで指定したグループアドレスの延べ数との合計になります。

注 9

構成およびリソース状況によっては最大数が BSU-LA 搭載時は 140000 以下、BSU-LB 搭載時は 280000 以下となることがあります。

注 10

マルチキャスト中継エントリの延べ下流インタフェース数は、IPv4 マルチキャストと IPv6 マルチキャストの合計

です。

注 11
PIM-SM/SSM 使用時だけ設定できます。

注 12
すべての route-map で指定した access-list 内のアドレスの延べ数です。

注 13
エクストラネットで指定した route-map を使用します。route-map に指定した access-list 内で、ホストアドレス (32 ビットマスク) として指定したマルチキャストアドレスが対象となります。
装置当たりの上限は、すべての VRF で指定した PIM-SM VRF ゲートウェイのグループアドレスの延べ数です。
また、静的加入グループ数で指定したグループアドレス数との合計になります。

表 3-98 PIM-DM での隣接ルータ数に対するマルチキャスト経路情報のエントリ数

隣接ルータ数	マルチキャスト経路情報のエントリ数
256	1000
128	2000
64	4000
32	8000

表 3-99 使用インタフェース数に対する IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数

使用インタフェース数	IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連動させる設定数
31	256
63	128
127	64
255	32

表 3-100 加入グループ数に対する IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数

加入グループ (延べ数)	IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連動させる設定数
64	256
128	128
256	64
512	32
1024	16
2048	8
4096	4
8128	2

表 3-101 IPv4 でのインタフェース当たりの加入グループ数

マルチキャスト動作インタフェース数	インタフェース当たりの加入可能グループ数
31	256
63	128
127	64

3. 収容条件

マルチキャスト動作インタフェース数	インタフェース当たりの加入可能グループ数
255	32

(a) IPv4 マルチキャスト使用時の注意事項

マルチキャストデータの送信元に対して到達できるすべてのインタフェースに PIM の設定が必要です。

(b) マルチキャストデータの送信元サーバに関する注意

マルチキャストデータの送信元となるサーバの中には、マルチキャストパケットをバーストトラフィックとして送信する特性を持つものがあります。この特性を持つサーバから受信したマルチキャストデータを、マルチキャスト配信する場合には注意が必要です。マルチキャスト配信先の回線を収容するネットワークインタフェース機構 (NIF) の種類によって、マルチキャスト動作可能なインタフェース数が異なります。マルチキャスト動作可能なインタフェース数を次の表に示します。

表 3-102 マルチキャスト動作可能なインタフェース数

NIF 略称	マルチキャスト動作可能なインタフェース数 (推奨値)
NK1G-24T	ポート当たり 16 インタフェース
NK1G-24S	ポート当たり 16 インタフェース
NK1GS-8M	NIF 当たり 255 インタフェース
NK10G-4RX	ポート当たり 32 インタフェース
NK10G-8RX	ポート当たり 32 インタフェース

注

推奨値は、送信元サーバが、マルチキャストパケットを 8 バーストで送信する特性 (サーバで 8 パケット分のマルチキャストデータをいったん蓄積したあとに、ネットワークに対して連続的に送信する特性) を持っていることを想定しています。バースト数が大きくなると、パケットを一部廃棄することがあるので、マルチキャストを定義するインタフェース数を少なくする必要があります。

(2) IPv6 マルチキャスト

IPv6 マルチキャストを設定できるインタフェース数およびルーティングテーブルのエントリ数を次の表に示します。

複数の VRF で IPv6 マルチキャストを使用する場合、グローバルネットワークとすべての VRF の合計を本収容条件内に収めてください。

表 3-103 IPv6 マルチキャストエントリ最大数

項目	最大数	
	BSU-LA	BSU-LB
PIM-SM/SSM マルチキャストインタフェース数 ¹ ²	127 / 装置	255 / 装置
MLD 動作インタフェース数 ¹	127 / 装置	255 / 装置
マルチキャスト送信元の数	256 / グループ	256 / グループ
PIM-SM/SSM マルチキャストルーティングエントリ ((S,G) エントリ, (*,G) エントリ, およびネガティブキャッシュ) 数 S: 送信元 IP アドレス G: グループアドレス	1000 / 装置	8000 / 装置

項目	最大数	
	BSU-LA	BSU-LB
MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連携動作させる設定数 (ソース, グループペア数) ³	256 / 装置	256 / 装置
MLDv2 で 1Report につき処理できる record 情報 ⁴	32record / メッセージ 32 ソース / record	32record / メッセージ 32 ソース / record
MLD 加入グループ数 ^{5 6}	256 / 装置	256 / 装置
マルチキャストルータ隣接数	256 / 装置	256 / 装置
ランデブーポイント数	2 / グループ	2 / グループ
1 装置当たりランデブーポイントで設定できるグループ数 ⁷	128 / 装置	128 / 装置
1 ネットワーク (VPN) 当たりランデブーポイントに設定できる延べグループ数	128 / ネットワーク (VPN) 256 / 装置 ⁸	128 / ネットワーク (VPN) 256 / 装置 ⁸
1 ネットワーク (VPN) 当たりの BSR 候補数	16 / ネットワーク (VPN) 256 / 装置 ⁸	16 / ネットワーク (VPN) 256 / 装置 ⁸
静的加入グループ数 ^{9 10}	2000 / 装置	4000 / 装置
静的ランデブーポイント (RP) ルータアドレス数	16 / 装置	16 / 装置
MLD グループ当たりのソース数	256 / グループ	256 / グループ
遠隔のマルチキャストサーバアドレスを直接接続サーバとして扱う設定数	256 / 装置 16 / インタフェース	256 / 装置 16 / インタフェース
マルチキャスト中継エントリの延べ下流インタフェース数 ^{11 12}	140000 / 装置	280000 / 装置
マルチキャストを設定できる VRF 数	127 / 装置	249 / 装置
エクストラネットのマルチキャストフィルタ数 ¹³	512 / 装置	512 / 装置
エクストラネットで使用する route-map 数	256 / 装置 256 / VRF	256 / 装置 256 / VRF
PIM-SM VRF ゲートウェイ動作マルチキャストアドレス数 ¹⁴	256 / 装置 256 / VRF	256 / 装置 256 / VRF

注 1
マルチホームをサポートします。

注 2
IPv6 マルチキャストインタフェースとして、このほかにカプセル化用インタフェースが一つ存在します。このため、IPv6 PIM-SM マルチキャストインタフェース全体の数は、BSU-LA 搭載時は 128 個、BSU-LB 搭載時は 256 個になりますが、ユーザが設定できるのはそのうち BSU-LA 搭載時は 127 個、BSU-LB 搭載時は 255 個です。また、PIM-SM と PIM-SSM の合計で BSU-LA 搭載時は 127 / 装置、BSU-LB 搭載時は 255 / 装置となります。

注 3
マルチキャストで使用するインタフェース数および加入グループ数によって設定できる数が変わります。「表 3-104 使用インタフェース数に対する MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数」および「表 3-105 加入グループ数に対する MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数」に示す範囲内で使用してください。加入グループ数は、動的および静的加入グループ数の総計です。同一グループアドレスが異なるインタフェースに加入している場合、加入グループ数は一つでなく、加入したインタフェースの数になります。

3. 収容条件

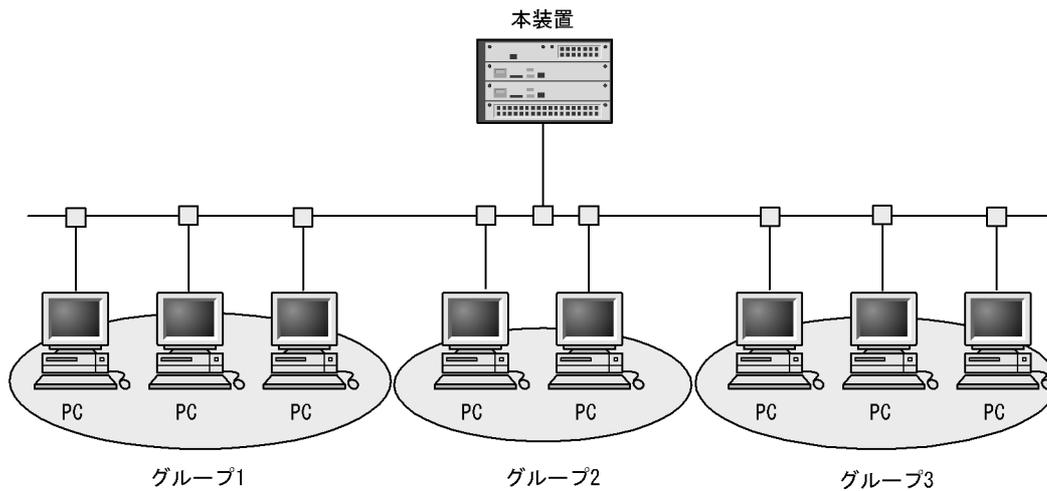
注 4

一つの Report メッセージで処理できるソース数は延べ 1024 ソースまでです。ソース情報のない record も 1 ソースとして数えます。

MLDv2 (EXCLUDE モード) で PIM-SSM を連携動作させる設定をした場合、その設定に一致した EXCLUDE record で定義されているソース数を数えます。また、受信した Report メッセージ内に EXCLUDE record が複数存在し、MLDv2 (EXCLUDE モード) で PIM-SSM を連携動作させる設定で追加したソース数が延べ 1024 を超えた場合、以降のそのメッセージ内の EXCLUDE record で、連携動作の対象となる EXCLUDE record についてマルチキャスト中継情報は作成しません。

注 5

本装置に直接接続しているグループの数を示します。MLDv2 使用時に送信元を指定する場合のグループ数は、送信元とグループの組み合わせの数となります。次の図の例ではグループ数が 3 になります。



注 6

IPv6 でのインタフェース当たりの加入可能グループ数を「表 3-106 IPv6 でのインタフェース当たりの加入可能グループ数」に示します。

注 7

グループを指定しないでランデブーポイントを設定した場合、デフォルトグループが設定されます。グローバルネットワークおよび VRF でランデブーポイントを設定する場合、デフォルトグループも 1 グループとして、装置内またはネットワーク (VPN) 内の総グループ数が収容条件内になるように設定してください。

注 8

本装置のグローバルネットワークとすべての VRF に接続するネットワーク (VPN) 上の総数です。

注 9

静的加入グループ数とは、各マルチキャストインタフェースで静的加入するグループアドレスの総数です。同一グループアドレスを複数の異なるインタフェースに静的加入設定した場合、静的加入グループ数は一つではなく、静的加入設定したインタフェースの数になります。また、PIM-SM VRF ゲートウェイで指定したグループアドレスの延べ数との合計になります。

注 10

一つのインタフェースに設定できる静的加入グループ数は 256 までです。

注 11

構成およびリソース状況によっては最大数が BSU-LA 搭載時は 140000 以下、BSU-LB 搭載時は 280000 以下となることがあります。

注 12

マルチキャスト中継エントリの延べ下流インタフェース数は、IPv4 マルチキャストと IPv6 マルチキャストの合計です。

注 13

すべての route-map で指定した access-list 内のアドレスの延べ数です。

注 14

エキストラネットで指定した route-map を使用します。route-map に指定した access-list 内で、ホストアドレス（128 ビットマスク）として指定したマルチキャストアドレスが対象となります。

装置当たりの上限は、すべての VRF で指定した PIM-SM VRF ゲートウェイのグループアドレスの延べ数です。また、静的加入グループ数で指定したグループアドレス数との合計になります。

表 3-104 使用インタフェース数に対する MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数

使用インタフェース数	MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連動させる設定数
31	256
63	256
127	256
255	256

表 3-105 加入グループ数に対する MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数

加入グループ数 (延べ数)	MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連動させる設定数
64	256
128	128
256	64
512	32
1024	16
2048	8
4096	4
8128	2

表 3-106 IPv6 でのインタフェース当たりの加入可能グループ数

マルチキャスト動作インタフェース数	インタフェース当たりの加入可能グループ数
31	256
63	128
127	64
255	32

(a) PIM-SM / SSM 使用時の注意事項

マルチキャストデータの送信元に対して到達できるすべてのインタフェースに PIM の設定が必要です。

(b) マルチキャストデータの送信元サーバに関する注意

IPv6 でのマルチキャストデータの送信元サーバに関する注意の内容は、IPv4 と同様です。詳細は、「(1) IPv4 マルチキャストの (b) マルチキャストデータの送信元サーバに関する注意」を参照してください。

3.2.14 VRF 【OP-NPAR】

設定できる VRF 数を次の表に示します。VRF 設定可能数にグローバルネットワークは含みません。

表 3-107 設定できる VRF 数

VRF 動作モード	VRF 設定可能数	説明
設定なし	-	• VRF は動作しません
axrp-enable	63	• IPv4 だけが VRF インスタンスで動作します • Ring Protocol が動作します
l2protocol-disable	249	• IPv4 だけが VRF インスタンスで動作します • レイヤ 2 プロトコルが動作しません
axrp-enable-ipv4-ipv6	63	• IPv4 と IPv6 のどちらも VRF インスタンスで動作します • Ring Protocol が動作します
gsrp-enable-ipv4-ipv6	124	• IPv4 と IPv6 のどちらも VRF インスタンスで動作します • GSRP が動作します
l2protocol-disable-ipv4-ipv6	249	• IPv4 と IPv6 のどちらも VRF インスタンスで動作します • レイヤ 2 プロトコルが動作しません

(凡例) - : 設定できない

3.3 AX6600S の搭載条件【AX6600S】

3.3.1 最大収容ポート数

各モデルの最大収容可能ポート数を次の表に示します。

表 3-108 最大収容可能ポート数

モデル名	イーサネット		
	10GBASE-R	1000BASE-X	10/100/1000BASE-T
AX6604S	32	96	96
AX6608S	64	192	192

3.3.2 最大搭載数

(1) 機器搭載数

各モデルへの冗長化構成を含めた機器最大搭載数を次の表に示します。

表 3-109 機器最大搭載数

機器	AX6604S	AX6608S
CSU	2 (冗長化構成時)	2 (冗長化構成時)
NIF	4	8
PS (AC 電源)	4 (冗長化構成時)	4 (冗長化構成時)
PS (DC 電源)	2 (冗長化構成時)	2 (冗長化構成時)

(2) 電源機構の搭載数

電源機構の最大搭載数は「表 3-109 機器最大搭載数」を参照してください。また、電源機構搭載条件については、マニュアル「コンフィグレーションガイド Vol.2 16. 電源機構 (PS) の冗長化」を参照してください。

(3) NIF 最大搭載数

NIF の種別によって最大搭載数が異なります。NIF 種別ごとの最大搭載数を次に示します。

表 3-110 NIF 種別ごとの最大搭載数

NIF 種別	サイズ	AX6604S	AX6608S
		装置当たり	装置当たり
NK1G-24T	シングル	4	8
NK1G-24S	シングル	4	8
NK1GS-8M	シングル	4	8
NK10G-4RX	シングル	4	8
NK10G-8RX	シングル	4	8

3.4 AX6600S の収容条件【AX6600S】

本節で使用する VLAN ポート数とは各 VLAN に所属するポート数の延べ数の合計です。

例えば、VLAN 1 ~ 100 を設定し、それぞれの VLAN に 2 回線が所属している場合、VLAN ポート数は $100 \times 2 = 200$ となります。

3.4.1 テーブルエントリ数

(1) 概要

本項で使用するテーブルエントリ数とは、経路数やフィルタ・QoS のエントリ数を意味します。

本装置では、ネットワーク構成に合わせ、適切なテーブルエントリ数の配分パターンを選ぶことができます。配分パターンはコンフィグレーションコマンドによって変更できます。

エントリの配分パターンは経路系、フロー系をそれぞれ用意しています。経路系テーブルエントリ、フロー系テーブルエントリ定義を次の表に示します。

表 3-111 経路系テーブルエントリ、フロー系テーブルエントリ内容定義

項目	内容
経路系エントリ	IPv4 ユニキャスト経路 IPv4 マルチキャスト経路 IPv6 ユニキャスト経路 IPv6 マルチキャスト経路 MAC アドレスエントリ ARP NDP
フロー系エントリ	フィルタエントリ (ポリシーベースルーティングおよびポリシーベーススイッチングを含む) QoS エントリ

(2) テーブル容量種別

テーブル容量に対応した名称を次の表に示します。

表 3-112 経路系テーブル容量名称

テーブル容量	対応 CSU
standard	CSU-1A
extended	CSU-1B

表 3-113 フロー系テーブル容量名称

テーブル容量	対応 CSU
standard ¹	CSU-1A
standard-advance ²	
extended ³	CSU-1B
extended-advance ²	

- 注 1 CSU-1A でのデフォルトのテーブル容量です。
 注 2 フロー検出拡張モードを使用する場合に指定します。
 注 3 CSU-1B でのデフォルトのテーブル容量です。

(3) 配分パターン

配分パターンを次の表に示します。

表 3-114 経路系テーブルエントリ配分パターン

パターン名称	意味
default	全エントリ混在
ipv4-uni	IPv4 ユニキャスト主体, マルチキャスト, IPv6 無し
ipv4-ipv6-uni	IPv4 ユニキャスト / IPv6 ユニキャスト主体, マルチキャスト無し
vlan	L2 主体, マルチキャスト無し

注 デフォルトのパターン

表 3-115 standard および standard-advance のフロー系テーブルエントリ配分パターン

パターン名称	意味
default	フィルタ, QoS 均等

注 デフォルトのパターン

表 3-116 extended および extended-advance のフロー系テーブルエントリ配分パターン

パターン名称	意味
default	フィルタ, QoS 均等
filter-only	フィルタ専用
qos-only	QoS 専用
filter	フィルタ主体
qos	QoS 主体

注 デフォルトのパターン

経路系テーブルエントリ数とフロー系テーブルエントリ数を次の表に示します。

VRF 機能使用時の最大エントリ数は, 全 VRF のエントリ数の合計です。

本項表中の「k」の単位は 1024 です。例えば, 24k は $24 \times 1024 = 24576$ であることを表しています。

表 3-117 standard の経路系テーブルエントリ数

パターン名	IPv4 ユニ キャスト経 路 ¹	IPv4 マル チキャスト 経路	IPv6 ユニ キャスト経 路 ²	IPv6 マル チキャスト 経路	MAC ア ドレス	ARP	NDP
default	32768 (32k)	4000	16384 (16k)	1000	24576 (24k)	12288 (12k)	12288 (12k)
ipv4-uni	65536 (64k)	-	-	-	24576 (24k)	12288 (12k)	-

3. 収容条件

パターン名	IPv4 ユニキャスト経路 ¹	IPv4 マルチキャスト経路	IPv6 ユニキャスト経路 ²	IPv6 マルチキャスト経路	MAC アドレス	ARP	NDP
ipv4-ipv6-uni	32768 (32k)	-	32768 (32k)	-	24576 (24k)	12288 (12k)	12288 (12k)
vlan	8192 (8k)	-	8192 (8k)	-	49152 (48k)	8192 (8k)	8192 (8k)

(凡例) - : 該当なし

注 注 は次表を参照してください。

表 3-118 extended の経路系テーブルエントリ数

パターン名	IPv4 ユニキャスト経路 ¹	IPv4 マルチキャスト経路	IPv6 ユニキャスト経路 ²	IPv6 マルチキャスト経路	MAC アドレス	ARP	NDP
default	65536 (64k)	8000	32768 (32k)	8000	65536 (64k)	24576 (24k)	24576 (24k)
ipv4-uni	212992 (208k)	-	-	-	24576 (24k)	24576 (24k)	-
ipv4-ipv6-uni	106496 (104k)	-	106496 (104k)	-	24576 (24k)	24576 (24k)	24576 (24k)
vlan	8192 (8k)	-	8192 (8k)	-	122880 (120k)	8192 (8k)	8192 (8k)

(凡例) - : 該当なし

注 1 IPv4 ユニキャスト経路数には次の情報が含まれます。

- RIP, OSPF, BGP4, スタティックを合わせたアクティブ経路
- 他 VRF (グローバルネットワークを含む) からインポートされた, アクティブ状態のエクストラネット経路
- IPv4 インタフェース数 × 4 : 直結経路のホスト経路, サブネット経路, ブロードキャスト経路 (ホストアドレスの全情報が 0 と 1 の 2 経路)
- ARP エントリ数
- ループバックインタフェースを指定の場合は 1 経路が加算されます。
VRF でループバックインタフェースを使用する場合は, VRF ごとに 1 経路が加算されます。
- RIP バージョン 2 を使用する場合は 1 経路が加算されます。
VRF で RIP バージョン 2 を使用する場合は, VRF ごとに 1 経路が加算されます。
- OSPF を使用する場合は 2 経路が加算されます。
VRF で OSPF を使用する場合は, VRF ごとに 2 経路が加算されます。
- vrrp でアクセプトモードを設定して, マスタ状態になっている場合は 1 経路が加算されます。
- ここに示した以外に 4 経路を装置固定情報として使用します。
VRF を使用する場合は, VRF ごとに 1 経路を装置固定情報として使用します。

注 2 IPv6 ユニキャスト経路数には次の情報が含まれます。

- RIPng, OSPFv3, BGP4+, スタティックを合わせたアクティブ経路数
- IPv6 インタフェース数 × 5 : 直結経路のグローバルアドレス, リンクローカルアドレスそれぞれのホスト経路およびサブネット経路, 直結経路のリンクローカルマルチキャストアドレス
- NDP エントリ数
- ループバックインタフェースを指定の場合は 1 経路が加算されます。
VRF でループバックインタフェースを使用する場合は, VRF ごとに 1 経路が加算されます。
- vrrp でアクセプトモードを設定して, マスタ状態になっている場合は 1 経路が加算されます。
- ここに示した以外に 1 経路を装置固定情報として使用します。
VRF を使用する場合は, VRF ごとに 1 経路を装置固定情報として使用します。

表 3-119 standard のフロー系エントリ数

パターン名	フィルタ	QoS
default (フィルタ, QoS 均等)	4000	4000

表 3-120 standard-advance のフロー系エントリ数

パターン名	フィルタ	QoS
default (フィルタ, QoS 均等)	2000 (300)	2000

注

括弧内の値は DHCP snooping が有効な場合のフィルタエントリ数です。

表 3-121 extended および extended-advance のフロー系エントリ数

パターン名	フィルタ	QoS
default (フィルタ, QoS 均等)	16000 (6000)	16000
filter-only (フィルタ専用)	32000 (22000)	-
qos-only (QoS 専用)	-	32000
filter (フィルタ主体)	24000 (14000)	8000
qos (QoS 主体)	8000 (4000)	24000

(凡例) - : 該当なし

注

括弧内の値は, extended-advance で DHCP snooping が有効な場合のフィルタエントリ数です。

3.4.2 CSU 経路配分パターン

CSU 経路配分パターンに応じた収容可能な IP ユニキャスト, IP マルチキャストの経路エントリ数, MAC アドレスエントリ数, および IP インタフェース数を次の表に示します。表中の「k」の単位は 1024 です。

(1) CSU-1A (standard) の経路配分パターン

表 3-122 CSU-1A 経路配分パターンと収容経路エントリ数 (その1)

経路配分パターン	IPv4 ユニキャスト					IPv4 マルチキャスト		IPv4 インタフェース数	MAC アドレスエントリ数
	最大経路エントリ数		プロトコル別最大経路エントリ数			PIM-SM/SSM PIM-DM			
	アクティブ/非アクティブの合計	アクティブ	RIP+OS PF	BGP	スタティック	(S,G) エントリ数	インタフェース数		
default	131072 (128k)	32768 (32K)	10000	131072 (128k)	4096	1	1	4096	24576 (24k)
ipv4-uni	262144 (256k)	65536 (64k)	10000	262144 (256k)	4096	-	-	4096	24576 (24k)
ipv4-ipv6-uni	131072 (128k)	32768 (32k)	10000	131072 (128k)	4096	-	-	4096	24576 (24k)
vlan	32768 (32k)	8192	10000	32768 (32k)	4096	-	-	4096	49152 (48k)

(凡例) - : 該当なし

注 注 は次表を参照してください。

表 3-123 CSU-1A 経路配分パターンと収容経路エントリ数 (その2)

経路配分パターン	IPv6 ユニキャスト					IPv6 マルチキャスト		IPv6 インタフェース数
	最大経路エントリ数		プロトコル別最大経路エントリ数			PIM-SM/SSM		
	アクティブ/非アクティブの合計	アクティブ	RIPng+OS PFv3	BGP4+	スタティック	(S,G) エントリ数	インタフェース数	
default	65536 (64k)	16384 (16k)	10000	65536 (64k)	4096	2	2	4096
ipv4-uni	-	-	-	-	-	-	-	-
ipv4-ipv6-uni	131072 (128k)	32768 (32k)	10000	131072 (128k)	4096	-	-	4096
vlan	32768 (32k)	8192	10000	32768 (32k)	4096	-	-	4096

(凡例) - : 該当なし

注 1,2

(S,G) エントリ数とインタフェース数の組み合わせは、次のどれかの組み合わせとなります。IPv4 と IPv6 のマルチキャストに関しては、IPv4 マルチキャストと IPv6 マルチキャストを混在で使用する場合、(S,G) エントリ数とインタフェース数は、IPv4 と IPv6 の合計値が次の表のエントリ数以内となるようにしてください。

注 1 の場合の組み合わせを次の表に示します。

表 3-124 IPv4 マルチキャスト単独使用の場合の (S,G) エントリ数とインタフェース数の組み合わせ

(S,G) エントリ数	インタフェース数
4000	31
2000	63
1000	127

注 2 の場合の組み合わせを次の表に示します。

表 3-125 IPv6 マルチキャスト単独使用, または IPv4/IPv6 マルチキャスト混在使用の場合の (S,G) エントリ数とインタフェース数の組み合わせ

(S,G) エントリ数	インタフェース数
1000	31
500	63
250	127

(2) CSU-1B (extended) の経路配分パターン

表 3-126 CSU-1B 経路配分パターンと収容経路エントリ数 (その 1)

経路配分パターン	IPv4 ユニキャスト					IPv4 マルチキャスト		IPv4 インタフェース数	MAC アドレスエントリ数
	最大経路エントリ数		プロトコル別最大経路エントリ数			PIM-SM/SSM PIM-DM			
	アクティブ/非アクティブの合計	アクティブ	RIP+OSPF	BGP	スタティック	(S,G) エントリ数	インタフェース数		
default	262144 (256k)	65536 (64K)	10000	262144 (256k)	4096			4096	65536 (64k)
ipv4-uni	851968 (832k)	212992 (208k)	10000	851968 (832k)	4096	-	-	4096	24576 (24k)
ipv4-ipv6-uni	425984 (416k)	106496 (104k)	10000	425984 (416k)	4096	-	-	4096	24576 (24k)
vlan	32768 (32k)	8192	10000	32768 (32k)	4096	-	-	4096	122880 (120k)

(凡例) - : 該当なし

注 注 は次表を参照してください。

表 3-127 CSU-1B 経路配分パターンと収容経路エントリ数 (その2)

経路配分パターン	IPv6 ユニキャスト					IPv6 マルチキャスト	IPv6 インタフェース数
	最大経路エントリ数		プロトコル別最大経路エントリ数			PIM-SM/SSM	
	アクティブ/非アクティブの合計	アクティブ	RIPng+OS PFv3	BGP4+	スタティック	(S,G)エントリ数	
default	131072 (128k)	32768 (32k)	10000	131072 (128k)	4096		4096
ipv4-uni	-	-	-	-	-	-	-
ipv4-ipv6-uni	425984 (416k)	106496 (104k)	10000	425984 (416k)	4096	-	4096
vlan	32768 (32k)	8192	10000	32768 (32k)	4096	-	4096

(凡例) - : 該当なし

注

(S,G) エントリ数とインタフェース数の組み合わせは、次のどれかの組み合わせとなります。IPv4 と IPv6 のマルチキャストに関しては、IPv4 マルチキャストと IPv6 マルチキャストを混在で使用する場合、(S,G) エントリ数とインタフェース数は、IPv4 と IPv6 の合計値が次の表のエントリ数以内となるようにしてください。

組み合わせを次の表に示します。

表 3-128 (S,G) エントリ数とインタフェース数の組み合わせ

(S,G) エントリ数	インタフェース数
8000	31
4000	63
2000	127
1000	255

3.4.3 リンクアグリゲーション

コンフィグレーションによって設定できるリンクアグリゲーションの収容条件を次の表に示します。

表 3-129 リンクアグリゲーションの収容条件

モデル	装置当たりの最大チャンネルグループ数	チャンネルグループ当たりの最大ポート数
AX6604S	48	16
AX6608S	63	16

3.4.4 レイヤ 2 スイッチ

(1) MAC アドレステーブル

L2 スイッチ機能では、複数の機能で MAC アドレステーブルを使用しています。例えば、MAC アドレス

の学習機能では、接続された端末の MAC アドレスをダイナミックに学習して MAC アドレステーブルへ登録します。

MAC アドレステーブルの最大エン트리数については、次の表を参照してください。

- 表 3-122 CSU-1A 経路配分パターンと収容経路エン트리数（その 1）
- 表 3-126 CSU-1B 経路配分パターンと収容経路エン트리数（その 1）

MAC アドレステーブルを使用する機能と、その機能による MAC アドレステーブルの使用量を次の表に示します。

表 3-130 MAC アドレステーブルを使用する機能

機能名	使用量
MAC アドレス学習抑止機能	設定した VLAN ごとに 1 エン트리
スタティック MAC アドレス登録機能	登録した MAC アドレスごとに 1 エン트리
スタティック ARP/NDP 登録機能	登録した ARP/NDP エン트리ごとに 1 エン트리
MAC アドレス学習機能 ARP/NDP 学習機能	学習したアドレスごとに 1 エン트리
Ring Protocol 機能	[マスタノード時] リング ID ごとに 2 エン트리 [共有ノード時] リング ID ごとに 1 エン트리
IGMP/MLD snooping 機能（学習）	学習した MAC アドレスごとに 1 エン트리
IGMP snooping 機能	設定した VLAN ごとに 2 エン트리
MLD snooping 機能	設定した VLAN ごとに 8 エン트리
IEEE802.1X	認証済み端末ごとに 1 エン트리
Web 認証機能	認証済み端末ごとに 1 エン트리
MAC 認証機能	認証済み端末ごとに 1 エン트리

注 MAC アドレスと対応する ARP/NDP を学習した場合は合わせて 1 エン트리となります

MAC アドレステーブルのエン트리数が最大エン트리数に達した場合、新たなエントリを登録できなくなるため、上記の収容条件内で運用してください。

運用中は、運用コマンド show system で MAC アドレステーブルの使用状況を確認できます。

(2) MAC アドレス学習

MAC アドレス学習数の収容条件は、「表 3-122 CSU-1A 経路配分パターンと収容経路エン트리数（その 1）」「表 3-126 CSU-1B 経路配分パターンと収容経路エン트리数（その 1）」で示した MAC アドレステーブルの最大エン트리数となります。「表 3-130 MAC アドレステーブルを使用する機能」に示したほかの機能を使用した場合は、ほかの機能で使用した分だけ MAC アドレス学習数の最大数が減少します。

(3) スタティック MAC アドレス登録

スタティック MAC アドレス登録機能の収容条件を次の表に示します。

3. 収容条件

表 3-131 スタティック MAC アドレスの登録数

モデル	装置当たり
AX6600S シリーズ共通	1000

MAC アドレステーブルに空きがない場合は、スタティック MAC アドレス登録機能の最大数まで登録できないことがあります。

(4) VLAN

コンフィグレーションによって設定できる VLAN の数を次の表に示します。

表 3-132 VLAN 数

モデル	装置当たり VLAN	ポート当たり VLAN	VLAN ポート数
AX6600S シリーズ共通	4095	4095	100000

VLAN ポート数が収容条件を超えた場合、CPU の利用率が高くなり、コンフィグレーションコマンドや運用コマンドのレスポンスが遅くなったり、実行できなくなったりすることがあります。

(a) プロトコル VLAN

プロトコル VLAN では、イーサネットフレーム内の Ethernet Type, LLC SAP, および SNAP type フィールドの値を基にプロトコルの識別を行います。コンフィグレーションによって設定できるプロトコル VLAN の収容条件を次の表に示します。

表 3-133 プロトコル VLAN のプロトコルの種類数

モデル	装置当たり	ポート当たり
AX6600S シリーズ共通	16	16

表 3-134 プロトコル VLAN 数

モデル	装置当たり
AX6600S シリーズ共通	96

表 3-135 プロトコルポート数

モデル	装置当たり
AX6600S シリーズ共通	96

(b) MAC VLAN

MAC VLAN の収容条件を次の表に示します。

表 3-136 MAC VLAN の登録 MAC アドレス数

モデル	コンフィグレーションによる最大登録 MAC アドレス数	L2 認証機能による最大登録 MAC アドレス数	コンフィグレーションによる登録数と L2 認証機能による登録数の同時登録最大 MAC アドレス数
AX6600S シリーズ 共通	4096	4096	4096

(c) Tag 変換

コンフィグレーションによって設定できる Tag 変換情報エントリ数を次の表に示します。

表 3-137 Tag 変換情報エントリ数

モデル	装置当たり
AX6600S シリーズ共通	4096

注 Tag 変換情報エントリをポートチャンネルインタフェースに設定する場合、Tag 変換情報エントリ数は該当チャンネルグループのポート数で計算します。

(d) VLAN トンネリング

コンフィグレーションによって設定できる VLAN トンネリングの数を次の表に示します。

表 3-138 VLAN トンネリングの数

モデル	装置当たり
AX6600S シリーズ共通	4095

(e) VLAN 識別テーブル

VLAN 識別テーブルは、フレーム受信時に VLAN を識別するためのテーブルです。プロトコル VLAN、MAC VLAN、および Tag 変換では、VLAN 識別テーブルを使用します。これらの機能を同時に使用する場合は、次の収容条件となります。

ポートごとのプロトコル数 + 登録 MAC アドレス数 + Tag 変換情報エントリ数 4096

ポートごとのプロトコル数

装置内の各プロトコルポートに設定するプロトコル数の合計。リンクアグリゲーションを使用する場合は、ポートチャンネルインタフェースに設定するプロトコル数で計算するため、チャンネルグループの収容ポート数は無関係です。

登録 MAC アドレス数

コンフィグレーションによる MAC アドレス登録数と L2 認証機能による MAC アドレス登録数の合計。

Tag 変換情報エントリ数

コンフィグレーションで設定する Tag 変換情報エントリの数。リンクアグリゲーションを使用する場合は、ポートチャンネルインタフェースに設定する Tag 変換情報エントリ数で計算するため、チャンネルグループの収容ポート数は無関係です。

(5) スパニングツリー

スパニングツリーの収容条件を種類ごとに次の表に示します。

なお、スパニングツリーの VLAN ポート数は、スパニングツリーが動作する VLAN に所属するポート数の延べ数です。チャンネルグループの場合、チャンネルグループ当たりの物理ポート数を数えます。ただし、次の VLAN やポートは、VLAN ポート数に含めません。

- コンフィグレーションコマンド state で suspend パラメータが設定されている VLAN
- VLAN トンネリングを設定しているポート
- BPDU ガード機能を設定しているが、BPDU フィルタ機能を設定していないポート
- PortFast 機能と BPDU フィルタ機能を設定しているアクセスポート

表 3-139 PVST+ の収容条件

モデル	Ring Protocol 共存有無	対象 VLAN 数	VLAN ポート数
AX6600S シリーズ共通	共存なし	250	1000
	共存あり	128	900

表 3-140 シングルスパニングツリーの収容条件

モデル	Ring Protocol 共存有無	対象 VLAN 数	VLAN ポート数	
AX6600S シリーズ 共通	共存なし	4095	シングルだけ	10000
			PVST+ 併用時	5000
	共存あり		シングルだけ	9000
			PVST+ 併用時	4500

注

PVST+ 併用時、PVST+ の VLAN ポート数とシングルスパニングツリーの VLAN ポート数との合計が最大値となります。

表 3-141 マルチプルスパニングツリーの収容条件

モデル	Ring Protocol 共存有無	MST インスタンス数	MST インスタンスごとの対象 VLAN 数	VLAN ポート数
AX6600S シリーズ 共通	共存なし	16	200	10000
	共存あり	16	200	9000

注

MST インスタンス 0 は除きます。MST インスタンス 0 の対象 VLAN 数は 4095 となります。なお、運用中は運用コマンド show spanning-tree port-count で対象 VLAN 数と VLAN ポート数を確認できます。

(6) Ring Protocol

(a) Ring Protocol

Ring Protocol の収容条件を次の表に示します。

表 3-142 Ring Protocol 収容条件

項目	リング当たり	装置当たり
リング数	-	16 ¹
VLAN マッピング数	-	128 ²
VLAN グループ数	2	32
VLAN グループの VLAN 数	4094 ³	4094 ³
リングポート数 ⁴	2	32

(凡例) - : 該当なし

注 1

リングネットワークの構成によっては、最大数の 16 個まで設定できない場合があります。

注 2

Ring Protocol と VRF 機能を併用する (コンフィグレーションコマンド vrf mode の axrp-enable パラメータ, または axrp-enable-ipv4-ipv6 パラメータを設定している) 場合, 装置当たりの VLAN マッピング数は 64 となります。

【OP-NPAR】

注 3

制御 VLAN 用に VLAN を一つ消費するため, VLAN グループに使用できる VLAN 最大数は 4094 となります。

注 4

チャンネルグループの場合は, チャンネルグループ単位で 1 ポートと数えます。

(b) 仮想リンク

仮想リンクの収容条件を次の表に示します。

表 3-143 仮想リンクの収容条件

項目	最大数
装置当たりの仮想リンク ID 数	1
仮想リンク当たりの VLAN 数	1
拠点当たりのリングノード数	2
ネットワーク全体での仮想リンクの拠点数	250

(c) Ring Protocol とスパニングツリーまたは GSRP 併用時の物理ポート数

Ring Protocol とスパニングツリー, または Ring Protocol と GSRP の併用時の収容条件を次の表に示します。なお, リングポートを収容している NIF が対象となります。

表 3-144 Ring Protocol とスパニングツリーまたは GSRP 併用時の収容条件

NIF 略称	使用可能な物理ポート数 ^{1 2}
NK1G-24T	PSP シングルアクト運転の場合, 12 ポートまで
	PSP ダブルアクト運転の場合, すべてのポート
NK1G-24S	PSP シングルアクト運転の場合, 12 ポートまで
	PSP ダブルアクト運転の場合, すべてのポート
NK1GS-8M	すべてのポート
NK10G-4RX	PSP シングルアクト運転の場合, 1 ポートまで

3. 収容条件

NIF 略称	使用可能な物理ポート数 ¹ ²
	PSP ダブルアクト運転の場合、2 ポートまで ³ ⁴
NK10G-8RX	PSP シングルアクト運転の場合、1 ポートまで
	PSP ダブルアクト運転の場合、2 ポートまで ⁴ ⁵

注 1

収容条件を超える物理ポートを使用した場合、常時または一時的にリングポートに高負荷のトラフィックが流れると、仮想リンクの制御フレームが廃棄されるおそれがあります。

注 2

収容条件は、対象 NIF でリングポートを収容した場合に、その NIF で使用可能な物理ポート数の最大となります。

注 3

ポート番号が 1 ~ 2、または 3 ~ 4 のどちらかの範囲で使用してください。

注 4

CSU の冗長性を確保したい場合は、使用する物理ポートを 1 ポートまでで運用してください。

注 5

ポート番号が 1 ~ 2、3 ~ 4、5 ~ 6、または 7 ~ 8 のどれかの範囲で使用してください。

(7) ポリシーベーススイッチング

ポリシーベーススイッチングでは、フィルタのフロー検出を使用して、ポリシーベーススイッチングの対象にするフローを検出します。なお、ポリシーベーススイッチングは、フロー系エントリの配分パターンが qos-only 以外、かつ経路系テーブル容量が extended のときだけ使用できます。

装置当たりのポリシーベーススイッチンググループのエントリ数を次の表に示します。

表 3-145 装置当たりのポリシーベーススイッチンググループのエントリ数

項目	エントリ数
アクセスリストエントリ数	「表 3-148 フィルタ・QoS エントリ数」を参照 ¹
ポリシーベーススイッチングリスト数	1000 ²
ポリシーベーススイッチングリスト情報内に設定できる経路数	8

注 1

エントリ数の算出方法は、「3.4.5 フィルタ・QoS」と同じです。

注 2

1 ポリシーベーススイッチングリスト情報を 1 リストとして登録します。このため、複数のアクセスリストで同一のポリシーベーススイッチングリスト情報を設定した場合、使用するリスト数は 1 リストと計算します。

(8) IGMP snooping / MLD snooping

IGMP snooping の収容条件を次の表に示します。IGMP snooping で学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。登録可能なマルチキャスト MAC アドレス数を次の表に示します。

表 3-146 IGMP snooping 収容条件

モデル	マルチキャスト同時使用	最大数		
		設定 VLAN 数 ¹	収容ポート数 ²	登録エントリ数
AX6600S シリーズ共通 (CSU-1A 搭載時)		256	16	1000
			32	500
			64	250
	×	256	16	2000
			32	1000
			64	500
			128	250
AX6600S シリーズ共通 (CSU-1B 搭載時)		256	32	2000
			64	1000
	×	256	32	4000
			64	2000
			128	1000

(凡例)

: IPv4 マルチキャスト, または IPv6 マルチキャストを同時使用する

×: IPv4 マルチキャスト, または IPv6 マルチキャストを同時使用しない

注 1

snooping が動作するポート数 (snooping 設定 VLAN に収容されるポートの総和) は装置全体で最大 4096 です。例えば, おのおの 10 ポート収容している 128 個の VLAN で snooping を動作させる場合, snooping 動作ポート数は 1280 となります。

注 2

リンクアグリゲーションポートは 1 ポートと数えます。

MLD snooping の収容条件を次の表に示します。MLD snooping で学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。登録可能なマルチキャスト MAC アドレス数を次の表に示します。

表 3-147 MLD snooping 収容条件

モデル	マルチキャスト同時使用	最大数		
		設定 VLAN 数 ¹	収容ポート数 ²	登録エントリ数
AX6600S シリーズ共通 (CSU-1A 搭載時)		256	16	1000
			32	500
			64	250
	×	256	16	2000
			32	1000
			64	500
			128	250
AX6600S シリーズ共通		256	32	2000

3. 収容条件

モデル	マルチキャスト同時使用	最大数		
		設定 VLAN 数 ¹	収容ポート数 ²	登録エントリ数
(CSU-1B 搭載時)			64	1000
	×	256	32	4000
			64	2000
			128	1000

(凡例)

：IPv4 マルチキャスト，または IPv6 マルチキャストを同時使用する

×：IPv4 マルチキャスト，または IPv6 マルチキャストを同時使用しない

注 1

snooping が動作するポート数 (snooping 設定 VLAN に収容されるポートの総和) は装置全体で最大 4096 です。例えば、おのおの 10 ポート収容している 128 個の VLAN で snooping を動作させる場合、snooping 動作ポート数は 1280 となります。

注 2

リンクアグリゲーションポートは 1 ポートと数えます。

3.4.5 フィルタ・QoS

(1) フィルタ・QoS

フィルタおよび QoS の収容条件を示します。ここでのエントリ数とは、コンフィグレーション (access-list, qos-flow-list) で設定したリストを装置内部で使用する形式 (エントリ) に変換したあとの数です。

(a) フィルタ・QoS エントリ数

フィルタ，および QoS の最大エントリ数を次の表に示します。

表 3-148 フィルタ・QoS エントリ数

モデル	フィルタの最大エントリ数		QoS の最大エントリ数	
	入出力インタフェース当たり	装置当たり	入出力インタフェース当たり	装置当たり
AX6600S シリーズ共通 (CSU-1A 搭載時)	4000	4000	4000	4000
AX6600S シリーズ共通 (CSU-1B 搭載時)	32000	32000	32000	32000

フロー制御はフローコンフィグレーションで設定しますが、リストに設定するフロー検出条件パラメータによって使用するエントリ数が異なります。複数エントリを使用するフロー検出条件のパラメータを次の表に示します。

表 3-149 複数エントリを使用するフロー検出条件

複数エントリを使用する フロー検出条件のパラメータ	使用エントリ数算出例
宛先 IPv4 アドレス, 送信元 IPv4 アドレス, 宛先 IPv6 アドレスを範囲指定	指定された IP アドレスが幾つのサブネットに区切られるかによってエントリ数が決定。 例えば, 宛先 IPv4 アドレスに 192.168.0.1 - 192.168.0.4 と指定した場合, 192.168.0.1/32, 192.168.0.2/31, 192.168.0.4/32 の三つのサブネットに区切られるため, 3 エントリとなります。
宛先ポート番号を範囲指定, 送信元ポート番号を範囲指定	指定された値が最大 16 ビットのマスクで区切ったときに幾つに分けられるかによってエントリ数が決定。 例えば, 宛先ポート番号に 135 - 140 と指定した場合, <ul style="list-style-type: none"> 135/16 = 0000 0000 1000 0111 (2 進表記) 136/14 = 0000 0000 1000 10xx (2 進表記) 140/16 = 0000 0000 1000 1100 (2 進表記) の三つの領域に区切られるため, 3 エントリとなります。
VLAN ID を複数指定	指定された VLAN ID 複数指定の中で, 次に示す総和をエントリ数とします。 <ul style="list-style-type: none"> 各単数指定部分: 1 エントリ。 各範囲指定部分: 前項と同様の方式で最大 12 ビットとして算出したエントリ数。 例えば, 1, 4-7, 16-18 と指定した場合, 1:1/12 = 0000 0000 0001(2 進表記) 4-7:4/10 = 0000 0000 01xx(2 進表記) 16-18:16/11 = 0000 0001 000x(2 進表記) 18/12 = 0000 0001 0010(2 進表記) のエントリとなります。
TCP セッション維持 (ack フラグが ON, または rst フラグが ON のパケット検出)	2 エントリ使用します。

1 リストに上記のフロー検出条件を複数指定した場合, おおのこのフロー検出条件で使用するエントリ数を掛け合わせた値が, 1 リストで使用するエントリ数となります。

1 リストに上記のフロー検出条件を一つ指定した場合は, 指定したフロー検出条件で使用するエントリ数が 1 リストで使用するエントリ数となります。

二つ以上指定した場合は, おおのこのフロー検出条件で使用するエントリ数を掛け合わせた値が, 1 リストで使用するエントリ数となります。

上記のフロー検出条件を指定していない場合は, 1 リストで使用するエントリ数は 1 エントリとなります。

(b) 帯域監視機能でのエントリ数

帯域監視機能のエントリ数は, ストームコントロール機能と併用です。帯域監視モードと動作概要を次の表に示します。

表 3-150 帯域監視モードと動作概要

帯域監視モード	モード指定時の帯域監視機能の動作概要
upc-in-and-storm-control	<ul style="list-style-type: none"> 帯域監視は受信側にだけ設定可 一つのフローエントリごとに, 最大帯域制御または最低帯域監視のどちらかを設定可 ストームコントロール機能が使用可能
upc-in-in	<ul style="list-style-type: none"> 帯域監視は受信側にだけ設定可 一つのフローエントリで最大帯域制御と最低帯域監視の同時監視可 ストームコントロール機能は使用不可

3. 収容条件

帯域監視モード	モード指定時の帯域監視機能の動作概要
upc-in-out	<ul style="list-style-type: none"> 帯域監視を受信側および送信側に設定可 一つのフローエントリごとに、最大帯域制御または最低帯域監視のどちらかを設定可 ストームコントロール機能は使用不可

各モードの帯域監視機能の収容条件を次の表に示します。

表 3-151 装置当たりの帯域監視機能のエントリ数

帯域監視モード	帯域監視機能でのエントリ数	ストームコントロール機能
upc-in-and-storm-control	744	
upc-in-in	1000	×
upc-in-out	1000	×

(凡例) :有効 ×:無効

1 リストに指定した帯域監視機能の内容によって、1 リストで使用するエントリ数が異なります。その内容を次の表に示します。

表 3-152 1 リストで使用する帯域監視機能のエントリ数

1 リストに指定した帯域監視機能	使用エントリ数
最大帯域制御だけ	1
最低帯域監視だけ	1
最大帯域制御と最低帯域監視の両方を指定	2

(c) 階層化シェーパ

階層化シェーパのユーザ数の収容条件を次の表に示します。

表 3-153 階層化シェーパの最大ユーザ数

モデル	回線当たりの最大ユーザ数	装置当たりの最大ユーザ数
AX6600S シリーズ共通	1024	32768

注 デフォルトユーザを含む数です。

(2) アクセスリストロギング

アクセスリストロギングの収容条件を示します。

アクセスリストロギングの最大アクセスリストログ情報数を次の表に示します。

表 3-154 最大アクセスリストログ情報数

モデル	最大アクセスリストログ情報数
AX6600S シリーズ共通 (CSU-1A 搭載時)	2000
AX6600S シリーズ共通 (CSU-1B 搭載時)	4000

3.4.6 レイヤ 2 認証

(1) レイヤ 2 認証

レイヤ 2 認証共通の収容条件を次の表に示します。

表 3-155 認証専用 IPv4 アクセスリストに設定できるフィルタ条件数

モデル	認証専用 IPv4 アクセスリストに設定できるフィルタ条件数
AX6600S シリーズ共通	10

(2) IEEE802.1X

IEEE802.1X の収容条件を次に示します。

本装置の IEEE802.1X では、三つの認証モードをサポートしています。

- ポート単位認証
- VLAN 単位認証（静的）
- VLAN 単位認証（動的）

VLAN 単位認証を使用する場合の、IEEE802.1X を設定可能な装置当たりの総ポート数を次の表に示します。

表 3-156 IEEE802.1X を設定可能な装置当たりの総ポート数

モデル	IEEE802.1X を設定可能な装置当たりの総ポート数
AX6600S シリーズ共通	1024

注

IEEE802.1X を設定可能な装置当たりの総ポート数とは、VLAN 単位認証を設定した VLAN での VLAN ポート数の総和の最大値を指します。VLAN 内にチャンネルグループが含まれている場合は、チャンネルグループを構成する物理ポート数に関係なく、チャンネルグループを 1 ポートとして計算します。また、1 ポートに VLAN が Tag で多重化されている場合も個別に数えます。例えば、一つのポートに Tag で多重化された 10 個の VLAN が設定されていた場合、その 10 個の VLAN で VLAN 単位認証を動作させると、総ポート数は 10 ポートになります。

各認証モードでの単位当たりの最大認証端末数を次の表に示します。

表 3-157 各認証モードでの単位当たりの最大認証端末数

モデル	認証モード		
	ポート単位認証	VLAN 単位認証 （静的）	VLAN 単位認証 （動的）
AX6600S シリーズ共通	256 / ポート	256 / VLAN	4096 / 装置

注

IEEE802.1X (VLAN 単位認証 (動的)), Web 認証 (ダイナミック VLAN モード) および MAC 認証 (ダイナミック VLAN モード) を同時に動作させた場合は、それぞれの認証端末数の合計で装置当たり 4096 までとなります。

本装置の最大認証端末数を次の表に示します。

3. 収容条件

表 3-158 本装置の最大認証端末数

モデル	3モード合計での最大認証端末数
AX6600S シリーズ共通	4096 / 装置

注

IEEE802.1X (ポート単位認証および VLAN 単位認証 (静的)), Web 認証 (固定 VLAN モード) および MAC 認証 (固定 VLAN モード) を同時に動作させた場合は, それぞれの認証端末数の合計で装置当たり 4096 までとなります。

(3) Web 認証

Web 認証の収容条件を次の表に示します。

表 3-159 Web 認証 (固定 VLAN モード) の最大認証端末数

モデル	装置当たりの最大認証端末数
AX6600S シリーズ共通	4096

注

Web 認証 (固定 VLAN モード), IEEE802.1X (ポート単位認証および VLAN 単位認証 (静的)) および MAC 認証 (固定 VLAN モード) を同時に動作させた場合は, それぞれの認証端末数の合計で装置当たり 4096 までとなります。

表 3-160 Web 認証 (ダイナミック VLAN モード) の最大認証端末数

モデル	装置当たりの最大認証端末数
AX6600S シリーズ共通	4096

注

Web 認証 (ダイナミック VLAN モード), IEEE802.1X (VLAN 単位認証 (動的)) および MAC 認証 (ダイナミック VLAN モード) を同時に動作させた場合は, それぞれの認証端末数の合計で装置当たり 4096 までとなります。

表 3-161 Web 認証 (レガシーモード) の最大認証端末数

モデル	装置当たりの最大認証端末数
AX6600S シリーズ共通	4096

注

Web 認証 (レガシーモード) および IEEE802.1X (VLAN 単位認証 (動的)) を同時に動作させた場合は, それぞれの認証端末数の合計で装置当たり 4096 までとなります。

表 3-162 Web 認証の装置当たりの内蔵 Web 認証 DB 登録ユーザ数

モデル	装置当たりの内蔵 Web 認証 DB 登録ユーザ数
AX6600S シリーズ共通	300

注

内蔵 Web 認証 DB に登録したユーザ ID を複数の端末で使用すると, 最大認証端末数まで端末を認証できます。ただし, 認証対象となるユーザ ID の数が内蔵 Web 認証 DB の最大登録数より多い場合は, RADIUS サーバを用いた RADIUS 認証方式を使用してください。

表 3-163 Web 認証の画面入れ替えで指定できる認証画面ファイル合計サイズ

モデル	装置当たりの指定できる認証画面ファイルの合計サイズ
AX6600S シリーズ共通	1024K バイト

表 3-164 Web 認証の画面入れ替えで指定できる認証画面ファイル数

モデル	装置当たりの指定できる認証画面ファイル数
AX6600S シリーズ共通	100

(4) MAC 認証

MAC 認証の収容条件を次の表に示します。

表 3-165 MAC 認証 (固定 VLAN モード) の最大認証端末数

モデル	装置当たりの最大認証端末数
AX6600S シリーズ共通	4096

注

MAC 認証 (固定 VLAN モード), IEEE802.1X (ポート単位認証および VLAN 単位認証 (静的)) および Web 認証 (固定 VLAN モード) を同時に動作させた場合は, それぞれの認証端末数の合計で 4096 までとなります。

表 3-166 MAC 認証 (ダイナミック VLAN モード) の最大認証端末数

モデル	装置当たりの最大認証端末数
AX6600S シリーズ共通	4096

注

MAC 認証 (ダイナミック VLAN モード), IEEE802.1X (VLAN 単位認証 (動的)) および Web 認証 (ダイナミック VLAN モード) を同時に動作させた場合は, それぞれの認証端末数の合計で 4096 までとなります。

表 3-167 MAC 認証の装置当たりの内蔵 MAC 認証 DB 登録ユーザ数

モデル	装置当たりの内蔵 MAC 認証 DB 登録ユーザ数
AX6600S シリーズ共通	1024

注

内蔵 MAC 認証 DB を使用した場合で VLAN ID をチェックしないときは, 認証対象となる MAC アドレスと VLAN ID 数 (Tag 使用時の VLAN ID 数も含む) の組み合わせ合計数が最大認証端末数に到達するまで端末を認証できます。ただし, 認証する端末 (MAC アドレス) と VLAN ID の組み合わせ合計数が内蔵 MAC 認証 DB の最大登録数より多い場合は, RADIUS サーバを用いた RADIUS 認証方式を使用してください。

(5) 認証 VLAN

認証 VLAN の収容条件を次の表に示します。

表 3-168 最大認証端末数

モデル	装置当たりの最大認証端末数
AX6600S シリーズ共通	4096

3. 収容条件

表 3-169 接続可能な認証サーバ数

モデル	装置当たりの接続可能な認証サーバ数
AX6600S シリーズ共通	10

表 3-170 設定可能な認証済み VLAN 数

モデル	装置当たりの設定可能な認証済み VLAN 数
AX6600S シリーズ共通	4094

3.4.7 DHCP snooping

DHCP snooping の収容条件を次の表に示します。

表 3-171 DHCP snooping の最大エントリ数

フロー系テーブル容量名称	フロー系テーブルエントリ配分パターン	バインディングデータベースエントリ数 ¹		端末フィルタエントリ数 ²
		ダイナミック/スタティックの合計	スタティック	
standard	default (フィルタ, QoS 均等)	-	-	-
standard-advance	default (フィルタ, QoS 均等)	1100	256	1100
extended	default (フィルタ, QoS 均等)	-	-	-
	filter-only (フィルタ専用)	-	-	-
	qos-only (QoS 専用)	-	-	-
	filter (フィルタ主体)	-	-	-
	qos (QoS 主体)	-	-	-
extended-advance	default (フィルタ, QoS 均等)	8000	1024	8000
	filter-only (フィルタ専用)	8000	1024	8000
	qos-only (QoS 専用)	-	-	-
	filter (フィルタ主体)	8000	1024	8000
	qos (QoS 主体)	2000	1024	2000

(凡例) - : DHCP snooping は使用できない

注 1

untrust ポート配下の端末当たり 1 エントリを消費します。

注 2

バインディングデータベースエントリ配下のポート当たり 1 エントリを消費します。
チャンネルグループの場合、チャンネルグループ当たりのポート数を数えます。

表 3-172 DHCP snooping の最大 VLAN 数

フロー系テーブル容量名称	最大 VLAN 数
standard	-

フロー系テーブル容量名称	最大 VLAN 数
standard-advance	512
extended	-
extended-advance	2048

(凡例) - : DHCP snooping は使用できない

3.4.8 冗長化構成による高信頼化

(1) GSRP

GSRP の収容条件を次の表に示します。

GSRP の VLAN ポート数は、チャンネルグループの場合、チャンネルグループ当たりの物理ポート数を数えます。

表 3-173 GSRP 収容条件

モデル	レイヤ 3 冗長機能	VLAN ポート数の合計	VLAN グループ最大数	VLAN グループ当たりの VLAN 最大数
AX6600S シリーズ 共通	あり	10000	128	4095
	なし	100000	128	4095

注

GSRP と VRF 機能を併用する (コンフィギュレーションコマンド `vrf mode` の `gsrp-enable-ipv4-ipv6` パラメータを設定している) 場合、VLAN グループ当たりの VLAN 最大数は 250 となります。【OP-NPAR】

(2) VRRP

VRRP に関する収容条件を次の表に示します。

表 3-174 VRRP 収容条件

モデル	仮想ルータ最大数		track 設定最大数	track 割り当て最大数	
	インタフェース当たり	装置当たり		仮想ルータ当たり	装置当たり
AX6600S シリーズ 共通	255 ¹	255 ¹	255	16 ²	255 ²

注 1 IPv4/IPv6 の仮想ルータの合計数です。

注 2 障害監視インタフェースと VRRP ボーリングの合計数です。

表 3-175 VRRP 収容条件 (グループ切替機能使用時)

モデル	仮想ルータ最大数		最大グループ数	1グループ当たりの最大フォロ-仮想ルータ数	track 設定最大数	track 割り当て最大数	
	インタフェース当たり	装置当たり				仮想ルータ当たり	装置当たり
AX6600S シリーズ共通	255 ¹	4095 ¹	255	4094	255	16 ²	255 ²

注 1 IPv4/IPv6 の仮想ルータの合計数は 255 までです。ただし、グループ切替機能を利用し、フォロ-仮想ルータを作成することで、最大 4095 の仮想ルータが動作できます。

注 2 障害監視インタフェースと VRRP ボーリングの合計数です。

3.4.9 ネットワークの障害検出による高信頼化機能

(1) IEEE802.3ah/UDLD

IEEE802.3ah/UDLD の収容条件を次の表に示します。

表 3-176 設定可能ポート数

モデル	設定可能ポート数
AX6604S	96
AX6608S	192

(2) L2 ループ検知

(a) L2 ループ検知フレーム送信レート

L2 ループ検知の L2 ループ検知フレーム送信レートを次の表に示します。

表 3-177 L2 ループ検知フレーム送信レート

モデル	L2 ループ検知フレームの送信レート (装置当たり) ¹	
	スパニングツリー, GSRP, Ring Protocol のどれかを使用している場合	スパニングツリー, GSRP, Ring Protocol のどれも使用していない場合
AX6600S シリーズ共通	90pps (推奨値) ²	600pps (最大値) ³

- L2 ループ検知フレーム送信レート算出式

L2 ループ検知フレーム送信対象の VLAN ポート数 ÷ L2 ループ検知フレームの送信レート (pps) × 送信間隔 (秒)

注 1

送信レートは上記の条件式に従って、自動的に 600pps 以内で変動します。

注 2

スパニングツリー, GSRP, Ring Protocol のどれかを使用している場合は、90pps 以下に設定してください。90pps より大きい場合、スパニングツリー, GSRP, Ring Protocol の正常動作を保障できません。

注 3

600pps を超えるフレームは送信しません。送信できなかったフレームに該当するポートや VLAN ではループ障害を検知できなくなります。必ず 600pps 以下に設定してください。

(b) ネットワーク全体での動作可能装置数

ネットワーク全体で本機能が動作可能な装置台数は、AX6700S シリーズ、AX6600S シリーズ、AX6300S シリーズの合計で 64 台までです。

(c) 物理ポート数

L2 ループ検知を運用時の物理ポート数の収容条件を次の表に示します。

表 3-178 物理ポートの収容条件

NIF 略称	使用可能な物理ポート数 ¹
NK1G-24T	PSP シングルアクト運転の場合、12 ポートまで
	PSP ダブルアクト運転の場合、すべてのポート
NK1G-24S	PSP シングルアクト運転の場合、12 ポートまで
	PSP ダブルアクト運転の場合、すべてのポート
NK1GS-8M	すべてのポート
NK10G-4RX	PSP シングルアクト運転の場合、1 ポートまで
	PSP ダブルアクト運転の場合、2 ポートまで ^{2 3}
NK10G-8RX	PSP シングルアクト運転の場合、1 ポートまで
	PSP ダブルアクト運転の場合、2 ポートまで ^{3 4}

注 1

収容条件を超える物理ポートを使用した場合、常時または一時的に高負荷のトラフィックが流れると、L2 ループ検知フレームが廃棄されるおそれがあります。廃棄されることでループ障害の検知が遅れる場合があります。

注 2

ポート番号が 1 ~ 2、または 3 ~ 4 のどちらかの範囲で使用してください。

注 3

CSU の冗長性を確保したい場合は、使用する物理ポートを 1 ポートまでで運用してください。

注 4

ポート番号が 1 ~ 2、3 ~ 4、5 ~ 6、または 7 ~ 8 のどれかの範囲で使用してください。

(3) CFM

CFM の収容条件を次の表に示します。

表 3-179 CFM の収容条件

モデル	ドメイン数	MA 数	MEP 数	MIP 数	CFM ポート 総数 ^{1 2}	リモート MEP 総数 ^{2 3}
AX6600S シ リーズ共通	8 / 装置	192 / 装置	192 / 装置	192 / 装置	1024 / 装 置	8064 / 装置

注 1

CFM ポート総数とは、MA のプライマリ VLAN のうち、CFM のフレームを送信する VLAN ポートの総数です。

Down MEP だけの MA の場合

Down MEP の VLAN ポートの総数

3. 収容条件

Up MEP を含む MA の場合

プライマリ VLAN の全 VLAN ポートの総数

なお、CFM ポート総数は運用コマンド `show cfm summary` で確認できます。

注 2

CFM ポート総数およびリモート MEP 総数は、CCM 送信間隔がデフォルト値のときの収容条件です。CCM 送信間隔を変更すると、CFM ポート総数およびリモート MEP 総数の収容条件が変わります。CCM 送信間隔による CFM ポート総数およびリモート MEP 総数の収容条件を次の表に示します。

表 3-180 CCM 送信間隔による収容条件

モデル	CCM 送信間隔	CFM ポート総数	リモート MEP 総数
AX6600S シリーズ共通	1 分以上	1024 / 装置	8064 / 装置
	10 秒	256 / 装置	4032 / 装置
	1 秒	192 / 装置	400 / 装置

注 3

リモート MEP 総数とは、自装置以外の MEP の総数です。MEP からの CCM 受信性能に影響しません。リモート MEP 総数は運用コマンド `show cfm remote-mep` で確認できます。

表 3-181 CFM の物理ポートおよびチャネルグループの収容条件

モデル	MEP・MIP を設定可能な物理ポートおよびチャネルグループの総数
AX6600S シリーズ 共通	全ポート

注

MEP・MIP は同一ポートに対して複数設定できます。チャネルグループの場合は、チャネルグループ単位で 1 ポートと数えます。

表 3-182 CFM のデータベース収容条件

モデル	MEP CCM データベース エントリ数	MIP CCM データベース エントリ数	Linktrace データベース エントリ数
AX6600S シリーズ共通	63 / MEP	12288 / 装置	1024 / 装置

注

1 ルート当たり 256 装置の情報を保持する場合は、最大で 4 ルート分を保持します (1024 ÷ 256 装置 = 4 ルート)。

3.4.10 隣接装置情報の管理 (LLDP/OADP)

隣接装置情報 (LLDP/OADP) の収容条件を次の表に示します。

表 3-183 隣接装置情報 (LLDP/OADP) の収容条件

モデル	LLDP 隣接装置情報	OADP 隣接装置情報
AX6600S シリーズ共通	192	250

注

LLDP/OADP の隣接装置情報数とは、本装置に接続されている隣接装置から収集できる情報のことで、基本的に 1 隣接装置当たり 1 情報を収集できます。

3.4.11 IPv4・IPv6 パケット中継

(1) IP アドレスを設定できるインタフェース数

本装置は次のインタフェースに IP アドレスを設定できます。

- VLAN インタフェース
- マネージメントポート

ここでは、IP アドレスを設定できるインタフェースの最大数について説明します。また、設定できる IP アドレスの最大数について説明します。

インタフェースに対してサポートする最大インタフェース数を次の表に示します。ここで示す値は、IPv4 と IPv6 との合計の値です。なお、IPv4 と IPv6 を同一のインタフェースに設定することも、個別に設定することもできます。

表 3-184 インタフェースに対する最大インタフェース数

モデル	VLAN インタフェース数 (装置当たり)	マネージメントポート (装置当たり)
AX6600S シリーズ共通	4095	1

(2) マルチホームの最大サブネット数

LAN のマルチホーム接続では一つのインタフェースに対して、複数の IPv4 アドレス、または IPv6 アドレスを設定できます。

(a) IPv4 の場合

IPv4 でのマルチホームの最大サブネット数を次の表に示します。ただし、マネージメントポートは IPv4 のマルチホーム不可のため 1 になります。

表 3-185 マルチホームの最大サブネット数 (IPv4 の場合)

モデル	マルチホーム サブネット数 (インタフェース当たり)
AX6600S シリーズ共通	256

(b) IPv6 の場合

IPv6 でのマルチホームの最大サブネット数を次の表に示します。なお、ここで示す値にはリンクローカルアドレスを含みます。一つのインタフェースには必ず一つのリンクローカルアドレスが設定されます。このため、すべてのインタフェースで IPv6 グローバルアドレスだけを設定した場合、実際に装置に設定される IPv6 アドレス数は、表の数値に自動生成される IPv6 リンクローカルアドレス数 1 を加算した 8 にな

ります。

表 3-186 マルチホームの最大サブネット数 (IPv6 の場合)

モデル	マルチホーム サブネット数 (インタフェース当たり)
AX6600S シリーズ共通	7

(3) IP アドレス最大設定数

(a) IPv4 アドレス

コンフィグレーションで設定できる IPv4 アドレスの最大数を次の表に示します。なお、この表で示す値は、インタフェースに設定できる IPv4 アドレス数です。

表 3-187 コンフィグレーションで装置に設定できる IPv4 アドレスの最大数

モデル	VLAN インタフェースに設定できる IPv4 アドレス数 (装置当たり)	マネージメントポートに設定できる IPv4 アドレス数 (装置当たり)
AX6600S シリーズ共通	4096	1

(b) IPv6 アドレス

コンフィグレーションで設定できる装置当たりの IPv6 アドレスの最大数を次の表に示します。なお、ここで示す値はインタフェースに設定する IPv6 アドレスの数です。また、IPv6 リンクローカルアドレスの数も含まれます。一つのインタフェースには必ず一つの IPv6 リンクローカルアドレスが設定されます。このため、すべてのインタフェースに IPv6 グローバルアドレスを設定した場合、インタフェースには自動で IPv6 リンクローカルアドレスが付与され、実際に装置に設定される IPv6 アドレスの数は次の表に示す値となります。

表 3-188 コンフィグレーションで装置に設定できる IPv6 アドレスの最大数

モデル	VLAN インタフェースに設定できる IPv6 アドレス数 (装置当たり)	マネージメントポートに設定できる IPv6 アドレス数 (装置当たり)
AX6600S シリーズ共通	4096	7

表 3-189 VLAN インタフェースに設定される IPv6 アドレス数

コンフィグレーションで VLAN インタフェースに設定する IPv6 アドレスの数		自動で設定する IPv6 リンク ローカルアドレスの数	VLAN インタフェースに 設定される IPv6 アドレス 数
IPv6 リンクローカルアド レス	IPv6 グローバルアドレ ス		
4095	0	0	4095
0	4096	4095	8191

注 IPv6 グローバルアドレスは、マルチホームを使用することで 4096 まで設定できます。

表 3-190 マネージメントポートに設定される IPv6 アドレス数

コンフィグレーションでマネージメントポートに設定する IPv6 アドレスの数		自動で設定する IPv6 リンクローカルアドレスの数	マネージメントポートに設定される IPv6 アドレス数
IPv6 リンクローカルアドレス	IPv6 グローバルアドレス		
1	0	0	1
0	7	1	8

(4) 最大相手装置数

本装置が接続する通信可能な最大相手装置数を示します。この場合の相手装置はスイッチに限らず、端末も含まれます。

(a) ARP エントリ数

IPv4 の場合、ARP によって、送信しようとするパケットの宛先アドレスに対応するハードウェアアドレスを決定します。最大相手装置数は、ARP エントリ数によって決まります。ARP エントリはコンフィグレーションコマンドを使用することで、スタティックに 4096 エントリ登録できます。本装置でサポートする ARP エントリの最大数については、次の表を参照してください。最大エントリ数は、スタティックで登録したエントリ数を含みます。

- 表 3-117 standard の経路系テーブルエントリ数
- 表 3-118 extended の経路系テーブルエントリ数

(b) NDP エントリ数

IPv6 の場合、NDP でのアドレス解決によって、送信しようとするパケットの宛先アドレスに対応するハードウェアアドレスを決定します。最大相手装置数は NDP エントリ数によって決まります。NDP エントリは、コンフィグレーションコマンドを使用することで、スタティックに 4096 エントリ登録できます。本装置でサポートする NDP エントリの最大数については、次の表を参照してください。最大エントリ数は、スタティックで登録したエントリ数を含みます。

- 表 3-117 standard の経路系テーブルエントリ数
- 表 3-118 extended の経路系テーブルエントリ数

(c) RA の最大相手端末数

RA ではルータから通知される IPv6 アドレス情報を基に端末でアドレスを生成します。本装置での最大相手端末数を次の表に示します。

表 3-191 RA の最大相手端末数

モデル	RA の最大相手端末数	
	インタフェース当たり	装置当たり
AX6600S シリーズ共通	4096	4096

(5) ポリシーベースルーティング

ポリシーベースルーティングでは、フィルタのフロー検出を使用して、ポリシーベースルーティングの対象にするフローを検出します。なお、フロー系エントリの配分パターンが qos-only の場合、ポリシーベースルーティングは使用できません。

3. 収容条件

(a) ポリシーベースルーティングの収容条件

アクセスリストの動作に中継先の経路を指定

アクセスリストの動作に中継先の経路を指定する場合の収容条件を次の表に示します。

表 3-192 装置当たりのポリシーベースルーティングのエントリ数

項目	IPv4 ポリシーベースルーティング	IPv6 ポリシーベースルーティング
アクセスリストエントリ数	「表 3-148 フィルタ・QoS エントリ数」を参照 ¹	「表 3-148 フィルタ・QoS エントリ数」を参照 ¹
ネクストホップエントリ数	256 ²	256 ²

注 1

エントリ数の算出方法は、「3.4.5 フィルタ・QoS」と同じです。

注 2

1 ネクストホップを 1 エントリとして登録します。このため、複数のアクセスリストで同一のネクストホップを設定した場合、使用するエントリ数は 1 エントリと計算します。

アクセスリストの動作にポリシーベースルーティングリスト情報を指定

アクセスリストの動作にポリシーベースルーティングリスト情報を指定する場合の収容条件を次の表に示します。

表 3-193 装置当たりのポリシーベースルーティンググループのエントリ数

項目	IPv4 ポリシーベースルーティンググループ	IPv6 ポリシーベースルーティンググループ
アクセスリストエントリ数	「表 3-148 フィルタ・QoS エントリ数」を参照 ¹	-
ポリシーベースルーティングリスト数	256 ²	-
ポリシーベースルーティングリスト情報内に設定できる経路数	8	-
ポリシーベースルーティングのトラッキング機能と連携できる経路数	1024 ³	-

(凡例) - : 該当なし

注 1

エントリ数の算出方法は、「3.4.5 フィルタ・QoS」と同じです。

注 2

1 ポリシーベースルーティングリスト情報を 1 リストとして登録します。このため、複数のアクセスリストで同一のポリシーベースルーティングリスト情報を設定した場合、使用するリスト数は 1 リストと計算します。

注 3

1 トラック ID を 1 エントリとして登録します。このため、複数の経路で同一のトラック ID を設定した場合、使用するエントリ数は 1 エントリと計算します。

(b) トラッキング機能の収容条件

ポリシーベースルーティングのトラッキング機能の収容条件を次の表に示します。

表 3-194 トラッキング機能の収容条件

項目	収容条件
トラックの数	1024
ポーリング監視トラックの数	1024

注 コンフィグレーションコマンド `type icmp` を設定したトラックの数です。

(6) DHCP/BOOTP リレー

DHCP/BOOTP リレーの収容条件を次の表に示します。

表 3-195 DHCP/BOOTP リレーの最大数

モデル	クライアント接続インタフェース数	サーバ台数 (グローバルネットワーク, VRF ごと)	VRF 使用時の装置 当たりのサーバ台数
AX6600S シリーズ共通	2048	16	256

(7) IPv6 DHCP リレー

IPv6 DHCP リレーの収容条件を次の表に示します。

表 3-196 IPv6 DHCP リレーの最大数

モデル	装置当たりの最大数	
	配布プレフィックス数	インタフェース数
AX6600S シリーズ共通	1024	1024

注

クライアントを直接収容した場合に IPv6 DHCP サーバによって配布される PD プレフィックス数です。ほかのリレー経由の packets や PD プレフィックス以外の情報は、この条件に関係なく中継できます。

(8) DHCP サーバ

DHCP サーバで設定できるインタフェース数および配布可能 IP アドレス数などを次の表に示します。

表 3-197 DHCP サーバの最大数

モデル	最大配布可能 IP アドレス数	最大固定 IP アドレス割り当て数	最大インタフェース数	最大管理サブネット数
AX6600S シリーズ共通	8192	320	2048	2048

(9) IPv6 DHCP サーバ

IPv6 DHCP サーバの収容条件を次の表に示します。

表 3-198 IPv6 DHCP サーバの最大数

モデル	装置当たりの最大数	
	インタフェース数	最大配布可能 Prefix
AX6600S シリーズ共通	1024	1024

3.4.12 IPv4・IPv6 ルーティングプロトコル

(1) 最大隣接ルータ数

最大隣接ルータ数の定義を次の表に示します。

表 3-199 最大隣接ルータ数の定義

ルーティングプロトコル別	最大隣接ルータ数の定義
スタティックルーティング	ネクストホップ・アドレスの数
RIP, RIPng	RIP/RIPng が動作するインタフェース数
OSPF, OSPFv3	本装置が OSPF/OSPFv3 指定ルータ (DR, BDR) になるネットワークの場合、そのネットワーク上のそのほかすべての OSPF/OSPFv3 ルータ数。本装置が OSPF/OSPFv3 指定ルータにならないネットワークの場合、そのネットワーク上の指定ルータ (DR, BDR) 数。
BGP4, BGP4+	BGP4/BGP4+ ピア数

最大隣接ルータ数を次の表に示します。

表 3-200 最大隣接ルータ数

ルーティングプロトコル	最大隣接ルータ数	
	ポリシーベースルーティングのトラッキング機能を使用しない	ポリシーベースルーティングのトラッキング機能を使用する
スタティックルーティング (IPv4, IPv6 の合計)	4096	4096
RIP	200	100
RIPng	200	100
OSPF	200	100
OSPFv3	100	50
BGP4	200	100
BGP4+	200	100
RIP, OSPF, BGP4, RIPng, OSPFv3, BGP4+ の合計	256	128

注

動的監視機能を使用する隣接ルータは、ポーリング間隔によって数が制限されます。詳細は、次の表を参照してください。

表 3-201 スタティックの動的監視機能を使用できる最大隣接ルータ数

ポーリング周期	動的監視機能を使用できる最大隣接ルータ数
1 秒	60

ポーリング周期	動的監視機能を使用できる最大隣接ルータ数
5 秒	300
10 秒	600
20 秒	1200

(2) 経路エントリ数と最大隣接ルータ数の関係

最大経路エントリ数と最大隣接ルータ数の関係を次の表に示します。

表 3-202 経路エントリ数と最大隣接ルータ数の関係

ルーティングプロトコル	経路エントリ数 ¹	最大隣接ルータ数 ²	
		ポリシーベースルーティングのトラッキング機能を使用しない	ポリシーベースルーティングのトラッキング機能を使用する
RIP	1000	100	50
	2000	50	25
	10000	10	5
RIPng	1000	100	50
	2000	50	25
	10000	10	5
OSPF ^{3 4}	1000	200	100
	2000	100	50
	5000	40	20
	10000	20	10
OSPFv3 ^{3 5}	1000	100	50
	2000	50	25
	5000	20	10
	10000	10	5
BGP4	6	200	100
BGP4+	6	200	100

注 1
経路エントリ数は代替経路を含みます。

注 2
各ルーティングプロトコル (RIP, RIPng, OSPF, OSPFv3, BGP4, BGP4+) を併用して使用する場合の最大隣接ルータ数は、それぞれ $1/n$ (n : 使用ルーティングプロトコル数) です。例えば、BGP4, BGP4+ を使用しないで、OSPF (1000 経路) と OSPFv3 (1000 経路) を併用して使用する場合の最大隣接ルータ数は $1/2$ となり、OSPF では 100, OSPFv3 では 50 となります。

注 3
OSPF/OSPFv3 の最大経路エントリ数は LSA 数を意味します。

注 4
VRF で OSPF を使用している場合、装置全体の最大隣接ルータ数は 200 ですが、各 VRF で保持している LSA 数 × 各 VRF の隣接ルータ数の総計が 20 万を超えないようにしてください。

注 5

3. 収容条件

VRF で OSPFv3 を使用している場合，装置全体の最大隣接ルータ数は 100 ですが，各 VRF で保持している LSA 数 × 各 VRF の隣接ルータ数の総計が 10 万を超えないようにしてください。

注 6

「表 3-122 CSU-1A 経路配分パターンと収容経路エントリ数 (その 1)」, 「表 3-123 CSU-1A 経路配分パターンと収容経路エントリ数 (その 2)」, 「表 3-126 CSU-1B 経路配分パターンと収容経路エントリ数 (その 1)」, および 「表 3-127 CSU-1B 経路配分パターンと収容経路エントリ数 (その 2)」を参照してください。

(3) 本装置で設定できるコンフィギュレーションの最大数

ルーティングプロトコルについて，設定できるコンフィギュレーションの最大数を次の表に示します。

なお，この表で示す値はコンフィギュレーションで設定できる最大数です。運用する際は本章にある収容条件をすべて満たすようにしてください。

表 3-203 コンフィギュレーションの最大設定数

分類	コンフィギュレーション コマンド	最大数の定義	最大 設定数
IPv4 スタティック	ip route	テーブル容量が standard 時の設定 行数	8192
		テーブル容量が extended 時の設定 行数	16384
IPv6 スタティック	ipv6 route	テーブル容量が standard 時の設定 行数	8192
		テーブル容量が extended 時の設定 行数	16384
IPv4 集約経路	ip summary-address	設定行数	1024
IPv6 集約経路	ipv6 summary-address	設定行数	1024
RIP	network	設定行数	256
	ip rip authentication key	設定行数	512
OSPF	area range	設定行数	1024
	area virtual-link	authentication-key , message-digest-key パラメータを 設定した行数の総計	512
	ip ospf authentication-key ip ospf message-digest-key	各設定行数の総計	512
	network	設定行数	512
	router ospf	設定行数	256
BGP4	network	設定行数	1024
OSPFv3	area range	設定行数	1024
	ipv6 router ospf	設定行数	128
BGP4+	network	設定行数	1024
経路フィルタ	distribute-list in (RIP) distribute-list out (RIP) redistribute (RIP)	各設定行数の総計	2048
	distribute-list in (OSPF) distribute-list out (OSPF) redistribute (OSPF)	各設定行数の総計	2048

分類	コンフィギュレーション コマンド	最大数の定義	最大 設定数
	distribute-list in (BGP4) distribute-list out (BGP4) redistribute (BGP4)	各設定行数の総計	2048
	distribute-list in (RIPng) distribute-list out (RIPng) redistribute (RIPng)	各設定行数の総計	2048
	distribute-list in (OSPFv3) distribute-list out (OSPFv3) redistribute (OSPFv3)	各設定行数の総計	1024
	distribute-list in (BGP4+) distribute-list out (BGP4+) redistribute (BGP4+)	各設定行数の総計	2048
	ip as-path access-list	設定 <Id> の種類数	1024
		設定行数	4096
	ip community-list	設定 <Id> の種類数	512
		standard 指定の設定行数	1024
		expanded 指定の設定行数	1024
	ip prefix-list	設定 <Id> の種類数	2048
		設定行数	8192
	ipv6 prefix-list	設定 <Id> の種類数	2048
		設定行数	8192
	neighbor in (BGP4) neighbor out (BGP4)	<IPv4-Address> の設定行数の総計	256
		<Peer-Group> の設定行数の総計	256
	neighbor in (BGP4+) neighbor out (BGP4+)	<IPv6-Address> の設定行数の総計	256
		<Peer-Group> の設定行数の総計	256
	route-map	設定 <Id> の種類数	1024
		設定 <Id> と <Seq> の組み合わせ 種類数	4096
	match as-path	各設定行で指定したパラメータの 総計	4096
	match community	各設定行で指定したパラメータの 総計	4096
	match interface	各設定行で指定したパラメータの 総計	2048
	match ip address match ipv6 address	各設定行で指定したパラメータの 総計	4096
	match ip route-source match ipv6 route-source	各設定行で指定したパラメータの 総計	2048
	match origin	設定行数	2048
	match protocol	各設定行で指定したパラメータの 総計	4096
	match route-type	設定行数	2048

3. 収容条件

分類	コンフィギュレーション コマンド	最大数の定義	最大 設定数
	match tag	各設定行で指定したパラメータの 総計	2048
	match vrf	各設定行で指定したパラメータの 総計	4096
	set as-path prepend count set distance set local-preference set metric set metric-type set origin set tag	どれか一つが設定された route-map の、<Id> と <Seq> の 組み合わせ種類数	4096
	set community	各設定行で指定したパラメータの 総計	2048
	set community-delete	各設定行で指定したパラメータの 総計	2048

3.4.13 IPv4・IPv6 マルチキャストルーティングプロトコル

(1) IPv4 マルチキャスト

IPv4 マルチキャストを設定できるインタフェース数およびルーティングテーブルのエントリ数を次の表に示します。

複数の VRF で IPv4 マルチキャストを使用する場合、グローバルネットワークとすべての VRF の合計を本収容条件内に収めてください。ただし、CSU-1A では VRF 機能をサポートしていません。

なお、PIM-DM はグローバルネットワークでだけ動作します。また、本装置では、PIM-SM と PIM-DM は同時に動作できません。

表 3-204 IPv4 マルチキャストの最大数

項目	最大数	
	CSU-1A	CSU-1B
PIM-SM/SSM または PIM-DM マルチキャストインタフェース数 ¹	127 / 装置	255 / 装置
IGMP 動作インタフェース数	127 / 装置	255 / 装置
マルチキャスト送信元の数	256 / グループ 3000 / 装置	256 / グループ 3000 / 装置
PIM-SM/SSM マルチキャスト経路情報のエントリ ((S,G) エントリ, (*,G) エントリ, およびネガティブキャッシュ) 数, または PIM-DM マルチキャスト経路情報のエントリ ((S,G) エントリ) 数 ¹ S: 送信元 IP アドレス G: グループアドレス	4000 / 装置	8000 / 装置
IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連携動作させる設定数 (ソース, グループのペア数) ²	256 / 装置	256 / 装置
IGMPv3 で 1Report につき処理できる record 情報 ³	32record / メッセージ 32 ソース / record	32record / メッセージ 32 ソース / record
IGMP 加入グループ数 ^{4 5}	2000 / 装置	3000 / 装置

項目	最大数	
	CSU-1A	CSU-1B
マルチキャストルータ隣接数 ¹	256 / 装置	256 / 装置
ランデブーポイント数	2 / グループ	2 / グループ
1 装置当たりランデブーポイントで設定できるグループ数 ⁶	128 / 装置	128 / 装置
1 ネットワーク (VPN) 当たりランデブーポイントに設定できる延べグループ数	128 / ネットワーク 128 / 装置	128 / ネットワーク (VPN) 256 / 装置 ⁷
1 ネットワーク (VPN) 当たりの BSR 候補数	16 / ネットワーク 16 / 装置	16 / ネットワーク (VPN) 256 / 装置 ⁷
静的加入グループ数 ⁸	256 / 装置	256 / 装置
静的ランデブーポイント (RP) ルータアドレス数	16 / 装置	16 / 装置
IGMP グループ当たりのソース数	256 / グループ	256 / グループ
マルチキャスト中継エントリの延べ下流インタフェース数 ^{9 10}	140000 / 装置	280000 / 装置
マルチキャストを設定できる VRF 数 ¹¹	-	249 / 装置
エクストラネットのマルチキャストフィルタ数 ¹²	-	512 / 装置
エクストラネットで使用する route-map 数	-	256 / 装置 256 / VRF
PIM-SM VRF ゲートウェイ動作マルチキャストアドレス数 ¹³	-	256 / 装置 256 / VRF

(凡例) - : 該当なし

注 1

PIM-DM を使用する場合、隣接ルータ数によって使用できるマルチキャスト経路情報のエントリ数が異なります。「表 3-205 PIM-DM での隣接ルータ数に対するマルチキャスト経路情報のエントリ数」に示す範囲内で使用してください。

注 2

マルチキャストで使用するインタフェース数および加入グループ数によって設定できる数が変わります。「表 3-206 使用インタフェース数に対する IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数」および「表 3-207 加入グループ数に対する IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数」に示す範囲内で使用してください。加入グループ数は、動的および静的加入グループ数の総計です。同一グループアドレスが異なるインタフェースに加入している場合、加入グループ数は一つではなく、加入したインタフェースの数になります。

注 3

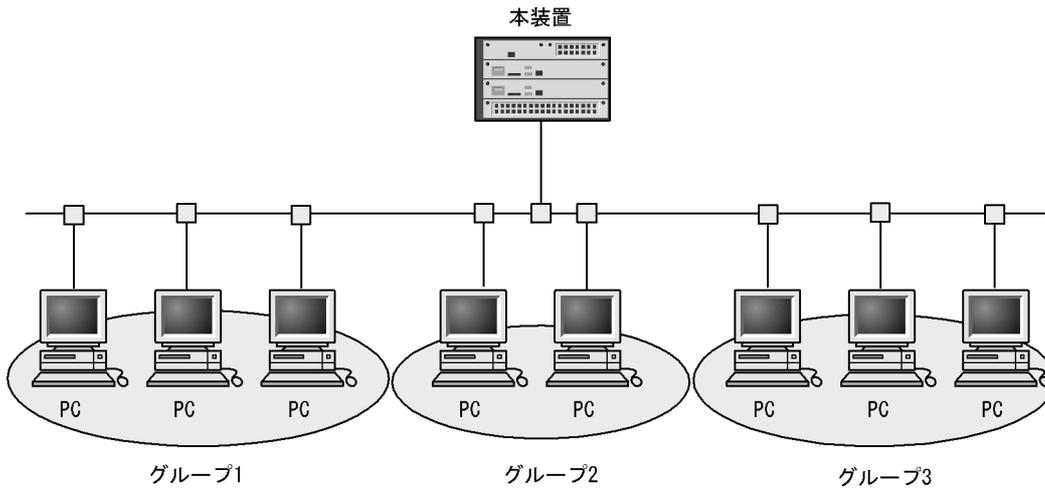
一つの Report メッセージで処理できるソース数は延べ 256 ソースまでです。ソース情報のない record も 1 ソースとして数えます。

IGMPv3 (EXCLUDE モード) で PIM-SSM を連携動作させる設定をした場合、その設定に一致した EXCLUDE record で定義されているソース数を数えます。また、受信した Report メッセージ内に EXCLUDE record が複数存在し、IGMPv3 (EXCLUDE モード) で PIM-SSM を連携動作させる設定で追加したソース数が延べ 256 を超えた場合、以降のそのメッセージ内の EXCLUDE record で、連携動作の対象となる EXCLUDE record についてマルチキャスト中継情報は作成しません。

注 4

本装置に直接接続しているグループの数を示します。IGMPv3 使用時に送信元を指定する場合のグループ数は、送信元とグループの組み合わせの数となります。次の図の例ではグループ数が 3 になります。

3. 収容条件



注 5

IPv4でのインタフェース当たりの加入可能グループ数を「表 3-208 IPv4でのインタフェース当たりの加入グループ数」に示します。

注 6

グループを指定しないでランデブーポイントを設定した場合、デフォルトグループが設定されます。グローバルネットワークおよびVRFでランデブーポイントを設定する場合、デフォルトグループも1グループとして、装置内またはネットワーク(VPN)内の総グループ数が収容条件内になるように設定してください。

注 7

本装置のグローバルネットワークとすべてのVRFに接続するネットワーク(VPN)上の総数です。

注 8

静的加入グループ数とは、各マルチキャストインタフェースで静的加入するグループアドレスの総数です。同一グループアドレスを複数の異なるインタフェースに静的加入設定した場合、静的加入グループ数は一つではなく、静的加入設定したインタフェースの数になります。また、PIM-SM VRF ゲートウェイで指定したグループアドレスの延べ数との合計になります。

注 9

構成およびリソース状況によっては最大数がCSU-1A搭載時は140000以下、CSU-1B搭載時は280000以下となることがあります。

注 10

マルチキャスト中継エントリの延べ下流インタフェース数は、IPv4マルチキャストとIPv6マルチキャストの合計です。

注 11

PIM-SM/SSM 使用時だけ設定できます。

注 12

すべてのroute-mapで指定したaccess-list内のアドレスの延べ数です。

注 13

エクストラネットで指定したroute-mapを使用します。route-mapに指定したaccess-list内で、ホストアドレス(32ビットマスク)として指定したマルチキャストアドレスが対象となります。装置当たりの上限は、すべてのVRFで指定したPIM-SM VRFゲートウェイのグループアドレスの延べ数です。また、静的加入グループ数で指定したグループアドレス数との合計になります。

表 3-205 PIM-DMでの隣接ルータ数に対するマルチキャスト経路情報のエントリ数

隣接ルータ数	マルチキャスト経路情報のエントリ数
256	1000

隣接ルータ数	マルチキャスト経路情報のエントリ数
128	2000
64	4000
32	8000

表 3-206 使用インタフェース数に対する IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数

使用インタフェース数	IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連動させる設定数
31	256
63	128
127	64
255	32

表 3-207 加入グループ数に対する IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数

加入グループ (延べ数)	IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連動させる設定数
64	256
128	128
256	64
512	32
1024	16
2048	8
4096	4
8128	2

表 3-208 IPv4 でのインタフェース当たりの加入グループ数

マルチキャスト動作インタフェース数	インタフェース当たりの加入可能グループ数
31	256
63	128
127	64
255	32

(a) IPv4 マルチキャスト使用時の注意事項

マルチキャストデータの送信元に対して到達できるすべてのインタフェースに PIM の設定が必要です。

(b) マルチキャストデータの送信元サーバに関する注意

マルチキャストデータの送信元となるサーバの中には、マルチキャストパケットをバーストラフィックとして送信する特性を持つものがあります。この特性を持つサーバから受信したマルチキャストデータを、マルチキャスト配信する場合には注意が必要です。マルチキャスト配信先の回線を収容するネットワークインタフェース機構 (NIF) の種類によって、マルチキャスト動作可能なインタフェース数が異なります。マルチキャスト動作可能なインタフェース数を次の表に示します。

表 3-209 マルチキャスト動作可能なインタフェース数

NIF 略称	マルチキャスト動作可能なインタフェース数 (推奨値)
NK1G-24T	ポート当たり 16 インタフェース
NK1G-24S	ポート当たり 16 インタフェース
NK1GS-8M	NIF 当たり 255 インタフェース
NK10G-4RX	ポート当たり 32 インタフェース
NK10G-8RX	ポート当たり 32 インタフェース

注

推奨値は、送信元サーバが、マルチキャストパケットを 8 バーストで送信する特性（サーバで 8 パケット分のマルチキャストデータをいったん蓄積したあとに、ネットワークに対して連続的に送信する特性）を持っていることを想定しています。バースト数が大きくなると、パケットを一部廃棄することがあるので、マルチキャストを定義するインタフェース数を少なくする必要があります。

(2) IPv6 マルチキャスト

IPv6 マルチキャストを設定できるインタフェース数およびルーティングテーブルのエントリ数を次の表に示します。

複数の VRF で IPv6 マルチキャストを使用する場合、グローバルネットワークとすべての VRF の合計を本収容条件内に収めてください。ただし、CSU-1A では VRF 機能をサポートしていません。

表 3-210 IPv6 マルチキャストの最大数

項目	最大数	
	CSU-1A	CSU-1B
PIM-SM/SSM マルチキャストインタフェース数 ^{1 2}	127 / 装置	255 / 装置
MLD 動作インタフェース数 ¹	127 / 装置	255 / 装置
マルチキャスト送信元の数	256 / グループ	256 / グループ
PIM-SM/SSM マルチキャストルーティングエントリ (S,G) エントリ, (*,G) エントリ, およびネガティブキャッシュ) 数 S: 送信元 IP アドレス G: グループアドレス	1000 / 装置	8000 / 装置
MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連携動作させる設定数 (ソース, グループペア数) ³	256 / 装置	256 / 装置
MLDv2 で 1Report につき処理できる record 情報 ⁴	32record / メッセージ 32 ソース / record	32record / メッセージ 32 ソース / record
MLD 加入グループ数 ^{5 6}	256 / 装置	256 / 装置
マルチキャストルーティング隣接数	256 / 装置	256 / 装置
ランデブーポイント数	2 / グループ	2 / グループ
1 装置当たりランデブーポイントで設定できるグループ数 ⁷	128 / 装置	128 / 装置
1 ネットワーク (VPN) 当たりランデブーポイントに設定できる延べグループ数	128 / ネットワーク 128 / 装置	128 / ネットワーク (VPN) 256 / 装置 ⁸

項目	最大数	
	CSU-1A	CSU-1B
1 ネットワーク (VPN) 当たりの BSR 候補数	16 / ネットワーク 16 / 装置	16 / ネットワーク (VPN) 256 / 装置 ⁸
静的加入グループ数 ^{9 10}	2000 / 装置	4000 / 装置
静的ランデブポイント (RP) ルータアドレス数	16 / 装置	16 / 装置
MLD グループ当たりのソース数	256 / グループ	256 / グループ
遠隔のマルチキャストサーバアドレスを直接接続サーバとして扱う 設定数	256 / 装置 16 / インタフェー ス	256 / 装置 16 / インタフェー ス
マルチキャスト中継エントリの延べ下流インタフェース数 ^{11 12}	140000 / 装置	280000 / 装置
マルチキャストを設定できる VRF 数	-	249 / 装置
エクストラネットのマルチキャストフィルタ数 ¹³	-	512 / 装置
エクストラネットで使用する route-map 数	-	256 / 装置 256 / VRF
PIM-SM VRF ゲートウェイ動作マルチキャストアドレス数 ¹⁴	-	256 / 装置 256 / VRF

(凡例) - : 該当なし

注 1

マルチホームをサポートします。

注 2

IPv6 マルチキャストインタフェースとして、このほかにカプセル化用インタフェースが一つ存在します。このため、IPv6 PIM-SM マルチキャストインタフェース全体の数は、CSU-1A 搭載時は 128 個、CSU-1B 搭載時は 256 個になりますが、ユーザが設定できるのはそのうち CSU-1A 搭載時は 127 個、CSU-1B 搭載時は 255 個です。また、PIM-SM と PIM-SSM の合計で CSU-1A 搭載時は 127 / 装置、CSU-1B 搭載時は 255 / 装置となります。

注 3

マルチキャストで使用するインタフェース数および加入グループ数によって設定できる数が変わります。「表 3-211 使用インタフェース数に対する MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数」および「表 3-212 加入グループ数に対する MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数」に示す範囲内で使用してください。加入グループ数は、動的および静的加入グループ数の総計です。同一グループアドレスが異なるインタフェースに加入している場合、加入グループ数は一つでなく、加入したインタフェースの数になります。

注 4

一つの Report メッセージで処理できるソース数は延べ 1024 ソースまでです。ソース情報のない record も 1 ソースとして数えます。

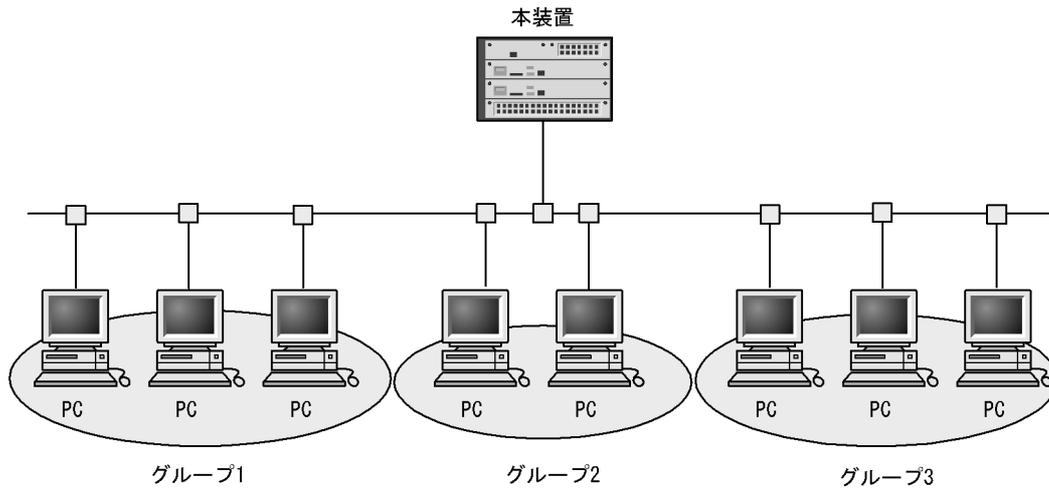
MLDv2 (EXCLUDE モード) で PIM-SSM を連携動作させる設定をした場合、その設定に一致した EXCLUDE record で定義されているソース数を数えます。また、受信した Report メッセージ内に EXCLUDE record が複数存在し、MLDv2 (EXCLUDE モード) で PIM-SSM を連携動作させる設定で追加したソース数が延べ 1024 を超えた場合、以降のそのメッセージ内の EXCLUDE record で、連携動作の対象となる EXCLUDE record についてマルチキャスト中継情報は作成しません。

注 5

本装置に直接接続しているグループの数を示します。MLDv2 使用時に送信元を指定する場合のグループ数は、送信元とグループの組み合わせの数となります。

次の図の例ではグループ数が 3 になります。

3. 収容条件



注 6

IPv6でのインタフェース当たりの加入可能グループ数を「表 3-213 IPv6でのインタフェース当たりの加入可能グループ数」に示します。

注 7

グループを指定しないでランデブーポイントを設定した場合、デフォルトグループが設定されます。グローバルネットワークおよびVRFでランデブーポイントを設定する場合、デフォルトグループも1グループとして、装置内またはネットワーク(VPN)内の総グループ数が収容条件内になるように設定してください。

注 8

本装置のグローバルネットワークとすべてのVRFに接続するネットワーク(VPN)上の総数です。

注 9

静的加入グループ数とは、各マルチキャストインタフェースで静的加入するグループアドレスの総数です。同一グループアドレスを複数の異なるインタフェースに静的加入設定した場合、静的加入グループ数は一つではなく、静的加入設定したインタフェースの数になります。また、PIM-SM VRF ゲートウェイで指定したグループアドレスの延べ数との合計になります。

注 10

一つのインタフェースに設定できる静的加入グループ数は256までです。

注 11

構成およびリソース状況によっては最大数がCSU-1A搭載時は140000以下、CSU-1B搭載時は280000以下となることがあります。

注 12

マルチキャスト中継エントリの延べ下流インタフェース数は、IPv4マルチキャストとIPv6マルチキャストの合計です。

注 13

すべてのroute-mapで指定したaccess-list内のアドレスの延べ数です。

注 14

エクストラネットで指定したroute-mapを使用します。route-mapに指定したaccess-list内で、ホストアドレス(128ビットマスク)として指定したマルチキャストアドレスが対象となります。装置当たりの上限は、すべてのVRFで指定したPIM-SM VRFゲートウェイのグループアドレスの延べ数です。また、静的加入グループ数で指定したグループアドレス数との合計になります。

表 3-211 使用インタフェース数に対する MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数

使用インタフェース数	MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連動させる設定数
31	256
63	256
127	256
255	256

表 3-212 加入グループ数に対する MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数

加入グループ数 (延べ数)	MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連動させる設定数
64	256
128	128
256	64
512	32
1024	16
2048	8
4096	4
8128	2

表 3-213 IPv6 でのインタフェース当たりの加入可能グループ数

マルチキャスト動作インタフェース数	インタフェース当たりの加入可能グループ数
31	256
63	128
127	64
255	32

(a) PIM-SM / SSM 使用時の注意事項

マルチキャストデータの送信元に対して到達できるすべてのインタフェースに PIM の設定が必要です。

(b) マルチキャストデータの送信元サーバに関する注意

IPv6 でのマルチキャストデータの送信元サーバに関する注意の内容は、IPv4 と同様です。詳細は、「(1) IPv4 マルチキャストの (b) マルチキャストデータの送信元サーバに関する注意」を参照してください。

3.4.14 VRF 【OP-NPAR】

設定できる VRF 数を次の表に示します。VRF 設定可能数にグローバルネットワークは含みません。

表 3-214 設定できる VRF 数

VRF 動作モード	VRF 設定可能数	説明
設定なし	-	• VRF は動作しません

3. 収容条件

VRF 動作モード	VRF 設定可能数	説明
axrp-enable	63	<ul style="list-style-type: none"> IPv4 だけが VRF インスタンスで動作します Ring Protocol が動作します
l2protocol-disable	249	<ul style="list-style-type: none"> IPv4 だけが VRF インスタンスで動作します レイヤ 2 プロトコルが動作しません
axrp-enable-ipv4-ipv6	63	<ul style="list-style-type: none"> IPv4 と IPv6 のどちらも VRF インスタンスで動作します Ring Protocol が動作します
gsrp-enable-ipv4-ipv6	124	<ul style="list-style-type: none"> IPv4 と IPv6 のどちらも VRF インスタンスで動作します GSRP が動作します
l2protocol-disable-ipv4-ipv6	249	<ul style="list-style-type: none"> IPv4 と IPv6 のどちらも VRF インスタンスで動作します レイヤ 2 プロトコルが動作しません

(凡例) - : 設定できない

3.5 AX6300S の搭載条件【AX6300S】

3.5.1 最大収容ポート数

各モデルの最大収容可能ポート数を次の表に示します。

表 3-215 最大収容可能ポート数

モデル名	イーサネット		
	10GBASE-R	1000BASE-X	10/100/1000BASE-T
AX6304S	32	96	96
AX6308S	64	192	192

3.5.2 最大搭載数

(1) 機器搭載数

各モデルへの冗長化構成を含めた機器最大搭載数を次の表に示します。

表 3-216 機器最大搭載数

機器	AX6304S	AX6308S
MSU	2 (冗長化構成時)	2 (冗長化構成時)
NIF	4	8
PS (AC 電源)	4 (冗長化構成時)	4 (冗長化構成時)
PS (DC 電源)	2 (冗長化構成時)	2 (冗長化構成時)

(2) 電源機構の搭載数

電源機構の最大搭載数は「表 3-216 機器最大搭載数」を参照してください。また、電源機構搭載条件については、マニュアル「コンフィグレーションガイド Vol.2 16. 電源機構 (PS) の冗長化」を参照してください。

(3) NIF 最大搭載数

NIF の種別によって最大搭載数が異なります。NIF 種別ごとの最大搭載数を次に示します。

NIF のダブルサイズは NIF のスロットを 2 スロット分使用し、シングルサイズは 1 スロット分使用します。

表 3-217 NIF 種別ごとの最大搭載数

NIF 種別	サイズ	AX6304S	AX6308S
		装置当たり	装置当たり
NH1G-16S	シングル	4	8
NH1G-24T	シングル	4	8
NH1G-24S	シングル	4	8
NH1G-48T	ダブル	2	4

3. 収容条件

NIF 種別	サイズ	AX6304S	AX6308S
		装置当たり	装置当たり
NH1GS-6M	シングル	4	8
NH10G-1RX	シングル	4	8
NH10G-4RX	シングル	4	8
NH10G-8RX	シングル	4	8

3.6 AX6300S の収容条件【AX6300S】

本節で使用する VLAN ポート数とは各 VLAN に所属するポート数の延べ数の合計です。

例えば、VLAN 1 ~ 100 を設定し、それぞれの VLAN に 2 回線が所属している場合、VLAN ポート数は $100 \times 2 = 200$ となります。

3.6.1 テーブルエントリ数

(1) 概要

本項で使用するテーブルエントリ数とは、経路数やフィルタ・QoS のエントリ数を意味します。

本装置では、ネットワーク構成に合わせ、適切なテーブルエントリ数の配分パターンを選ぶことができます。配分パターンはコンフィグレーションコマンドによって変更できます。

エントリの配分パターンは経路系、フロー系をそれぞれ用意しています。経路系テーブルエントリ、フロー系テーブルエントリ定義を次の表に示します。

表 3-218 経路系テーブルエントリ、フロー系テーブルエントリ内容定義

項目	内容
経路系エントリ	IPv4 ユニキャスト経路 IPv4 マルチキャスト経路 IPv6 ユニキャスト経路 IPv6 マルチキャスト経路 MAC アドレスエントリ ARP NDP
フロー系エントリ	フィルタエントリ（ポリシーベースルーティングおよびポリシーベーススイッチングを含む） QoS エントリ

(2) テーブル容量種別

テーブル容量に対応した名称を次の表に示します。

表 3-219 経路系テーブル容量名称

テーブル容量	対応 MSU
standard	MSU-1A, MSU-1A1
extended	MSU-1B, MSU-1B1

表 3-220 フロー系テーブル容量名称

テーブル容量	対応 MSU
standard ¹	MSU-1A, MSU-1A1
standard-advance ²	
extended ³	MSU-1B, MSU-1B1
extended-advance ²	

3. 収容条件

- 注 1 MSU-1A および MSU-1A1 でのデフォルトのテーブル容量です。
 注 2 フロー検出拡張モードを使用する場合に指定します。
 注 3 MSU-1B および MSU-1B1 でのデフォルトのテーブル容量です。

(3) 配分パターン

配分パターンを次の表に示します。

表 3-221 経路系テーブルエントリ配分パターン

パターン名称	意味
default	全エントリ混在
ipv4-uni	IPv4 ユニキャスト主体, マルチキャスト, IPv6 無し
ipv4-ipv6-uni	IPv4 ユニキャスト / IPv6 ユニキャスト主体, マルチキャスト無し
vlan	L2 主体, マルチキャスト無し

注 デフォルトのパターン

表 3-222 standard および standard-advance のフロー系テーブルエントリ配分パターン

パターン名称	意味
default	フィルタ, QoS 均等

注 デフォルトのパターン

表 3-223 extended および extended-advance のフロー系テーブルエントリ配分パターン

パターン名称	意味
default	フィルタ, QoS 均等
filter-only	フィルタ専用
qos-only	QoS 専用
filter	フィルタ主体
qos	QoS 主体

注 デフォルトのパターン

経路系テーブルエントリ数とフロー系テーブルエントリ数を次の表に示します。

VRF 機能使用時の最大エントリ数は, 全 VRF のエントリ数の合計です。

本項表中の「k」の単位は 1024 です。例えば, 24k は $24 \times 1024 = 24576$ であることを表しています。

表 3-224 standard の経路系テーブルエントリ数

パターン名	IPv4 ユニ キャスト経 路 ¹	IPv4 マル チキャスト 経路	IPv6 ユニ キャスト 経路 ²	IPv6 マル チキャスト 経路	MAC ア ドレス	ARP	NDP
default	32768 (32k)	4000	16384 (16k)	1000	24576 (24k)	12288 (12k)	12288 (12k)
ipv4-uni	65536 (64k)	-	-	-	24576 (24k)	12288 (12k)	-

パターン名	IPv4 ユニキャスト経路 ¹	IPv4 マルチキャスト経路	IPv6 ユニキャスト経路 ²	IPv6 マルチキャスト経路	MAC アドレス	ARP	NDP
ipv4-ipv6-uni	32768 (32k)	-	32768 (32k)	-	24576 (24k)	12288 (12k)	12288 (12k)
vlan	8192 (8k)	-	8192 (8k)	-	49152 (48k)	8192 (8k)	8192 (8k)

(凡例) - : 該当なし

注 注 は次表を参照してください。

表 3-225 extended の経路系テーブルエントリ数

パターン名	IPv4 ユニキャスト経路 ¹	IPv4 マルチキャスト経路	IPv6 ユニキャスト経路 ²	IPv6 マルチキャスト経路	MAC アドレス	ARP	NDP
default	65536 (64k)	8000	32768 (32k)	8000	65536 (64k)	24576 (24k)	24576 (24k)
ipv4-uni	212992 (208k)	-	-	-	24576 (24k)	24576 (24k)	-
ipv4-ipv6-uni	106496 (104k)	-	106496 (104k)	-	24576 (24k)	24576 (24k)	24576 (24k)
vlan	8192 (8k)	-	8192 (8k)	-	122880 (120k)	8192 (8k)	8192 (8k)

(凡例) - : 該当なし

注 1 IPv4 ユニキャスト経路数には次の情報が含まれます。

- RIP, OSPF, BGP4, スタティックを合わせたアクティブ経路
- 他 VRF (グローバルネットワークを含む) からインポートされた, アクティブ状態のエクストラネット経路
- IPv4 インタフェース数 × 4 : 直結経路のホスト経路, サブネット経路, ブロードキャスト経路 (ホストアドレスの全情報が 0 と 1 の 2 経路)
- ARP エントリ数
- ループバックインタフェースを指定の場合は 1 経路が加算されます。
VRF でループバックインタフェースを使用する場合は, VRF ごとに 1 経路が加算されます。
- RIP バージョン 2 を使用する場合は 1 経路が加算されます。
VRF で RIP バージョン 2 を使用する場合は, VRF ごとに 1 経路が加算されます。
- OSPF を使用する場合は 2 経路が加算されます。
VRF で OSPF を使用する場合は, VRF ごとに 2 経路が加算されます。
- vrrp でアクセプトモードを設定して, マスタ状態になっている場合は 1 経路が加算されます。
- ここに示した以外に 4 経路を装置固定情報として使用します。
VRF を使用する場合は, VRF ごとに 1 経路を装置固定情報として使用します。

注 2 IPv6 ユニキャスト経路数には次の情報が含まれます。

- RIPng, OSPFv3, BGP4+, スタティックを合わせたアクティブ経路数
- IPv6 インタフェース数 × 5 : 直結経路のグローバルアドレス, リンクローカルアドレスそれぞれのホスト経路およびサブネット経路, 直結経路のリンクローカルマルチキャストアドレス
- NDP エントリ数
- ループバックインタフェースを指定の場合は 1 経路が加算されます。
VRF でループバックインタフェースを使用する場合は, VRF ごとに 1 経路が加算されます。
- vrrp でアクセプトモードを設定して, マスタ状態になっている場合は 1 経路が加算されます。
- ここに示した以外に 1 経路を装置固定情報として使用します。
VRF を使用する場合は, VRF ごとに 1 経路を装置固定情報として使用します。

表 3-226 standard のフロー系エントリ数

パターン名	フィルタ	QoS
default (フィルタ, QoS 均等)	4000	4000

表 3-227 standard-advance のフロー系エントリ数

パターン名	フィルタ	QoS
default (フィルタ, QoS 均等)	2000 (300)	2000

注

括弧内の値は DHCP snooping が有効な場合のフィルタエントリ数です。

表 3-228 extended および extended-advance のフロー系エントリ数

パターン名	フィルタ	QoS
default (フィルタ, QoS 均等)	16000 (6000)	16000
filter-only (フィルタ専用)	32000 (22000)	-
qos-only (QoS 専用)	-	32000
filter (フィルタ主体)	24000 (14000)	8000
qos (QoS 主体)	8000 (4000)	24000

(凡例) - : 該当なし

注

括弧内の値は, extended-advance で DHCP snooping が有効な場合のフィルタエントリ数です。

3.6.2 MSU 経路配分パターン

MSU 経路配分パターンに応じた収容可能な IP ユニキャスト, IP マルチキャストの経路エントリ数, MAC アドレスエントリ数, および IP インタフェース数を次の表に示します。表中の「k」の単位は 1024 です。

(1) MSU-1A および MSU-1A1 (standard) の経路配分パターン

表 3-229 MSU-1A および MSU-1A1 経路配分パターンと収容経路エントリ数 (その1)

経路配分パターン	IPv4 ユニキャスト					IPv4 マルチキャスト	IPv4 インタフェース数	MAC アドレスエントリ数	
	最大経路エントリ数		プロトコル別最大経路エントリ数			PIM-SM/SSM PIM-DM			
	アクティブ/非アクティブの合計	アクティブ	RIP+OS PF	BGP	スタティック	(S,G) エントリ数			インタフェース数
default	131072 (128k)	32768 (32K)	10000	131072 (128k)	4096	1	1	4096	24576 (24k)
ipv4-uni	262144 (256k)	65536 (64k)	10000	262144 (256k)	4096	-	-	4096	24576 (24k)
ipv4-ipv6-uni	131072 (128k)	32768 (32k)	10000	131072 (128k)	4096	-	-	4096	24576 (24k)
vlan	32768 (32k)	8192	10000	32768 (32k)	4096	-	-	4096	49152 (48k)

(凡例) - : 該当なし

注 注 は次表を参照してください。

表 3-230 MSU-1A および MSU-1A1 経路配分パターンと収容経路エントリ数 (その2)

経路配分パターン	IPv6 ユニキャスト					IPv6 マルチキャスト	IPv6 インタフェース数	
	最大経路エントリ数		プロトコル別最大経路エントリ数			PIM-SM/SSM		
	アクティブ/非アクティブの合計	アクティブ	RIPng+OS PFv3	BGP4+	スタティック	(S,G) エントリ数		インタフェース数
default	65536 (64k)	16384 (16k)	10000	65536 (64k)	4096	2	2	4096
ipv4-uni	-	-	-	-	-	-	-	-
ipv4-ipv6-uni	131072 (128k)	32768 (32k)	10000	131072 (128k)	4096	-	-	4096
vlan	32768 (32k)	8192	10000	32768 (32k)	4096	-	-	4096

(凡例) - : 該当なし

注 1,2

(S,G) エントリ数とインタフェース数の組み合わせは、次のどれかの組み合わせとなります。IPv4 と IPv6 のマルチキャストに関しては、IPv4 マルチキャストと IPv6 マルチキャストを混在で使用する場合、(S,G) エントリ数とインタフェース数は、IPv4 と IPv6 の合計値が次の表のエントリ数以内となるようにしてください。

注 1 の場合の組み合わせを次の表に示します。

3. 収容条件

表 3-231 IPv4 マルチキャスト単独使用の場合の (S,G) エントリ数とインタフェース数の組み合わせ

(S,G) エントリ数	インタフェース数
4000	31
2000	63
1000	127

注 2 の場合の組み合わせを次の表に示します。

表 3-232 IPv6 マルチキャスト単独使用, または IPv4/IPv6 マルチキャスト混在使用の場合の (S,G) エントリ数とインタフェース数の組み合わせ

(S,G) エントリ数	インタフェース数
1000	31
500	63
250	127

(2) MSU-1B および MSU-1B1 (extended) の経路配分パターン

表 3-233 MSU-1B および MSU-1B1 経路配分パターンと収容経路エントリ数 (その1)

経路配分パターン	IPv4 ユニキャスト					IPv4 マルチキャスト		IPv4 インタフェース数	MAC アドレスエントリ数
	最大経路エントリ数		プロトコル別最大経路エントリ数			PIM-SM/SSM PIM-DM			
	アクティブ/非アクティブの合計	アクティブ	RIP+OS PF	BGP	スタティック	(S,G) エントリ数	インタフェース数		
default	262144 (256k)	65536 (64K)	10000	262144 (256k)	4096			4096	65536 (64k)
ipv4-uni	851968 (832k)	212992 (208k)	10000	851968 (832k)	4096	-	-	4096	24576 (24k)
ipv4-ipv6-uni	425984 (416k)	106496 (104k)	10000	425984 (416k)	4096	-	-	4096	24576 (24k)
vlan	32768 (32k)	8192	10000	32768 (32k)	4096	-	-	4096	122880 (120k)

(凡例) - : 該当なし

注 は次表を参照してください。

表 3-234 MSU-1B および MSU-1B1 経路配分パターンと収容経路エントリ数 (その 2)

経路配分パターン	IPv6 ユニキャスト					IPv6 マルチキャスト		IPv6 インタフェース数
	最大経路エントリ数		プロトコル別最大経路エントリ数			PIM-SM/SSM		
	アクティブ/非アクティブの合計	アクティブ	RIPng+OS PFv3	BGP4+	スタティック	(S,G) エントリ数	インタフェース数	
default	131072 (128k)	32768 (32k)	10000	131072 (128k)	4096			4096
ipv4-uni	-	-	-	-	-	-	-	-
ipv4-ipv6-uni	425984 (416k)	106496 (104k)	10000	425984 (416k)	4096	-	-	4096
vlan	32768 (32k)	8192	10000	32768 (32k)	4096	-	-	4096

(凡例) - : 該当なし

注

(S,G) エントリ数とインタフェース数の組み合わせは、次のどれかの組み合わせとなります。IPv4 と IPv6 のマルチキャストに関しては、IPv4 マルチキャストと IPv6 マルチキャストを混在で使用する場合、(S,G) エントリ数とインタフェース数は、IPv4 と IPv6 の合計値が次の表のエントリ数以内となるようにしてください。

組み合わせを次の表に示します。

表 3-235 (S,G) エントリ数とインタフェース数の組み合わせ

(S,G) エントリ数	インタフェース数
8000	31
4000	63
2000	127
1000	255

3.6.3 リンクアグリゲーション

コンフィグレーションによって設定できるリンクアグリゲーションの収容条件を次の表に示します。

表 3-236 リンクアグリゲーションの収容条件

モデル	装置当たりの最大チャンネルグループ数	チャンネルグループ当たりの最大ポート数
AX6304S	48	16
AX6308S	63	16

3.6.4 レイヤ 2 スイッチ

(1) MAC アドレステーブル

L2 スイッチ機能では、複数の機能で MAC アドレステーブルを使用しています。例えば、MAC アドレス

3. 収容条件

の学習機能では、接続された端末の MAC アドレスをダイナミックに学習して MAC アドレステーブルへ登録します。

MAC アドレステーブルの最大エン트리数については、次の表を参照してください。

- 表 3-229 MSU-1A および MSU-1A1 経路配分パターンと収容経路エン트리数（その 1）
- 表 3-233 MSU-1B および MSU-1B1 経路配分パターンと収容経路エン트리数（その 1）

MAC アドレステーブルを使用する機能と、その機能による MAC アドレステーブルの使用量を次の表に示します。

表 3-237 MAC アドレステーブルを使用する機能

機能名	使用量
MAC アドレス学習抑止機能	設定した VLAN ごとに 1 エン트리
スタティック MAC アドレス登録機能	登録した MAC アドレスごとに 1 エン트리
スタティック ARP/NDP 登録機能	登録した ARP/NDP エン트리ごとに 1 エン트리
MAC アドレス学習機能 ARP/NDP 学習機能	学習したアドレスごとに 1 エン트리
Ring Protocol 機能	[マスタノード時] リング ID ごとに 2 エン트리 [共有ノード時] リング ID ごとに 1 エン트리
IGMP/MLD snooping 機能（学習）	学習した MAC アドレスごとに 1 エン트리
IGMP snooping 機能	設定した VLAN ごとに 2 エン트리
MLD snooping 機能	設定した VLAN ごとに 8 エン트리
IEEE802.1X	認証済み端末ごとに 1 エン트리
Web 認証機能	認証済み端末ごとに 1 エン트리
MAC 認証機能	認証済み端末ごとに 1 エン트리

注 MAC アドレスと対応する ARP/NDP を学習した場合は合わせて 1 エン트리となります

MAC アドレステーブルのエン트리数が最大エン트리数に達した場合、新たなエントリを登録できなくなるため、上記の収容条件内で運用してください。

運用中は、運用コマンド show system で MAC アドレステーブルの使用状況を確認できます。

(2) MAC アドレス学習

MAC アドレス学習数の収容条件は、「表 3-229 MSU-1A および MSU-1A1 経路配分パターンと収容経路エン트리数（その 1）」「表 3-233 MSU-1B および MSU-1B1 経路配分パターンと収容経路エン트리数（その 1）」で示した MAC アドレステーブルの最大エン트리数となります。「表 3-237 MAC アドレステーブルを使用する機能」に示したほかの機能を使用した場合は、ほかの機能で使用した分だけ MAC アドレス学習数の最大数が減少します。

(3) スタティック MAC アドレス登録

スタティック MAC アドレス登録機能の収容条件を次の表に示します。

表 3-238 スタティック MAC アドレスの登録数

モデル	装置当たり
AX6300S シリーズ共通	1000

MAC アドレステーブルに空きがない場合は、スタティック MAC アドレス登録機能の最大数まで登録できないことがあります。

(4) VLAN

コンフィグレーションによって設定できる VLAN の数を次の表に示します。

表 3-239 VLAN 数

モデル	装置当たり VLAN	ポート当たり VLAN	VLAN ポート数
AX6300S シリーズ共通	4095	4095	100000

VLAN ポート数が収容条件を超えた場合、CPU の利用率が高くなり、コンフィグレーションコマンドや運用コマンドのレスポンスが遅くなったり、実行できなくなったりすることがあります。

(a) プロトコル VLAN

プロトコル VLAN では、イーサネットフレーム内の Ethernet-Type, LLC SAP, および SNAP type フィールドの値を基にプロトコルの識別を行います。コンフィグレーションによって設定できるプロトコル VLAN の収容条件を次の表に示します。

表 3-240 プロトコル VLAN のプロトコルの種類数

モデル	装置当たり	ポート当たり
AX6300S シリーズ共通	16	16

表 3-241 プロトコル VLAN 数

モデル	装置当たり
AX6300S シリーズ共通	96

表 3-242 プロトコルポート数

モデル	装置当たり
AX6300S シリーズ共通	96

(b) MAC VLAN

MAC VLAN の収容条件を次の表に示します。

3. 収容条件

表 3-243 MAC VLAN の登録 MAC アドレス数

モデル	コンフィグレーションによる最大登録 MAC アドレス数	L2 認証機能による最大登録 MAC アドレス数	コンフィグレーションによる登録数と L2 認証機能による登録数の同時登録最大 MAC アドレス数
AX6300S シリーズ 共通	4096	4096	4096

(c) Tag 変換

コンフィグレーションによって設定できる Tag 変換情報エントリ数を次の表に示します。

表 3-244 Tag 変換情報エントリ数

モデル	装置当たり
AX6300S シリーズ共通	4096

注 Tag 変換情報エントリをポートチャンネルインタフェースに設定する場合、Tag 変換情報エントリ数は該当チャンネルグループのポート数で計算します。

(d) VLAN トンネリング

コンフィグレーションによって設定できる VLAN トンネリングの数を次の表に示します。

表 3-245 VLAN トンネリングの数

モデル	装置当たり
AX6300S シリーズ共通	4095

(e) VLAN 識別テーブル

VLAN 識別テーブルは、フレーム受信時に VLAN を識別するためのテーブルです。プロトコル VLAN、MAC VLAN、および Tag 変換では、VLAN 識別テーブルを使用します。これらの機能を同時に使用する場合は、次の収容条件となります。

ポートごとのプロトコル数 + 登録 MAC アドレス数 + Tag 変換情報エントリ数 4096

ポートごとのプロトコル数

装置内の各プロトコルポートに設定するプロトコル数の合計。リンクアグリゲーションを使用する場合は、ポートチャンネルインタフェースに設定するプロトコル数で計算するため、チャンネルグループの収容ポート数は無関係です。

登録 MAC アドレス数

コンフィグレーションによる MAC アドレス登録数と L2 認証機能による MAC アドレス登録数の合計。

Tag 変換情報エントリ数

コンフィグレーションで設定する Tag 変換情報エントリの数。リンクアグリゲーションを使用する場合は、ポートチャンネルインタフェースに設定する Tag 変換情報エントリ数で計算するため、チャンネルグループの収容ポート数は無関係です。

(5) スパニングツリー

スパニングツリーの収容条件を種類ごとに次の表に示します。

なお、スパニングツリーの VLAN ポート数は、スパニングツリーが動作する VLAN に所属するポート数の延べ数です。チャンネルグループの場合、チャンネルグループ当たりの物理ポート数を数えます。ただし、次の VLAN やポートは、VLAN ポート数に含めません。

- コンフィグレーションコマンド `state` で `suspend` パラメータが設定されている VLAN
- VLAN トンネリングを設定しているポート
- BPDU ガード機能を設定しているが、BPDU フィルタ機能を設定していないポート
- PortFast 機能と BPDU フィルタ機能を設定しているアクセスポート

表 3-246 PVST+ の収容条件

モデル	Ring Protocol 共存有無	対象 VLAN 数	VLAN ポート数
AX6300S シリーズ共通	共存なし	250	1000
	共存あり	128	900

表 3-247 シングルスパニングツリーの収容条件

モデル	Ring Protocol 共存有無	対象 VLAN 数	VLAN ポート数	
AX6300S シリーズ 共通	共存なし	4095	シングルだけ	10000
			PVST+ 併用時	5000
	共存あり		シングルだけ	9000
			PVST+ 併用時	4500

注

PVST+ 併用時、PVST+ の VLAN ポート数とシングルスパニングツリーの VLAN ポート数との合計が最大値となります。

表 3-248 マルチプルスパニングツリーの収容条件

モデル	Ring Protocol 共存有無	MST インスタンス数	MST インスタンスごとの対象 VLAN 数	VLAN ポート数
AX6300S シリーズ 共通	共存なし	16	200	10000
	共存あり	16	200	9000

注

MST インスタンス 0 は除きます。MST インスタンス 0 の対象 VLAN 数は 4095 となります。なお、運用中は運用コマンド `show spanning-tree port-count` で対象 VLAN 数と VLAN ポート数を確認できます。

(6) Ring Protocol

(a) Ring Protocol

Ring Protocol の収容条件を次の表に示します。

3. 収容条件

表 3-249 Ring Protocol 収容条件

項目	リング当たり	装置当たり
リング数	-	16 ¹
VLAN マッピング数	-	128 ²
VLAN グループ数	2	32
VLAN グループの VLAN 数	4094 ³	4094 ³
リングポート数 ⁴	2	32

(凡例) - : 該当なし

注 1

リングネットワークの構成によっては、最大数の 16 個まで設定できない場合があります。

注 2

Ring Protocol と VRF 機能を併用する (コンフィギュレーションコマンド `vrf mode` の `axrp-enable` パラメータ、または `axrp-enable-ipv4-ipv6` パラメータを設定している) 場合、装置当たりの VLAN マッピング数は 64 となります。

【OP-NPAR】

注 3

制御 VLAN 用に VLAN を一つ消費するため、VLAN グループに使用できる VLAN 最大数は 4094 となります。

注 4

チャンネルグループの場合は、チャンネルグループ単位で 1 ポートと数えます。

(b) 仮想リンク

仮想リンクの収容条件を次の表に示します。

表 3-250 仮想リンクの収容条件

項目	最大数
装置当たりの仮想リンク ID 数	1
仮想リンク当たりの VLAN 数	1
拠点当たりのリングノード数	2
ネットワーク全体での仮想リンクの拠点数	250

(c) Ring Protocol とスパンニングツリーまたは GSRP 併用時の物理ポート数

Ring Protocol とスパンニングツリー、または Ring Protocol と GSRP の併用時の収容条件を次の表に示します。なお、リングポートを収容している NIF が対象となります。

表 3-251 Ring Protocol とスパンニングツリーまたは GSRP 併用時の収容条件

NIF 略称	使用可能な物理ポート数 ^{1 2}
NH1G-16S	先頭から 4 ポートごとに 1 ポート、合計 4 ポートまで
NH1G-24T	12 ポートまで
NH1G-24S	12 ポートまで
NH1G-48T	先頭から 4 ポートごとに 1 ポート、合計 12 ポートまで
NH1GS-6M	すべてのポート
NH10G-1RX	すべてのポート

NIF 略称	使用可能な物理ポート数 ¹ ²
NH10G-4RX	1 ポートだけ
NH10G-8RX	1 ポートだけ

注 1

収容条件を超える物理ポートを使用した場合、常時または一時的にリングポートに高負荷のトラフィックが流れると、仮想リンクの制御フレームが廃棄されるおそれがあります。

注 2

収容条件は、対象 NIF でリングポートを収容した場合に、その NIF で使用可能な物理ポート数の最大となります。

(7) ポリシーベーススイッチング

ポリシーベーススイッチングでは、フィルタのフロー検出を使用して、ポリシーベーススイッチングの対象にするフローを検出します。なお、ポリシーベーススイッチングは、フロー系エントリの配分パターンが qos-only 以外、かつ経路系テーブル容量が extended のときだけ使用できます。

装置当たりのポリシーベーススイッチンググループのエントリ数を次の表に示します。

表 3-252 装置当たりのポリシーベーススイッチンググループのエントリ数

項目	エントリ数
アクセスリストエントリ数	「表 3-255 フィルタ・QoS エントリ数」を参照 ¹
ポリシーベーススイッチングリスト数	1000 ²
ポリシーベーススイッチングリスト情報内に設定できる経路数	8

注 1

エントリ数の算出方法は、「3.6.5 フィルタ・QoS」と同じです。

注 2

1 ポリシーベーススイッチングリスト情報を 1 リストとして登録します。このため、複数のアクセスリストで同一のポリシーベーススイッチングリスト情報を設定した場合、使用するリスト数は 1 リストと計算します。

(8) IGMP snooping / MLD snooping

IGMP snooping の収容条件を次の表に示します。IGMP snooping で学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。登録可能なマルチキャスト MAC アドレス数を次の表に示します。

表 3-253 IGMP snooping 収容条件

モデル	マルチキャスト同時使用	最大数		
		設定 VLAN 数 ¹	収容ポート数 ²	登録エントリ数
AX6300S シリーズ共通 (MSU-1A または MSU-1A1 搭載時)		256	16	1000
			32	500
			64	250
	x	256	16	2000
			32	1000

3. 収容条件

モデル	マルチキャスト同時使用	最大数		
		設定 VLAN 数 ¹	収容ポート数 ²	登録エントリ数
AX6300S シリーズ共通 (MSU-1B または MSU-1B1 搭載時)		256	64	500
			128	250
			32	2000
	×	256	64	1000
			32	4000
			64	2000
			128	1000

(凡例)

：IPv4 マルチキャスト，または IPv6 マルチキャストを同時使用する

×：IPv4 マルチキャスト，または IPv6 マルチキャストを同時使用しない

注 1

snooping が動作するポート数 (snooping 設定 VLAN に収容されるポートの総和) は装置全体で最大 4096 です。例えば、おのおの 10 ポート収容している 128 個の VLAN で snooping を動作させる場合、snooping 動作ポート数は 1280 となります。

注 2

リンクアグリゲーションポートは 1 ポートと数えます。

MLD snooping の収容条件を次の表に示します。MLD snooping で学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。登録可能なマルチキャスト MAC アドレス数を次の表に示します。

表 3-254 MLD snooping 収容条件

モデル	マルチキャスト同時使用	最大数		
		設定 VLAN 数 ¹	収容ポート数 ²	登録エントリ数
AX6300S シリーズ共通 (MSU-1A または MSU-1A1 搭載時)		256	16	1000
			32	500
			64	250
	×	256	16	2000
			32	1000
			64	500
			128	250
AX6300S シリーズ共通 (MSU-1B または MSU-1B1 搭載時)		256	32	2000
			64	1000
	×	256	32	4000
			64	2000
			128	1000

(凡例)

- : IPv4 マルチキャスト, または IPv6 マルチキャストを同時使用する
- × : IPv4 マルチキャスト, または IPv6 マルチキャストを同時使用しない

注 1

snooping が動作するポート数 (snooping 設定 VLAN に収容されるポートの総和) は装置全体で最大 4096 です。例えば, おおの 10 ポート収容している 128 個の VLAN で snooping を動作させる場合, snooping 動作ポート数は 1280 となります。

注 2

リンクアグリゲーションポートは 1 ポートと数えます。

3.6.5 フィルタ・QoS

(1) フィルタ・QoS

フィルタおよび QoS の収容条件を示します。ここでのエン트리数とは, コンフィグレーション (access-list , qos-flow-list) で設定したリストを装置内部で使用する形式 (エントリ) に変換したあとの数です。

(a) フィルタ・QoS エントリ数

フィルタ, および QoS の最大エン트리数を次の表に示します。

表 3-255 フィルタ・QoS エントリ数

モデル	フィルタの最大エン트리数		QoS の最大エン트리数	
	入出力インタフェース当たり	装置当たり	入出力インタフェース当たり	装置当たり
AX6300S シリーズ共通 (MSU-1A または MSU-1A1 搭載時)	4000	4000	4000	4000
AX6300S シリーズ共通 (MSU-1B または MSU-1B1 搭載時)	32000	32000	32000	32000

フロー制御はフローコンフィグレーションで設定しますが, リストに設定するフロー検出条件パラメータによって使用するエン트리数が異なります。複数エントリを使用するフロー検出条件のパラメータを次の表に示します。

表 3-256 複数エントリを使用するフロー検出条件

複数エントリを使用する フロー検出条件のパラメータ	使用エン트리数算出例
宛先 IPv4 アドレス, 送信元 IPv4 アドレス, 宛先 IPv6 アドレスを範囲指定	指定された IP アドレスが幾つのサブネットに区切られるかによってエン트리数が決定。 例えば, 宛先 IPv4 アドレスに 192.168.0.1 - 192.168.0.4 と指定した場合, 192.168.0.1/32, 192.168.0.2/31, 192.168.0.4/32 の三つのサブネットに区切られるため, 3 エントリとなります。

3. 収容条件

複数エントリを使用する フロー検出条件のパラメータ	使用エントリ数算出例
宛先ポート番号を範囲指定，送信元ポート番号を範囲指定	指定された値が最大 16 ビットのマスクで区切ったときに幾つに分けられるかによってエントリ数が決定。 例えば，宛先ポート番号に 135 - 140 と指定した場合， <ul style="list-style-type: none"> • 135/16 = 0000 0000 1000 0111 (2 進表記) • 136/14 = 0000 0000 1000 10xx (2 進表記) • 140/16 = 0000 0000 1000 1100 (2 進表記) の三つの領域に区切られるため，3 エントリとなります。
VLAN ID を複数指定	指定された VLAN ID 複数指定の中で，次に示す総和をエントリ数とします。 <ul style="list-style-type: none"> • 各単数指定部分：1 エントリ。 • 各範囲指定部分：前項と同様の方式で最大 12 ビットとして算出したエントリ数。 例えば，1，4-7，16-18 と指定した場合， 1:1/12 = 0000 0000 0001(2 進表記) 4-7:4/10 = 0000 0000 01xx(2 進表記) 16-18:16/11 = 0000 0001 000x(2 進表記) 18/12 = 0000 0001 0010(2 進表記) のエントリとなります。
TCP セッション維持 (ack フラグが ON，または rst フラグが ON のパケット検出)	2 エントリ使用します。

1 リストに上記のフロー検出条件を複数指定した場合，おのこのフロー検出条件で使用するエントリ数を掛け合わせた値が，1 リストで使用するエントリ数となります。

1 リストに上記のフロー検出条件を一つ指定した場合は，指定したフロー検出条件で使用するエントリ数が 1 リストで使用するエントリ数となります。

二つ以上指定した場合は，おのこのフロー検出条件で使用するエントリ数を掛け合わせた値が，1 リストで使用するエントリ数となります。

上記のフロー検出条件を指定していない場合は，1 リストで使用するエントリ数は 1 エントリとなります。

(b) 帯域監視機能でのエントリ数

帯域監視機能のエントリ数は，ストームコントロール機能と併用です。帯域監視モードと動作概要を次の表に示します。

表 3-257 帯域監視モードと動作概要

帯域監視モード	モード指定時の帯域監視機能の動作概要
upc-in-and-storm-control	<ul style="list-style-type: none"> • 帯域監視は受信側にだけ設定可 • 一つのフローエントリごとに，最大帯域制御または最低帯域監視のどちらかを設定可 • ストームコントロール機能が使用可能
upc-in-in	<ul style="list-style-type: none"> • 帯域監視は受信側にだけ設定可 • 一つのフローエントリで最大帯域制御と最低帯域監視の同時監視可 • ストームコントロール機能は使用不可
upc-in-out	<ul style="list-style-type: none"> • 帯域監視を受信側および送信側に設定可 • 一つのフローエントリごとに，最大帯域制御または最低帯域監視のどちらかを設定可 • ストームコントロール機能は使用不可

各モードの帯域監視機能の収容条件を次の表に示します。

表 3-258 装置当たりの帯域監視機能のエントリ数

帯域監視モード	帯域監視機能でのエントリ数	ストームコントロール機能
upc-in-and-storm-control	744	
upc-in-in	1000	×
upc-in-out	1000	×

(凡例) :有効 ×:無効

1 リストに指定した帯域監視機能の内容によって、1 リストで使用するエントリ数が異なります。その内容を次の表に示します。

表 3-259 1 リストで使用する帯域監視機能のエントリ数

1 リストに指定した帯域監視機能	使用エントリ数
最大帯域制御だけ	1
最低帯域監視だけ	1
最大帯域制御と最低帯域監視の両方を指定	2

(c) 階層化シェーパ

階層化シェーパのユーザ数の収容条件を次の表に示します。

表 3-260 階層化シェーパの最大ユーザ数

モデル	回線当たりの最大ユーザ数	装置当たりの最大ユーザ数
AX6304S	512	12288
AX6308S	512	24576

注 デフォルトユーザを含む数です。

(2) アクセスリストロギング

アクセスリストロギングの収容条件を示します。

アクセスリストロギングの最大アクセスリストログ情報数を次の表に示します。

表 3-261 最大アクセスリストログ情報数

モデル	最大アクセスリストログ情報数
AX6300S シリーズ共通 (MSU-1A または MSU-1A1 搭載時)	2000
AX6300S シリーズ共通 (MSU-1B または MSU-1B1 搭載時)	4000

3.6.6 レイヤ 2 認証

(1) レイヤ 2 認証

レイヤ 2 認証共通の収容条件を次の表に示します。

3. 収容条件

表 3-262 認証専用 IPv4 アクセスリストに設定できるフィルタ条件数

モデル	認証専用 IPv4 アクセスリストに設定できるフィルタ条件数
AX6300S シリーズ共通	10

(2) IEEE802.1X

IEEE802.1X の収容条件を次に示します。

本装置の IEEE802.1X では、三つの認証モードをサポートしています。

- ポート単位認証
- VLAN 単位認証（静的）
- VLAN 単位認証（動的）

VLAN 単位認証を使用する場合の、IEEE802.1X を設定可能な装置当たりの総ポート数を次の表に示します。

表 3-263 IEEE802.1X を設定可能な装置当たりの総ポート数

モデル	IEEE802.1X を設定可能な装置当たりの総ポート数
AX6300S シリーズ共通	1024

注

IEEE802.1X を設定可能な装置当たりの総ポート数とは、VLAN 単位認証を設定した VLAN での VLAN ポート数の総和の最大値を指します。VLAN 内にチャンネルグループが含まれている場合は、チャンネルグループを構成する物理ポート数に関係なく、チャンネルグループを 1 ポートとして計算します。また、1 ポートに VLAN が Tag で多重化されている場合も個別に数えます。例えば、一つのポートに Tag で多重化された 10 個の VLAN が設定されていた場合、その 10 個の VLAN で VLAN 単位認証を動作させると、総ポート数は 10 ポートになります。

各認証モードでの単位当たりの最大認証端末数を次の表に示します。

表 3-264 各認証モードでの単位当たりの最大認証端末数

モデル	認証モード		
	ポート単位認証	VLAN 単位認証 （静的）	VLAN 単位認証 （動的）
AX6300S シリーズ共通	256 / ポート	256 / VLAN	4096 / 装置

注

IEEE802.1X（VLAN 単位認証（動的））、Web 認証（ダイナミック VLAN モード）および MAC 認証（ダイナミック VLAN モード）を同時に動作させた場合は、それぞれの認証端末数の合計で装置当たり 4096 までとなります。

本装置の最大認証端末数を次の表に示します。

表 3-265 本装置の最大認証端末数

モデル	3 モード合計での最大認証端末数
AX6300S シリーズ共通	4096 / 装置

注

IEEE802.1X (ポート単位認証および VLAN 単位認証 (静的)), Web 認証 (固定 VLAN モード) および MAC 認証 (固定 VLAN モード) を同時に動作させた場合は, それぞれの認証端末数の合計で装置当たり 4096 までとなります。

(3) Web 認証

Web 認証の収容条件を次の表に示します。

表 3-266 Web 認証 (固定 VLAN モード) の最大認証端末数

モデル	装置当たりの最大認証端末数
AX6300S シリーズ共通	4096

注

Web 認証 (固定 VLAN モード), IEEE802.1X (ポート単位認証および VLAN 単位認証 (静的)) および MAC 認証 (固定 VLAN モード) を同時に動作させた場合は, それぞれの認証端末数の合計で装置当たり 4096 までとなります。

表 3-267 Web 認証 (ダイナミック VLAN モード) の最大認証端末数

モデル	装置当たりの最大認証端末数
AX6300S シリーズ共通	4096

注

Web 認証 (ダイナミック VLAN モード), IEEE802.1X (VLAN 単位認証 (動的)) および MAC 認証 (ダイナミック VLAN モード) を同時に動作させた場合は, それぞれの認証端末数の合計で装置当たり 4096 までとなります。

表 3-268 Web 認証 (レガシーモード) の最大認証端末数

モデル	装置当たりの最大認証端末数
AX6300S シリーズ共通	4096

注

Web 認証 (レガシーモード) および IEEE802.1X (VLAN 単位認証 (動的)) を同時に動作させた場合は, それぞれの認証端末数の合計で装置当たり 4096 までとなります。

表 3-269 Web 認証の装置当たりの内蔵 Web 認証 DB 登録ユーザ数

モデル	装置当たりの内蔵 Web 認証 DB 登録ユーザ数
AX6300S シリーズ共通	300

注

内蔵 Web 認証 DB に登録したユーザ ID を複数の端末で使用すると, 最大認証端末数まで端末を認証できます。ただし, 認証対象となるユーザ ID の数が内蔵 Web 認証 DB の最大登録数より多い場合は, RADIUS サーバを用いた RADIUS 認証方式を使用してください。

表 3-270 Web 認証の画面入れ替えで指定できる認証画面ファイル合計サイズ

モデル	装置当たりの指定できる認証画面ファイルの合計サイズ
AX6300S シリーズ共通	1024K バイト

3. 収容条件

表 3-271 Web 認証の画面入れ替えで指定できる認証画面ファイル数

モデル	装置当たりの指定できる認証画面ファイル数
AX6300S シリーズ共通	100

(4) MAC 認証

MAC 認証の収容条件を次の表に示します。

表 3-272 MAC 認証 (固定 VLAN モード) の最大認証端末数

モデル	装置当たりの最大認証端末数
AX6300S シリーズ共通	4096

注

MAC 認証 (固定 VLAN モード), IEEE802.1X (ポート単位認証および VLAN 単位認証 (静的)) および Web 認証 (固定 VLAN モード) を同時に動作させた場合は, それぞれの認証端末数の合計で 4096 までとなります。

表 3-273 MAC 認証 (ダイナミック VLAN モード) の最大認証端末数

モデル	装置当たりの最大認証端末数
AX6300S シリーズ共通	4096

注

MAC 認証 (ダイナミック VLAN モード), IEEE802.1X (VLAN 単位認証 (動的)) および Web 認証 (ダイナミック VLAN モード) を同時に動作させた場合は, それぞれの認証端末数の合計で 4096 までとなります。

表 3-274 MAC 認証の装置当たりの内蔵 MAC 認証 DB 登録ユーザ数

モデル	装置当たりの内蔵 MAC 認証 DB 登録ユーザ数
AX6300S シリーズ共通	1024

注

内蔵 MAC 認証 DB を使用した場合で VLAN ID をチェックしないときは, 認証対象となる MAC アドレスと VLAN ID 数 (Tag 使用時の VLAN ID 数も含む) の組み合わせ合計数が最大認証端末数に到達するまで端末を認証できます。ただし, 認証する端末 (MAC アドレス) と VLAN ID の組み合わせ合計数が内蔵 MAC 認証 DB の最大登録数より多い場合は, RADIUS サーバを用いた RADIUS 認証方式を使用してください。

(5) 認証 VLAN

認証 VLAN の収容条件を次の表に示します。

表 3-275 最大認証端末数

モデル	装置当たりの最大認証端末数
AX6300S シリーズ共通	4096

表 3-276 接続可能な認証サーバ数

モデル	装置当たりの接続可能な認証サーバ数
AX6300S シリーズ共通	10

表 3-277 設定可能な認証済み VLAN 数

モデル	装置当たりの設定可能な認証済み VLAN 数
AX6300S シリーズ共通	4094

3.6.7 DHCP snooping

DHCP snooping の収容条件を次の表に示します。

表 3-278 DHCP snooping の最大エントリ数

フロー系テーブル容量名称	フロー系テーブルエントリ配分パターン	バインディングデータベースエントリ数 ¹		端末フィルタエントリ数 ²
		ダイナミック / スタティックの合計	スタティック	
standard	default (フィルタ, QoS 均等)	-	-	-
standard-advance	default (フィルタ, QoS 均等)	1100	256	1100
extended	default (フィルタ, QoS 均等)	-	-	-
	filter-only (フィルタ専用)	-	-	-
	qos-only (QoS 専用)	-	-	-
	filter (フィルタ主体)	-	-	-
	qos (QoS 主体)	-	-	-
extended-advance	default (フィルタ, QoS 均等)	8000	1024	8000
	filter-only (フィルタ専用)	8000	1024	8000
	qos-only (QoS 専用)	-	-	-
	filter (フィルタ主体)	8000	1024	8000
	qos (QoS 主体)	2000	1024	2000

(凡例) - : DHCP snooping は使用できない

注 1

untrust ポート配下の端末当たり 1 エントリを消費します。

注 2

バインディングデータベースエントリ配下のポート当たり 1 エントリを消費します。
チャンネルグループの場合、チャンネルグループ当たりのポート数を数えます。

表 3-279 DHCP snooping の最大 VLAN 数

フロー系テーブル容量名称	最大 VLAN 数
standard	-
standard-advance	512
extended	-
extended-advance	2048

3. 収容条件

(凡例) - : DHCP snooping は使用できない

3.6.8 冗長化構成による高信頼化

(1) GSRP

GSRP の収容条件を次の表に示します。

GSRP の VLAN ポート数は、チャンネルグループの場合、チャンネルグループ当たりの物理ポート数を数えます。

表 3-280 GSRP 収容条件

モデル	レイヤ 3 冗長機能	VLAN ポート数の合計	VLAN グループ最大数	VLAN グループ当たりの VLAN 最大数
AX6300S シリーズ 共通	あり	10000	128	4095
	なし	100000	128	4095

注

GSRP と VRF 機能を併用する (コンフィグレーションコマンド `vrf mode` の `gsrp-enable-ipv4-ipv6` パラメータを設定している) 場合、VLAN グループ当たりの VLAN 最大数は 250 となります。【OP-NPAR】

(2) VRRP

VRRP に関する収容条件を次の表に示します。

表 3-281 VRRP 収容条件

モデル	仮想ルータ最大数		track 設定最大数	track 割り当て最大数	
	インタフェース当たり	装置当たり		仮想ルータ当たり	装置当たり
AX6300S シリーズ 共通	255 ¹	255 ¹	255	16 ²	255 ²

注 1 IPv4/IPv6 の仮想ルータの合計数です。

注 2 障害監視インタフェースと VRRP ポーリングの合計数です。

表 3-282 VRRP 収容条件 (グループ切替機能使用時)

モデル	仮想ルータ最大数		最大グループ数	1グループ当たりの最大フォロー仮想ルータ数	track 設定最大数	track 割り当て最大数	
	インタフェース当たり	装置当たり				仮想ルータ当たり	装置当たり
AX6300S シリーズ 共通	255 ¹	4095 ¹	255	4094	255	16 ²	255 ²

注 1 IPv4/IPv6 の仮想ルータの合計数は 255 までです。ただし、グループ切替機能を利用し、フォロー仮想ルータを作成することで、最大 4095 の仮想ルータが動作できます。

注 2 障害監視インタフェースと VRRP ポーリングの合計数です。

3.6.9 ネットワークの障害検出による高信頼化機能

(1) IEEE802.3ah/UDLD

IEEE802.3ah/UDLD の収容条件を次の表に示します。

表 3-283 設定可能ポート数

モデル	設定可能ポート数
AX6304S	96
AX6308S	192

(2) L2 ループ検知

(a) L2 ループ検知フレーム送信レート

L2 ループ検知の L2 ループ検知フレーム送信レートを次の表に示します。

表 3-284 L2 ループ検知フレーム送信レート

モデル	L2 ループ検知フレームの送信レート (装置当たり) ¹	
	スパニングツリー, GSRP, Ring Protocol のどれかを使用している場合	スパニングツリー, GSRP, Ring Protocol のどれも使用していない場合
AX6300S シリーズ共通	90pps (推奨値) ²	600pps (最大値) ³

- L2 ループ検知フレーム送信レート算出式

L2 ループ検知フレーム送信対象の VLAN ポート数 ÷ L2 ループ検知フレームの送信レート (pps) × 送信間隔 (秒)

注 1

送信レートは上記の条件式に従って、自動的に 600pps 以内で変動します。

注 2

スパニングツリー, GSRP, Ring Protocol のどれかを使用している場合は、90pps 以下に設定してください。90pps より大きい場合、スパニングツリー, GSRP, Ring Protocol の正常動作を保障できません。

注 3

600pps を超えるフレームは送信しません。送信できなかったフレームに該当するポートや VLAN ではループ障害を検知できなくなります。必ず 600pps 以下に設定してください。

(b) ネットワーク全体での動作可能装置数

ネットワーク全体で本機能が動作可能な装置台数は、AX6700S シリーズ, AX6600S シリーズ, AX6300S シリーズの合計で 64 台までです。

(c) 物理ポート数

L2 ループ検知を運用時の物理ポート数の収容条件を次の表に示します。

表 3-285 物理ポートの収容条件

NIF 略称	使用可能な物理ポート数
NH1G-16S	先頭から 4 ポートごとに 1 ポート, 合計 4 ポートまで
NH1G-24T	12 ポートまで
NH1G-24S	12 ポートまで

3. 収容条件

NIF 略称	使用可能な物理ポート数
NH1G-48T	先頭から 4 ポートごとに 1 ポート, 合計 12 ポートまで
NH1GS-6M	すべてのポート
NH10G-1RX	すべてのポート
NH10G-4RX	1 ポートだけ
NH10G-8RX	1 ポートだけ

注

収容条件を超える物理ポートを使用した場合, 常時または一時的に高負荷のトラフィックが流れると, L2 ループ検知フレームが廃棄されるおそれがあります。廃棄されることでループ障害の検知が遅れる場合があります。

(3) CFM

CFM の収容条件を次の表に示します。

表 3-286 CFM の収容条件

モデル	ドメイン数	MA 数	MEP 数	MIP 数	CFM ポート 総数 ^{1 2}	リモート MEP 総数 ^{2 3}
AX6300S シリーズ共通	8 / 装置	192 / 装置	192 / 装置	192 / 装置	1024 / 装置	8064 / 装置

注 1

CFM ポート総数とは, MA のプライマリ VLAN のうち, CFM のフレームを送信する VLAN ポートの総数です。

Down MEP だけの MA の場合

Down MEP の VLAN ポートの総数

Up MEP を含む MA の場合

プライマリ VLAN の全 VLAN ポートの総数

なお, CFM ポート総数は運用コマンド `show cfm summary` で確認できます。

注 2

CFM ポート総数およびリモート MEP 総数は, CCM 送信間隔がデフォルト値のときの収容条件です。CCM 送信間隔を変更すると, CFM ポート総数およびリモート MEP 総数の収容条件が変わりません。CCM 送信間隔による CFM ポート総数およびリモート MEP 総数の収容条件を次の表に示します。

表 3-287 CCM 送信間隔による収容条件

モデル	CCM 送信間隔	CFM ポート総数	リモート MEP 総数
AX6300S シリーズ共通	1 分以上	1024 / 装置	8064 / 装置
	10 秒	256 / 装置	4032 / 装置
	1 秒	192 / 装置	400 / 装置

注 3

リモート MEP 総数とは, 自装置以外の MEP の総数です。MEP からの CCM 受信性能に影響しません。リモート MEP 総数は運用コマンド `show cfm remote-mep` で確認できます。

表 3-288 CFM の物理ポートおよびチャンネルグループの収容条件

モデル	MEP・MIP を設定可能な物理ポートおよびチャンネルグループの総数
AX6300S シリーズ 共通	全ポート

注

MEP・MIP は同一ポートに対して複数設定できます。チャンネルグループの場合は、チャンネルグループ単位で 1 ポートと数えます。

表 3-289 CFM のデータベース収容条件

モデル	MEP CCM データベース エントリ数	MIP CCM データベース エントリ数	Linktrace データベース エントリ数
AX6300S シリーズ共通	63 / MEP	12288 / 装置	1024 / 装置

注

1 ルート当たり 256 装置の情報を保持する場合は、最大で 4 ルート分を保持します (1024 ÷ 256 装置 = 4 ルート)。

3.6.10 隣接装置情報の管理 (LLDP/OADP)

隣接装置情報 (LLDP/OADP) の収容条件を次の表に示します。

表 3-290 隣接装置情報 (LLDP/OADP) の収容条件

モデル	LLDP 隣接装置情報	OADP 隣接装置情報
AX6300S シリーズ共通	192	250

注

LLDP/OADP の隣接装置情報数とは、本装置に接続されている隣接装置から収集できる情報のことで、基本的に 1 隣接装置当たり 1 情報を収集できます。

3.6.11 IPv4・IPv6 パケット中継

(1) IP アドレスを設定できるインタフェース数

本装置は次のインタフェースに IP アドレスを設定できます。

- VLAN インタフェース
- マネージメントポート

ここでは、IP アドレスを設定できるインタフェースの最大数について説明します。また、設定できる IP アドレスの最大数について説明します。

インタフェースに対してサポートする最大インタフェース数を次の表に示します。ここで示す値は、IPv4 と IPv6 との合計の値です。なお、IPv4 と IPv6 を同一のインタフェースに設定することも、個別に設定することもできます。

表 3-291 インタフェースに対する最大インタフェース数

モデル	VLAN インタフェース数 (装置当たり)	マネージメントポート (装置当たり)
AX6300S シリーズ共通	4095	1

(2) マルチホームの最大サブネット数

LAN のマルチホーム接続では一つのインタフェースに対して、複数の IPv4 アドレス、または IPv6 アドレスを設定できます。

(a) IPv4 の場合

IPv4 でのマルチホームの最大サブネット数を次の表に示します。ただし、マネージメントポートは IPv4 のマルチホーム不可のため 1 になります。

表 3-292 マルチホームの最大サブネット数 (IPv4 の場合)

モデル	マルチホーム サブネット数 (インタフェース当たり)
AX6300S シリーズ共通	256

(b) IPv6 の場合

IPv6 でのマルチホームの最大サブネット数を次の表に示します。なお、ここで示す値にはリンクローカルアドレスを含みます。一つのインタフェースには必ず一つのリンクローカルアドレスが設定されます。このため、すべてのインタフェースで IPv6 グローバルアドレスだけを設定した場合、実際に装置に設定される IPv6 アドレス数は、表の数値に自動生成される IPv6 リンクローカルアドレス数 1 を加算した 8 になります。

表 3-293 マルチホームの最大サブネット数 (IPv6 の場合)

モデル	マルチホーム サブネット数 (インタフェース当たり)
AX6300S シリーズ共通	7

(3) IP アドレス最大設定数

(a) IPv4 アドレス

コンフィグレーションで設定できる IPv4 アドレスの最大数を次の表に示します。なお、この表で示す値は、インタフェースに設定できる IPv4 アドレス数です。

表 3-294 コンフィグレーションで装置に設定できる IPv4 アドレスの最大数

モデル	VLAN インタフェースに設定できる IPv4 アドレス数 (装置当たり)	マネージメントポートに設定できる IPv4 アドレス数 (装置当たり)
AX6300S シリーズ共通	4096	1

(b) IPv6 アドレス

コンフィグレーションで設定できる装置当たりの IPv6 アドレスの最大数を次の表に示します。なお、ここで示す値はインタフェースに設定する IPv6 アドレスの数です。また、IPv6 リンクローカルアドレスの

数も含まれます。一つのインタフェースには必ず一つの IPv6 リンクローカルアドレスが設定されます。このため、すべてのインタフェースに IPv6 グローバルアドレスを設定した場合、インタフェースには自動で IPv6 リンクローカルアドレスが付与され、実際に装置に設定される IPv6 アドレスの数は次の表に示す値となります。

表 3-295 コンフィグレーションで装置に設定できる IPv6 アドレスの最大数

モデル	VLAN インタフェースに設定できる IPv6 アドレス数 (装置当たり)	マネージメントポートに設定できる IPv6 アドレス数 (装置当たり)
AX6300S シリーズ共通	4096	7

表 3-296 VLAN インタフェースに設定される IPv6 アドレス数

コンフィグレーションで VLAN インタフェースに設定する IPv6 アドレスの数		自動で設定する IPv6 リンクローカルアドレスの数	VLAN インタフェースに設定される IPv6 アドレス数
IPv6 リンクローカルアドレス	IPv6 グローバルアドレス		
4095	0	0	4095
0	4096	4095	8191

注 IPv6 グローバルアドレスは、マルチホームを使用することで 4096 まで設定できます。

表 3-297 マネージメントポートに設定される IPv6 アドレス数

コンフィグレーションでマネージメントポートに設定する IPv6 アドレスの数		自動で設定する IPv6 リンクローカルアドレスの数	マネージメントポートに設定される IPv6 アドレス数
IPv6 リンクローカルアドレス	IPv6 グローバルアドレス		
1	0	0	1
0	7	1	8

(4) 最大相手装置数

本装置が接続する通信可能な最大相手装置数を示します。この場合の相手装置はスイッチに限らず、端末も含まれます。

(a) ARP エントリ数

IPv4 の場合、ARP によって、送信しようとするパケットの宛先アドレスに対応するハードウェアアドレスを決定します。最大相手装置数は、ARP エントリ数によって決まります。ARP エントリはコンフィグレーションコマンドを使用することで、スタティックに 4096 エントリ登録できます。本装置でサポートする ARP エントリの最大数については、次の表を参照してください。最大エントリ数は、スタティックで登録したエントリ数を含みます。

- 表 3-224 standard の経路系テーブルエントリ数
- 表 3-225 extended の経路系テーブルエントリ数

(b) NDP エントリ数

IPv6 の場合、NDP でのアドレス解決によって、送信しようとするパケットの宛先アドレスに対応する

3. 収容条件

ハードウェアアドレスを決定します。最大相手装置数は NDP エントリ数によって決まります。NDP エントリは、コンフィグレーションコマンドを使用することで、スタティックに 4096 エントリ登録できます。本装置でサポートする NDP エントリの最大数については、次の表を参照してください。最大エントリ数は、スタティックで登録したエントリ数を含みます。

- 表 3-224 standard の経路系テーブルエントリ数
- 表 3-225 extended の経路系テーブルエントリ数

(c) RA の最大相手端末数

RA ではルータから通知される IPv6 アドレス情報を基に端末でアドレスを生成します。本装置での最大相手端末数を次の表に示します。

表 3-298 RA の最大相手端末数

モデル	RA の最大相手端末数	
	インタフェース当たり	装置当たり
AX6300S シリーズ共通	4096	4096

(5) ポリシーベースルーティング

ポリシーベースルーティングでは、フィルタのフロー検出を使用して、ポリシーベースルーティングの対象にするフローを検出します。なお、フロー系エントリの配分パターンが qos-only の場合、ポリシーベースルーティングは使用できません。

(a) ポリシーベースルーティングの収容条件

アクセスリストの動作に中継先の経路を指定

アクセスリストの動作に中継先の経路を指定する場合の収容条件を次の表に示します。

表 3-299 装置当たりのポリシーベースルーティングのエントリ数

項目	IPv4 ポリシーベースルーティング	IPv6 ポリシーベースルーティング
アクセスリストエントリ数	「表 3-255 フィルタ・QoS エントリ数」を参照 ¹	「表 3-255 フィルタ・QoS エントリ数」を参照 ¹
ネクストホップエントリ数	256 ²	256 ²

注 1

エントリ数の算出方法は、「3.6.5 フィルタ・QoS」と同じです。

注 2

1 ネクストホップを 1 エントリとして登録します。このため、複数のアクセスリストで同一のネクストホップを設定した場合、使用するエントリ数は 1 エントリと計算します。

アクセスリストの動作にポリシーベースルーティングリスト情報を指定

アクセスリストの動作にポリシーベースルーティングリスト情報を指定する場合の収容条件を次の表に示します。

表 3-300 装置当たりのポリシーベースルーティンググループのエントリ数

項目	IPv4 ポリシーベースルーティンググループ	IPv6 ポリシーベースルーティンググループ
アクセスリストエントリ数	「表 3-255 フィルタ・QoS エントリ数」を参照 ¹	-
ポリシーベースルーティングリスト数	256 ²	-
ポリシーベースルーティングリスト情報内に設定できる経路数	8	-
ポリシーベースルーティングのトラッキング機能と連携できる経路数	1024 ³	-

(凡例) - : 該当なし

注 1

エントリ数の算出方法は、「3.6.5 フィルタ・QoS」と同じです。

注 2

1 ポリシーベースルーティングリスト情報を 1 リストとして登録します。このため、複数のアクセスリストで同一のポリシーベースルーティングリスト情報を設定した場合、使用するリスト数は 1 リストと計算します。

注 3

1 トラック ID を 1 エントリとして登録します。このため、複数の経路で同一のトラック ID を設定した場合、使用するエントリ数は 1 エントリと計算します。

(b) トラッキング機能の収容条件

ポリシーベースルーティングのトラッキング機能の収容条件を次の表に示します。

表 3-301 トラッキング機能の収容条件

項目	収容条件
トラックの数	1024
ポーリング監視トラックの数	1024

注 コンフィグレーションコマンド `type icmp` を設定したトラックの数です。

(6) DHCP/BOOTP リレー

DHCP/BOOTP リレーの収容条件を次の表に示します。

表 3-302 DHCP/BOOTP リレーの最大数

モデル	クライアント接続インタフェース数	サーバ台数 (グローバルネットワーク、 VRF ごと)	VRF 使用時の装置 当たりのサーバ台数
AX6300S シリーズ共通	2048	16	256

(7) IPv6 DHCP リレー

IPv6 DHCP リレーの収容条件を次の表に示します。

3. 収容条件

表 3-303 IPv6 DHCP リレーの最大数

モデル	装置当たりの最大数	
	配布プレフィックス数	インタフェース数
AX6300S シリーズ共通	1024	1024

注

クライアントを直接収容した場合に IPv6 DHCP サーバによって配布される PD プレフィックス数です。ほかのリレー経由の packets や PD プレフィックス以外の情報は、この条件に関係なく中継できます。

(8) DHCP サーバ

DHCP サーバで設定できるインタフェース数および配布可能 IP アドレス数などを次の表に示します。

表 3-304 DHCP サーバの最大数

モデル	最大配布可能 IP アドレス数	最大固定 IP アドレス割り当て数	最大インタフェース数	最大管理サブネット数
AX6300S シリーズ共通	8192	320	2048	2048

(9) IPv6 DHCP サーバ

IPv6 DHCP サーバの収容条件を次の表に示します。

表 3-305 IPv6 DHCP サーバの最大数

モデル	装置当たりの最大数	
	インタフェース数	最大配布可能 Prefix
AX6300S シリーズ共通	1024	1024

3.6.12 IPv4・IPv6 ルーティングプロトコル

(1) 最大隣接ルータ数

最大隣接ルータ数の定義を次の表に示します。

表 3-306 最大隣接ルータ数の定義

ルーティングプロトコル別	最大隣接ルータ数の定義
スタティックルーティング	ネクストホップ・アドレスの数
RIP, RIPng	RIP/RIPng が動作するインタフェース数
OSPF, OSPFv3	本装置が OSPF/OSPFv3 指定ルータ (DR, BDR) になるネットワークの場合、そのネットワーク上のほかすべての OSPF/OSPFv3 ルータ数。本装置が OSPF/OSPFv3 指定ルータにならないネットワークの場合、そのネットワーク上の指定ルータ (DR, BDR) 数。
BGP4, BGP4+	BGP4/BGP4+ ピア数

最大隣接ルータ数を次の表に示します。

表 3-307 最大隣接ルータ数

ルーティングプロトコル	最大隣接ルータ数	
	ポリシーベースルーティングのトラッキング機能を使用しない	ポリシーベースルーティングのトラッキング機能を使用する
スタティックルーティング (IPv4, IPv6 の合計)	4096	4096
RIP	200	100
RIPng	200	100
OSPF	200	100
OSPFv3	100	50
BGP4	200	100
BGP4+	200	100
RIP, OSPF, BGP4, RIPng, OSPFv3, BGP4+ の合計	256	128

注

動的監視機能を使用する隣接ルータは、ポーリング間隔によって数が制限されます。詳細は、次の表を参照してください。

表 3-308 スタティックの動的監視機能を使用できる最大隣接ルータ数

ポーリング周期	動的監視機能を使用できる最大隣接ルータ数
1 秒	60
5 秒	300
10 秒	600
20 秒	1200

(2) 経路エントリ数と最大隣接ルータ数の関係

最大経路エントリ数と最大隣接ルータ数の関係を次の表に示します。

表 3-309 経路エントリ数と最大隣接ルータ数の関係

ルーティングプロトコル	経路エントリ数 ¹	最大隣接ルータ数 ²	
		ポリシーベースルーティングのトラッキング機能を使用しない	ポリシーベースルーティングのトラッキング機能を使用する
RIP	1000	100	50
	2000	50	25
	10000	10	5
RIPng	1000	100	50
	2000	50	25
	10000	10	5
OSPF ^{3 4}	1000	200	100
	2000	100	50
	5000	40	20

3. 収容条件

ルーティングプロトコル	経路エントリ数 ¹	最大隣接ルータ数 ²	
		ポリシーベースルーティングのトラッキング機能を使用しない	ポリシーベースルーティングのトラッキング機能を使用する
	10000	20	10
OSPFv3 ^{3 5}	1000	100	50
	2000	50	25
	5000	20	10
	10000	10	5
BGP4	6	200	100
BGP4+	6	200	100

注 1

経路エントリ数は代替経路を含みます。

注 2

各ルーティングプロトコル (RIP, RIPng, OSPF, OSPFv3, BGP4, BGP4+) を併用して使用する場合の最大隣接ルータ数は、それぞれ $1/n$ (n : 使用ルーティングプロトコル数) です。例えば、BGP4, BGP4+ を使用しないで、OSPF (1000 経路) と OSPFv3 (1000 経路) を併用して使用する場合の最大隣接ルータ数は $1/2$ となり、OSPF では 100, OSPFv3 では 50 となります。

注 3

OSPF/OSPFv3 の最大経路エントリ数は LSA 数を意味します。

注 4

VRF で OSPF を使用している場合、装置全体の最大隣接ルータ数は 200 ですが、各 VRF で保持している LSA 数 × 各 VRF の隣接ルータ数の総計が 20 万を超えないようにしてください。

注 5

VRF で OSPFv3 を使用している場合、装置全体の最大隣接ルータ数は 100 ですが、各 VRF で保持している LSA 数 × 各 VRF の隣接ルータ数の総計が 10 万を超えないようにしてください。

注 6

「表 3-229 MSU-1A および MSU-1A1 経路配分パターンと収容経路エントリ数 (その 1)」, 「表 3-230 MSU-1A および MSU-1A1 経路配分パターンと収容経路エントリ数 (その 2)」, 「表 3-233 MSU-1B および MSU-1B1 経路配分パターンと収容経路エントリ数 (その 1)」, および 「表 3-234 MSU-1B および MSU-1B1 経路配分パターンと収容経路エントリ数 (その 2)」を参照してください。

(3) 本装置で設定できるコンフィギュレーションの最大数

ルーティングプロトコルについて、設定できるコンフィギュレーションの最大数を次の表に示します。

なお、この表で示す値はコンフィギュレーションで設定できる最大数です。運用する際は本章にある収容条件をすべて満たすようにしてください。

表 3-310 コンフィギュレーションの最大設定数

分類	コンフィギュレーションコマンド	最大数の定義	最大設定数
IPv4 スタティック	ip route	テーブル容量が standard 時の設定行数	8192
		テーブル容量が extended 時の設定行数	16384

分類	コンフィグレーション コマンド	最大数の定義	最大 設定数	
IPv6 スタティック	ipv6 route	テーブル容量が standard 時の設定 行数	8192	
		テーブル容量が extended 時の設定 行数	16384	
IPv4 集約経路	ip summary-address	設定行数	1024	
IPv6 集約経路	ipv6 summary-address	設定行数	1024	
RIP	network	設定行数	256	
	ip rip authentication key	設定行数	512	
OSPF	area range	設定行数	1024	
	area virtual-link	authentication-key , message-digest-key パラメータを 設定した行数の総計	512	
	ip ospf authentication-key ip ospf message-digest-key	各設定行数の総計	512	
	network	設定行数	512	
	router ospf	設定行数	256	
BGP4	network	設定行数	1024	
OSPFv3	area range	設定行数	1024	
	ipv6 router ospf	設定行数	128	
BGP4+	network	設定行数	1024	
経路フィルタ	distribute-list in (RIP) distribute-list out (RIP) redistribute (RIP)	各設定行数の総計	2048	
	distribute-list in (OSPF) distribute-list out (OSPF) redistribute (OSPF)	各設定行数の総計	2048	
	distribute-list in (BGP4) distribute-list out (BGP4) redistribute (BGP4)	各設定行数の総計	2048	
	distribute-list in (RIPng) distribute-list out (RIPng) redistribute (RIPng)	各設定行数の総計	2048	
	distribute-list in (OSPFv3) distribute-list out (OSPFv3) redistribute (OSPFv3)	各設定行数の総計	1024	
	distribute-list in (BGP4+) distribute-list out (BGP4+) redistribute (BGP4+)	各設定行数の総計	2048	
	ip as-path access-list	設定 <Id> の種類数		1024
		設定行数		4096
	ip community-list	設定 <Id> の種類数		512
		standard 指定の設定行数		1024
expanded 指定の設定行数			1024	
ip prefix-list	設定 <Id> の種類数		2048	

3. 収容条件

分類	コンフィギュレーション コマンド	最大数の定義	最大 設定数
		設定行数	8192
	ipv6 prefix-list	設定 <Id> の種類数	2048
		設定行数	8192
	neighbor in (BGP4) neighbor out (BGP4)	<IPv4-Address> の設定行数の総計	256
		<Peer-Group> の設定行数の総計	256
	neighbor in (BGP4+) neighbor out (BGP4+)	<IPv6-Address> の設定行数の総計	256
		<Peer-Group> の設定行数の総計	256
	route-map	設定 <Id> の種類数	1024
		設定 <Id> と <Seq> の組み合わせ 種類数	4096
	match as-path	各設定行で指定したパラメータの 総計	4096
	match community	各設定行で指定したパラメータの 総計	4096
	match interface	各設定行で指定したパラメータの 総計	2048
	match ip address match ipv6 address	各設定行で指定したパラメータの 総計	4096
	match ip route-source match ipv6 route-source	各設定行で指定したパラメータの 総計	2048
	match origin	設定行数	2048
	match protocol	各設定行で指定したパラメータの 総計	4096
	match route-type	設定行数	2048
	match tag	各設定行で指定したパラメータの 総計	2048
	match vrf	各設定行で指定したパラメータの 総計	4096
	set as-path prepend count set distance set local-preference set metric set metric-type set origin set tag	どれか一つが設定された route-map の、<Id> と <Seq> の 組み合わせ種類数	4096
	set community	各設定行で指定したパラメータの 総計	2048
	set community-delete	各設定行で指定したパラメータの 総計	2048

3.6.13 IPv4・IPv6 マルチキャストルーティングプロトコル

(1) IPv4 マルチキャスト

IPv4 マルチキャストを設定できるインタフェース数およびルーティングテーブルのエントリ数を次の表に示します。

複数の VRF で IPv4 マルチキャストを使用する場合、グローバルネットワークとすべての VRF の合計を本収容条件内に収めてください。ただし、MSU-1A および MSU-1A1 では VRF 機能をサポートしていません。

なお、PIM-DM はグローバルネットワークでだけ動作します。また、本装置では、PIM-SM と PIM-DM は同時に動作できません。

表 3-311 IPv4 マルチキャストの最大数

項目	最大数	
	MSU-1A MSU-1A1	MSU-1B MSU-1B1
PIM-SM/SSM または PIM-DM マルチキャストインタフェース数 ¹	127 / 装置	255 / 装置
IGMP 動作インタフェース数	127 / 装置	255 / 装置
マルチキャスト送信元の数	256 / グループ 3000 / 装置	256 / グループ 3000 / 装置
PIM-SM/SSM マルチキャスト経路情報のエントリ ((S,G) エントリ, (*,G) エントリ, およびネガティブキャッシュ) 数, または PIM-DM マルチキャスト経路情報のエントリ ((S,G) エントリ) 数 ¹ S: 送信元 IP アドレス G: グループアドレス	4000 / 装置	8000 / 装置
IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連携動作させる設定数 (ソース, グループのペア数) ²	256 / 装置	256 / 装置
IGMPv3 で 1Report につき処理できる record 情報 ³	32record / メッセージ 32 ソース / record	32record / メッセージ 32 ソース / record
IGMP 加入グループ数 ^{4 5}	2000 / 装置	3000 / 装置
マルチキャストルータ隣接数 ¹	256 / 装置	256 / 装置
ランデブーポイント数	2 / グループ	2 / グループ
1 装置当たりランデブーポイントで設定できるグループ数 ⁶	128 / 装置	128 / 装置
1 ネットワーク (VPN) 当たりランデブーポイントに設定できる延べグループ数	128 / ネットワーク 128 / 装置	128 / ネットワーク (VPN) 256 / 装置 ⁷
1 ネットワーク (VPN) 当たりの BSR 候補数	16 / ネットワーク 16 / 装置	16 / ネットワーク (VPN) 256 / 装置 ⁷
静的加入グループ数 ⁸	256 / 装置	256 / 装置
静的ランデブーポイント (RP) ルータアドレス数	16 / 装置	16 / 装置
IGMP グループ当たりのソース数	256 / グループ	256 / グループ
マルチキャスト中継エントリの延べ下流インタフェース数 ^{9 10}	140000 / 装置	280000 / 装置
マルチキャストを設定できる VRF 数 ¹¹	-	249 / 装置
エクストラネットのマルチキャストフィルタ数 ¹²	-	512 / 装置
エクストラネットで使用する route-map 数	-	256 / 装置 256 / VRF
PIM-SM VRF ゲートウェイ動作マルチキャストアドレス数 ¹³	-	256 / 装置 256 / VRF

3. 収容条件

(凡例) - : 該当なし

注 1

PIM-DM を使用する場合、隣接ルータ数によって使用できるマルチキャスト経路情報のエントリ数が異なります。「表 3-312 PIM-DM での隣接ルータ数に対するマルチキャスト経路情報のエントリ数」に示す範囲内で使用してください。

注 2

マルチキャストで使用するインタフェース数および加入グループ数によって設定できる数が変わります。「表 3-313 使用インタフェース数に対する IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数」および「表 3-314 加入グループ数に対する IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数」に示す範囲内で使用してください。加入グループ数は、動的および静的加入グループ数の総計です。同一グループアドレスが異なるインタフェースに加入している場合、加入グループ数は一つではなく、加入したインタフェースの数になります。

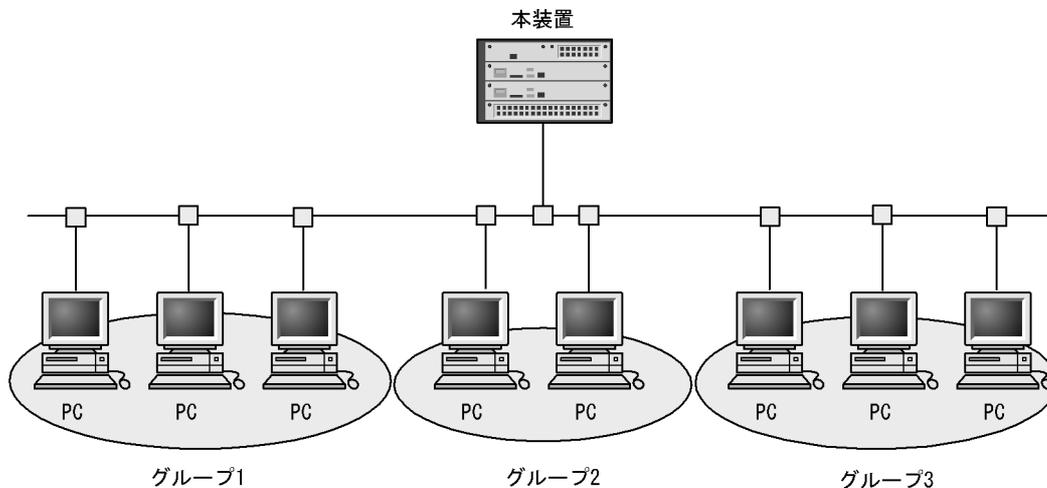
注 3

一つの Report メッセージで処理できるソース数は延べ 256 ソースまでです。ソース情報のない record も 1 ソースとして数えます。

IGMPv3 (EXCLUDE モード) で PIM-SSM を連携動作させる設定をした場合、その設定に一致した EXCLUDE record で定義されているソース数を数えます。また、受信した Report メッセージ内に EXCLUDE record が複数存在し、IGMPv3 (EXCLUDE モード) で PIM-SSM を連携動作させる設定で追加したソース数が延べ 256 を超えた場合、以降のそのメッセージ内の EXCLUDE record で、連携動作の対象となる EXCLUDE record についてマルチキャスト中継情報は作成しません。

注 4

本装置に直接接続しているグループの数を示します。IGMPv3 使用時に送信元を指定する場合のグループ数は、送信元とグループの組み合わせの数となります。次の図の例ではグループ数が 3 になります。



注 5

IPv4 でのインタフェース当たりの加入可能グループ数を「表 3-315 IPv4 でのインタフェース当たりの加入グループ数」に示します。

注 6

グループを指定しないでランデブーポイントを設定した場合、デフォルトグループが設定されます。グローバルネットワークおよび VRF でランデブーポイントを設定する場合、デフォルトグループも 1 グループとして、装置内またはネットワーク (VPN) 内の総グループ数が収容条件内になるように設定してください。

注 7

本装置のグローバルネットワークとすべての VRF に接続するネットワーク (VPN) 上の総数です。

注 8

静的加入グループ数とは、各マルチキャストインタフェースで静的加入するグループアドレスの総数です。同一グループアドレスを複数の異なるインタフェースに静的加入設定した場合、静的加入グループ数は一つではなく、静

的加入設定したインタフェースの数になります。
また、PIM-SM VRF ゲートウェイで指定したグループアドレスの延べ数との合計になります。

注 9

構成およびリソース状況によっては最大数が MSU-1A または MSU-1A1 搭載時は 140000 以下、MSU-1B または MSU-1B1 搭載時は 280000 以下となることがあります。

注 10

マルチキャスト中継エントリの延べ下流インタフェース数は、IPv4 マルチキャストと IPv6 マルチキャストの合計です。

注 11

PIM-SM/SSM 使用時だけ設定できます。

注 12

すべての route-map で指定した access-list 内のアドレスの延べ数です。

注 13

エクストラネットで指定した route-map を使用します。route-map に指定した access-list 内で、ホストアドレス (32 ビットマスク) として指定したマルチキャストアドレスが対象となります。

装置当たりの上限は、すべての VRF で指定した PIM-SM VRF ゲートウェイのグループアドレスの延べ数です。
また、静的加入グループ数で指定したグループアドレス数との合計になります。

表 3-312 PIM-DM での隣接ルータ数に対するマルチキャスト経路情報のエントリ数

隣接ルータ数	マルチキャスト経路情報のエントリ数
256	1000
128	2000
64	4000
32	8000

表 3-313 使用インタフェース数に対する IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数

使用インタフェース数	IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連動させる設定数
31	256
63	128
127	64
255	32

表 3-314 加入グループ数に対する IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数

加入グループ (延べ数)	IGMPv2/IGMPv3 (EXCLUDE モード) で PIM-SSM を連動させる設定数
64	256
128	128
256	64
512	32
1024	16
2048	8
4096	4
8128	2

表 3-315 IPv4 でのインタフェース当たりの加入グループ数

マルチキャスト動作インタフェース数	インタフェース当たりの加入可能グループ数
31	256
63	128
127	64
255	32

(a) IPv4 マルチキャスト使用時の注意事項

マルチキャストデータの送信元に対して到達できるすべてのインタフェースに PIM の設定が必要です。

(b) マルチキャストデータの送信元サーバに関する注意

マルチキャストデータの送信元となるサーバの中には、マルチキャストパケットをバーストトラフィックとして送信する特性を持つものがあります。この特性を持つサーバから受信したマルチキャストデータを、マルチキャスト配信する場合には注意が必要です。マルチキャスト配信先の回線を収容するネットワークインタフェース機構 (NIF) の種類によって、マルチキャスト動作可能なインタフェース数が異なります。マルチキャスト動作可能なインタフェース数を次の表に示します。

表 3-316 マルチキャスト動作可能なインタフェース数

NIF 略称	マルチキャスト動作可能なインタフェース数 (推奨値)
NH1G-16S	ポート当たり 16 インタフェース
NH1G-24T	ポート当たり 16 インタフェース
NH1G-24S	ポート当たり 16 インタフェース
NH1G-48T	ポート当たり 16 インタフェース
NH1GS-6M	NIF 当たり 255 インタフェース
NH10G-1RX	ポート当たり 32 インタフェース
NH10G-4RX	ポート当たり 32 インタフェース
NH10G-8RX	ポート当たり 32 インタフェース

注

推奨値は、送信元サーバが、マルチキャストパケットを 8 バーストで送信する特性 (サーバで 8 パケット分のマルチキャストデータをいったん蓄積したあとに、ネットワークに対して連続的に送信する特性) を持っていることを想定しています。バースト数が大きくなると、パケットを一部廃棄することがあるので、マルチキャストを定義するインタフェース数を少なくする必要があります。

(2) IPv6 マルチキャスト

IPv6 マルチキャストを設定できるインタフェース数およびルーティングテーブルのエントリ数を次の表に示します。

複数の VRF で IPv6 マルチキャストを使用する場合、グローバルネットワークとすべての VRF の合計を本収容条件内に収めてください。ただし、MSU-1A および MSU-1A1 では VRF 機能をサポートしていません。

表 3-317 IPv6 マルチキャストの最大数

項目	最大数	
	MSU-1A MSU-1A1	MSU-1B MSU-1B1
PIM-SM/SSM マルチキャストインタフェース数 ¹ ²	127 / 装置	255 / 装置
MLD 動作インタフェース数 ¹	127 / 装置	255 / 装置
マルチキャスト送信元の数	256 / グループ	256 / グループ
PIM-SM/SSM マルチキャストルーティングエントリ ((S,G) エントリ, (*,G) エントリ, およびネガティブキャッシュ) 数 S: 送信元 IP アドレス G: グループアドレス	1000 / 装置	8000 / 装置
MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連携動作させる設定数 (ソース, グループペア数) ³	256 / 装置	256 / 装置
MLDv2 で 1Report につき処理できる record 情報 ⁴	32record / メッセージ 32 ソース / record	32record / メッセージ 32 ソース / record
MLD 加入グループ数 ⁵ ⁶	256 / 装置	256 / 装置
マルチキャストルータ隣接数	256 / 装置	256 / 装置
ランデブーポイント数	2 / グループ	2 / グループ
1 装置当たりランデブーポイントで設定できるグループ数 ⁷	128 / 装置	128 / 装置
1 ネットワーク (VPN) 当たりランデブーポイントに設定できる延べグループ数	128 / ネットワーク 128 / 装置	128 / ネットワーク (VPN) 256 / 装置 ⁸
1 ネットワーク (VPN) 当たりの BSR 候補数	16 / ネットワーク 16 / 装置	16 / ネットワーク (VPN) 256 / 装置 ⁸
静的加入グループ数 ⁹ ¹⁰	2000 / 装置	4000 / 装置
静的ランデブーポイント (RP) ルータアドレス数	16 / 装置	16 / 装置
MLD グループ当たりのソース数	256 / グループ	256 / グループ
遠隔のマルチキャストサーバアドレスを直接接続サーバとして扱う設定数	256 / 装置 16 / インタフェース	256 / 装置 16 / インタフェース
マルチキャスト中継エントリの延べ下流インタフェース数 ¹¹ ¹²	140000 / 装置	280000 / 装置
マルチキャストを設定できる VRF 数	-	249 / 装置
エクストラネットのマルチキャストフィルタ数 ¹³	-	512 / 装置
エクストラネットで使用する route-map 数	-	256 / 装置 256 / VRF
PIM-SM VRF ゲートウェイ動作マルチキャストアドレス数 ¹⁴	-	256 / 装置 256 / VRF

(凡例) - : 該当なし

注 1

マルチホームをサポートします。

注 2

3. 収容条件

IPv6 マルチキャストインタフェースとして、このほかにカプセル化用インタフェースが一つ存在します。このため、IPv6 PIM-SM マルチキャストインタフェース全体の数は、MSU-1A または MSU-1A1 搭載時は 128 個、MSU-1B または MSU-1B1 搭載時は 256 個になりますが、ユーザが設定できるのはそのうち MSU-1A または MSU-1A1 搭載時は 127 個、MSU-1B または MSU-1B1 搭載時は 255 個です。また、PIM-SM と PIM-SSM の合計で MSU-1A または MSU-1A1 搭載時は 127 / 装置、MSU-1B または MSU-1B1 搭載時は 255 / 装置となります。

注 3

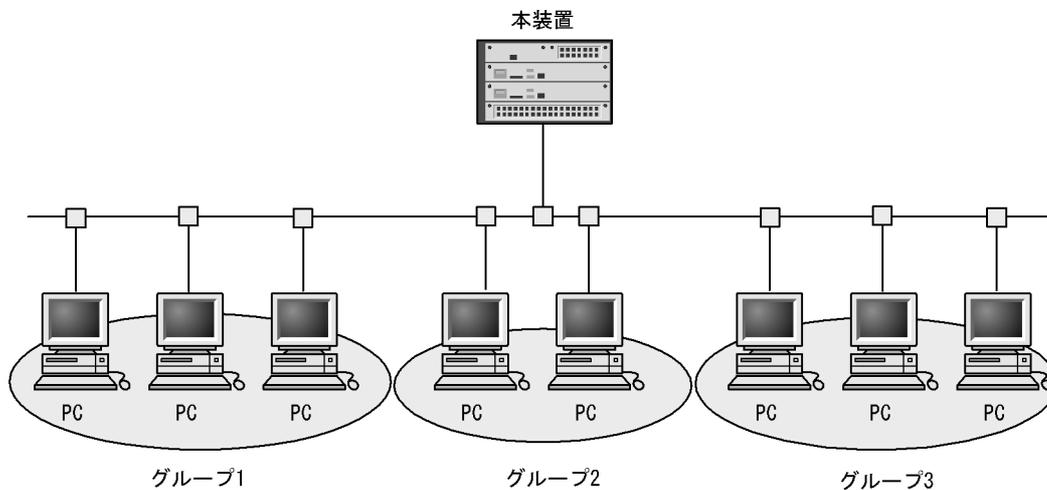
マルチキャストで使用するインタフェース数および加入グループ数によって設定できる数が変わります。「表 3-318 使用インタフェース数に対する MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数」および「表 3-319 加入グループ数に対する MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数」に示す範囲内で使用してください。加入グループ数は、動的および静的加入グループ数の総計です。同一グループアドレスが異なるインタフェースに加入している場合、加入グループ数は一つでなく、加入したインタフェースの数になります。

注 4

一つの Report メッセージで処理できるソース数は延べ 1024 ソースまでです。ソース情報のない record も 1 ソースとして数えます。MLDv2 (EXCLUDE モード) で PIM-SSM を連携動作させる設定をした場合、その設定に一致した EXCLUDE record で定義されているソース数を数えます。また、受信した Report メッセージ内に EXCLUDE record が複数存在し、MLDv2 (EXCLUDE モード) で PIM-SSM を連携動作させる設定で追加したソース数が延べ 1024 を超えた場合、以降のそのメッセージ内の EXCLUDE record で、連携動作の対象となる EXCLUDE record についてマルチキャスト中継情報は作成しません。

注 5

本装置に直接接続しているグループの数を示します。MLDv2 使用時に送信元を指定する場合のグループ数は、送信元とグループの組み合わせの数となります。次の図の例ではグループ数が 3 になります。



注 6

IPv6 でのインタフェース当たりの加入可能グループ数を「表 3-320 IPv6 でのインタフェース当たりの加入可能グループ数」に示します。

注 7

グループを指定しないでランデブーポイントを設定した場合、デフォルトグループが設定されます。グローバルネットワークおよび VRF でランデブーポイントを設定する場合、デフォルトグループも 1 グループとして、装置内またはネットワーク (VPN) 内の総グループ数が収容条件内になるように設定してください。

注 8

本装置のグローバルネットワークとすべての VRF に接続するネットワーク (VPN) 上の総数です。

注 9

静的加入グループ数とは、各マルチキャストインタフェースで静的加入するグループアドレスの総数です。同一グループアドレスを複数の異なるインタフェースに静的加入設定した場合、静的加入グループ数は一つではなく、静的加入設定したインタフェースの数になります。

また、PIM-SM VRF ゲートウェイで指定したグループアドレスの延べ数との合計になります。

注 10

一つのインタフェースに設定できる静的加入グループ数は 256 までです。

注 11

構成およびリソース状況によっては最大数が MSU-1A または MSU-1A1 搭載時は 140000 以下、MSU-1B または MSU-1B1 搭載時は 280000 以下となることがあります。

注 12

マルチキャスト中継エントリの延べ下流インタフェース数は、IPv4 マルチキャストと IPv6 マルチキャストの合計です。

注 13

すべての route-map で指定した access-list 内のアドレスの延べ数です。

注 14

エクストラネットに指定した route-map を使用します。route-map に指定した access-list 内で、ホストアドレス (128 ビットマスク) として指定したマルチキャストアドレスが対象となります。

装置当たりの上限は、すべての VRF で指定した PIM-SM VRF ゲートウェイのグループアドレスの延べ数です。

また、静的加入グループ数で指定したグループアドレス数との合計になります。

表 3-318 使用インタフェース数に対する MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数

使用インタフェース数	MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連動させる設定数
31	256
63	256
127	256
255	256

表 3-319 加入グループ数に対する MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連動させる設定可能数

加入グループ数 (延べ数)	MLDv1/MLDv2 (EXCLUDE モード) で PIM-SSM を連動させる設定数
64	256
128	128
256	64
512	32
1024	16
2048	8
4096	4
8128	2

表 3-320 IPv6 でのインタフェース当たりの加入可能グループ数

マルチキャスト動作インタフェース数	インタフェース当たりの加入可能グループ数
31	256
63	128

3. 収容条件

マルチキャスト動作インタフェース数	インタフェース当たりの加入可能グループ数
127	64
255	32

(a) PIM-SM / SSM 使用時の注意事項

マルチキャストデータの送信元に対して到達できるすべてのインタフェースに PIM の設定が必要です。

(b) マルチキャストデータの送信元サーバに関する注意

IPv6 でのマルチキャストデータの送信元サーバに関する注意の内容は、IPv4 と同様です。詳細は、「(1) IPv4 マルチキャストの (b) マルチキャストデータの送信元サーバに関する注意」を参照してください。

3.6.14 VRF 【OP-NPAR】

設定できる VRF 数を次の表に示します。VRF 設定可能数にグローバルネットワークは含みません。

表 3-321 設定できる VRF 数

VRF 動作モード	VRF 設定可能数	説明
設定なし	-	• VRF は動作しません
axrp-enable	63	• IPv4 だけが VRF インスタンスで動作します • Ring Protocol が動作します
l2protocol-disable	249	• IPv4 だけが VRF インスタンスで動作します • レイヤ 2 プロトコルが動作しません
axrp-enable-ipv4-ipv6	63	• IPv4 と IPv6 のどちらも VRF インスタンスで動作します • Ring Protocol が動作します
gsrp-enable-ipv4-ipv6	124	• IPv4 と IPv6 のどちらも VRF インスタンスで動作します • GSRP が動作します
l2protocol-disable-ipv4-ipv6	249	• IPv4 と IPv6 のどちらも VRF インスタンスで動作します • レイヤ 2 プロトコルが動作しません

(凡例) - : 設定できない

4

装置へのログイン

この章では、装置の起動と停止、およびログイン・ログアウト、運用管理の概要、運用端末とその接続形態について説明します。

4.1 運用端末による管理

4.2 装置起動

4.3 ログイン・ログアウト

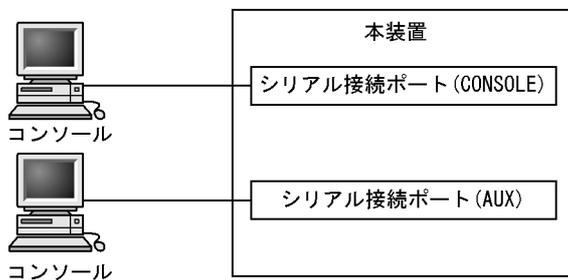
4.1 運用端末による管理

本装置の運用にはコンソールまたはリモート運用端末が必要です。コンソールは RS232C に接続する端末、リモート運用端末は IP ネットワーク経由で接続する端末です。また、本装置は IP ネットワーク経由で SNMP マネージャによるネットワーク管理にも対応しています。コンソールやリモート運用端末といった本装置の運用管理を行う端末を運用端末と呼びます。

4.1.1 運用端末の接続形態

コンソールは本装置のシリアル接続ポート（CONSOLE）に接続します。また、本装置のシリアル接続ポート（AUX）に接続することもできます。コンソールの接続形態を次の図に示します。

図 4-1 コンソールの接続形態

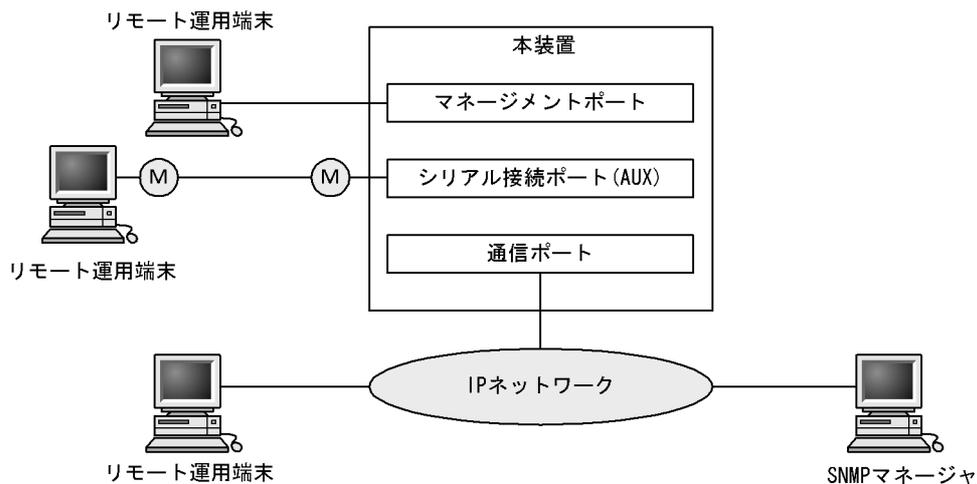


リモート運用端末は、次に示す三つの接続形態がとれます。

- マネージメントポート接続する形態
- 通信ポートが接続する IP ネットワークから接続する形態
- シリアル接続ポート（AUX）にダイヤルアップ IP 接続する形態

リモート運用端末の接続形態を次の図に示します。

図 4-2 リモート運用端末の接続形態



(凡例) (M) : モデム

(1) シリアル接続ポート (CONSOLE)

シリアル接続ポート (CONSOLE) にコンソールを接続します。コンフィグレーションを設定していなくても本ポートを介してログインできるので、初期導入時には本ポートからログインして、初期設定ができます。

(2) シリアル接続ポート (AUX)

シリアル接続ポート (AUX) にコンソールを接続します。コンフィグレーションを設定していなくても本ポートを介してログインできるので、初期導入時には本ポートからログインして、初期設定ができます。なお、シリアル接続ポート (AUX) から接続した場合、Rom, Boot 状態は表示されません。

(3) マネージメントポート

マネージメントポートを介して、遠隔のリモート運用端末からの本装置に対するログインや SNMP マネージャによるネットワーク管理ができます。このポートを介して telnet や ftp によって本装置へログインするためには、本装置のコンフィグレーションで IP アドレスおよびリモートアクセスの設定をする必要があります。

(4) 通信用ポート

マネージメントポートと同様の運用ができます。

(5) シリアル接続ポート (AUX) にダイヤルアップ IP 接続

リモート運用端末をマネージメントポート接続した場合と同様の運用ができます。本装置やモデムの設定については、「7.1.3 ダイヤルアップ IP 接続」を参照してください。

4.1.2 運用端末

コンソールとリモート運用端末の運用管理での適用範囲の違いを次の表に示します。

表 4-1 コンソールとリモート運用端末の運用管理での適用範囲の違い

運用機能	コンソール	リモート運用端末
遠隔からのログイン	不可	可
本装置から運用端末へのログイン	不可	可
アクセス制御	なし	あり
コマンド入力	可	可
ファイル転送方式	なし	ftp
IP 通信	不可	IPv4 および IPv6
SNMP マネージャ接続	不可	可
コンフィグレーション設定	不要	必要

(1) コンソール

コンソールは RS-232C に接続する端末で、一般的な通信端末、通信ソフトウェアが使用できます。コンソールが本装置と通信できるように、次の標準 VT-100 設定値 (本装置のデフォルト設定値) が通信ソフトウェアに設定されていることを確認してください。

- 通信速度：9600bit/s
- データ長：8 ビット

4. 装置へのログイン

- パリティビット：なし
- ストップビット：1ビット
- フロー制御：なし

シリアル接続ポート（CONSOLE）接続の場合に、通信速度を 9600bit/s 以外（1200 / 2400 / 4800 / 19200bit/s）で設定して使用したい場合は、コンフィグレーションコマンド `speed` で本装置側の通信速度設定を変更してください。ただし、実際に設定が反映されるのはコンソールからいったんログアウトしたあとになります。

なお、シリアル接続ポート（AUX）接続の場合は、通信速度は 9600bit/s 固定です。

図 4-3 コンソール接続時の通信速度の設定例

```
(config)# line console 0
(config-line)# speed 19200
```

！ 注意事項

コンソールを使用する場合は次の点に注意してください。

- 本装置ではコンソール端末からログインする際に、自動的に VT-100 の制御文字を使用して画面サイズを取得・設定します。VT-100 に対応していないコンソール端末では、不正な文字列が表示されたり、最初の CLI プロンプトがずれて表示されたりして、画面サイズが取得・設定できません。
また、ログインと同時にキー入力した場合、VT-100 の制御文字の表示結果が正常に取得できないため同様の現象となりますのでご注意ください。この場合は、再度ログインし直してください。
- 通信速度の設定が反映されるのは、ログアウトしたあとになります。コンソールからいったんログアウトしたあとで、使用している通信端末や通信ソフトウェアの通信速度の設定を変更してください。変更するまでは文字列が不正な表示になります（「login」プロンプトなど）。
- 通信速度を 9600bit/s 以外に設定して運用している場合、装置を起動（再起動）するとコンフィグレーションが装置に反映されるまでの間、不正な文字列が表示されます。

(2) リモート運用端末

本装置に IP ネットワーク経由で接続してコマンド操作を行う端末が、リモート運用端末です。telnet プロトコルのクライアント機能がある端末はリモート運用端末として使用できます。

！ 注意事項

本装置の telnet サーバは、改行コードとして [CR] を認識します。一部のクライアント端末では、改行コードとして [CR] および [LF] を送信します。これらの端末から接続した場合、空行が表示されたり、(y/n) 確認時にキー入力ができなかったりするなどの現象がおこります。このような場合は、各クライアント端末の設定を確認してください。

4.1.3 運用管理機能の概要

本装置はセットアップ作業が終了し、装置の電源 ON で運用に入ります。本装置と接続した運用端末では、運用コマンドやコンフィグレーションコマンドを実行し、装置の状態を調べたり、接続ネットワークの変更に伴うコンフィグレーションの変更を実施したりできます。本装置で実施する運用管理の種類を次の表に示します。

表 4-2 運用管理の種類

運用機能	概要
コマンド入力機能	コマンドラインによる入力を受け付けます。
ログイン制御機能	不正アクセス防止、パスワードチェックを行います。
コンフィグレーション編集機能	運用のためのコンフィグレーションを設定します。設定された情報はすぐ運用に反映されます。
ネットワークコマンド機能	リモート操作コマンドなどをサポートします。
ログ・統計情報	過去に発生した障害情報および回線使用率などの統計情報を表示します。
LED および障害部位の表示	LED によって本装置の状態を表示します。
MIB 情報収集	SNMP マネージャによるネットワーク管理を行います。
装置保守機能	装置を保守するための状態表示、装置とネットワークの障害を切り分けるための回線診断などのコマンドを持ちます。
MC 保守機能	MC のフォーマットなどを行います。

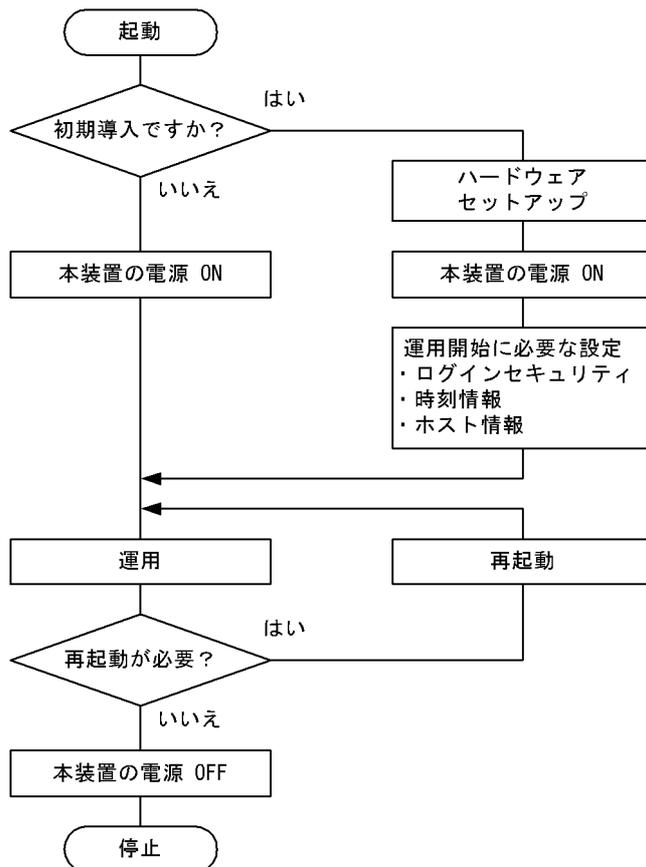
4.2 装置起動

この節では、装置の起動と停止について説明します。

4.2.1 起動から停止までの概略

本装置の起動から停止までの概略フローを次の図に示します。ハードウェアセットアップの内容についてはマニュアル「ハードウェア取扱説明書」を参照してください。

図 4-4 起動から停止までの概略フロー



4.2.2 装置の起動

本装置の起動、再起動の方法を次の表に示します。

表 4-3 起動、再起動の方法

起動の種類	内容	操作方法
電源 ON による起動	本装置の電源 OFF からの立ち上げです。	本体の電源スイッチを ON にします。
リセットによる再起動	障害発生などにより、本装置をリセットしたい場合に行います。	本体のリセットスイッチを押します。
コマンドによる再起動	障害発生などにより、本装置をリセットしたい場合に行います。	reload コマンドを実行します。

起動の種類	内容	操作方法
デフォルトリスタート	<p>パスワードを忘れてログインできない場合や、コマンド承認の設定ミスなどでコンソールからコマンドが実行できなくなった場合に行います。</p> <p>パスワードによるログイン認証、装置管理者モードへの変更（enable コマンド）時の認証、およびコマンド承認を行いませんのでデフォルトリスタートによる起動を行う場合は十分に注意してください。なお、アカウント、コンフィグレーションはデフォルトリスタート前のものが使用されます。</p> <p>また、ログインユーザ名を忘れると、デフォルトリスタートで起動してもログインできないので注意してください。</p> <p>デフォルトリスタート中に設定したパスワードは、装置再起動後に有効になります。</p> <p>デフォルトリスタートを実行する場合は、システム操作パネルから装置を停止したあとで実行してください。システム操作パネルから装置を停止する方法は、「11.1.8 装置の停止」を参照してください。</p> <p>なお、BCU/CSU/MSU を二重化構成で運用している場合は、両系の BCU/CSU/MSU に対してデフォルトリスタートを実行してください。実行するときは、運用系、待機系の順で実施してください。</p>	<p>本体のリセットスイッチを 5 秒以上押します。</p>

本装置を起動、再起動したときに STATUS ランプが赤点灯となった場合は、マニュアル「トラブルシューティングガイド」を参照してください。また、LED ランプ表示内容の詳細は、マニュアル「ハードウェア取扱説明書」を参照してください。

本装置は、ソフトウェアイメージを k.img という名称で書き込んだ MC をスロットに挿入して起動した場合、MC から起動します。MC から装置を起動した場合、アカウント、コンフィグレーションは工場出荷時の初期状態となり、設定しても保存することはできません。通常運用時は MC から起動しないでください。

4.2.3 装置の停止

本装置の電源を OFF にする場合は、アクセス中のファイルが壊れるおそれがあるので、本装置にログインしているユーザがいない状態で行ってください。運用コマンド reload stop で装置を停止させたあとに電源を OFF にすることを推奨します。

4.3 ログイン・ログアウト

この節では、ログインとログアウトについて説明します。

(1) ログイン

装置が起動すると、ログイン画面を表示します。この画面でユーザ名とパスワードを入力してください。正しく認証された場合は、コマンドプロンプトを表示します。また、認証に失敗した場合は " Login incorrect " のメッセージを表示し、ログインできません。ログイン画面を次の図に示します。

なお、初期導入時には、ユーザ名 operator でパスワードなしでログインができます。

図 4-5 ログイン画面

```
login: operator
Password: ***** ...1
Copyright (c) 2006 ALAXALA Networks Corporation. All rights reserved.
> ...2
```

1. パスワードが設定されていない場合は表示しません。
また、パスワードの入力文字は表示しません。
2. コマンドプロンプトを表示します。

(2) ログアウト

CLI での操作を終了してログアウトしたい場合は logout コマンドまたは exit コマンドを実行してください。ログアウト画面を次の図に示します。

図 4-6 ログアウト画面

```
> logout
login:
```

(3) 自動ログアウト

一定時間（デフォルト：60 分）内にキーの入力がなかった場合、自動的にログアウトします。なお、自動ログアウト時間はコンフィグレーションコマンド username，または運用コマンド set exec-timeout で変更できます。

5

コマンド操作

この章では、本装置でのコマンドの指定方法について説明します。

5.1 コマンド入力モード

5.2 CLI での操作

5.3 CLI の注意事項

5.1 コマンド入力モード

5.1.1 運用コマンド一覧

コマンド入力モードの切り換えおよびユーティリティに関する運用コマンド一覧を次の表に示します。

表 5-1 運用コマンド一覧

コマンド名	説明
enable	コマンド入力モードを一般ユーザモードから装置管理者モードに変更します。
disable	コマンド入力モードを装置管理者モードから一般ユーザモードに変更します。
quit	現在のコマンド入力モードを終了します。
exit	現在のコマンド入力モードを終了します。
logout	装置からログアウトします。
configure(configure terminal)	コマンド入力モードを装置管理者モードからコンフィグレーションコマンドモードに変更して、コンフィグレーションの編集を開始します。
diff	指定した二つのファイル同士を比較し、相違点を表示します。
grep	指定したファイルを検索して、指定したパターンを含む行を出力します。
more	指定したファイルの内容を一画面分だけ表示します。
less	指定したファイルの内容を一画面分だけ表示します。
tail	指定したファイルの指定された位置以降を出力します。
hexdump	ヘキサダンプを表示します。

注

「運用コマンドレファレンス Vol.1 8. ユーティリティ」を参照してください。

5.1.2 コマンド入力モード

本装置でコンフィグレーションの変更を実施したり、または装置の状態を参照したりする場合、適切なコマンド入力モードに遷移し、コンフィグレーションコマンドや運用コマンドを入力する必要があります。また、CLI プロンプトでコマンド入力モードを識別できます。

コマンド入力モードとプロンプトの対応を次の表に示します。

表 5-2 コマンド入力モードとプロンプトの対応

コマンド入力モード	実行可能なコマンド	プロンプト
一般ユーザモード	運用コマンド (configure, adduser コマンドなど、一部のコマンドは装置管理者モードでだけ実行可能です。)	>
装置管理者モード		#
コンフィグレーションコマンドモード	コンフィグレーションコマンド	(config)#

注

コンフィグレーションの編集集中に運用コマンドを実行したい場合、quit コマンドや exit コマンドに

よってコマンド入力モードを装置管理者モードに切り替えなくても、運用コマンドの先頭に「\$」を付けた形式で入力することで実行できます。

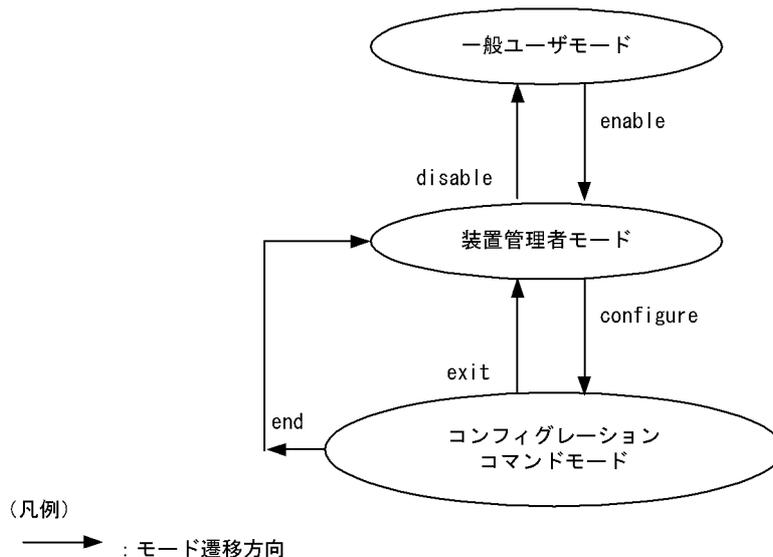
<例>

コンフィグレーションコマンドモードで運用コマンド show ip arp を実行する場合

```
(config)# $show ip arp
```

モード遷移の概要を次の図に示します。

図 5-1 モード遷移の概要



また、CLI プロンプトとして、次に示す場合でも、その状態を意味する文字がプロンプトの先頭に表示されます。

1. コンフィグレーションコマンド hostname でホスト名称を設定している場合、プロンプトに反映されません。
2. ランニングコンフィグレーションを編集し、その内容をスタートアップコンフィグレーションに保存していない場合、プロンプトの先頭に「！」が付きます。

1. ~ 2. のプロンプト表示例を次の図に示します。

図 5-2 プロンプト表示例

```
> enable
# configure
(config)# hostname "OFFICE1"
!OFFICE1(config)# save
OFFICE1(config)# quit
OFFICE1# quit
OFFICE1#
OFFICE1>
```

5.2 CLI での操作

5.2.1 補完機能

コマンドライン上で [Tab] を入力することで、コマンド入力時のコマンド名称やファイル名の入力を少なくすることができ、コマンド入力が簡単になります。補完機能を使用したコマンド入力の簡略化を次の図に示します。

図 5-3 補完機能を使用したコマンド入力の簡略化

```
(config)# in[Tab]
(config)# interface
```

[Tab] を入力することで使用できるパラメータやファイル名の一覧が表示されます。

```
(config)# interface [Tab]
gigabitethernet      port-channel      tengigabitethernet
loopback              range              vlan
(config)# interface
```

5.2.2 ヘルプ機能

コマンドライン上で [?] を入力することで、指定できるコマンドまたはパラメータを検索できます。また、コマンドやパラメータの意味を知ることができます。次の図に [?] 入力時の表示例を示します。

図 5-4 [?] 入力時の表示例

```
> show vlan ?
<vlan id list>      1 to 4095 ex. "5", "10-20" or "30,40"
channel-group-number Display the VLAN information specified by
channel-group-number
detail              Display the detailed VLAN information
list                Display the list of VLAN information
mac-vlan            Display the MAC VLAN information
port                Display the VLAN information specified by port number
summary            Display the summary of VLAN information
<cr>
> show vlan
```

なお、パラメータの入力途中でスペース文字を入れないで [?] を入力した場合は、補完機能が実行されません。また、コマンドパラメータで ? 文字を使用する場合は、[Ctrl] + [V] を入力後、[?] を入力してください。

5.2.3 入力エラー位置指摘機能

コマンドまたはパラメータを不正に入力した際、エラー位置を「^」で指摘し、次行にエラーメッセージ（マニュアル「運用コマンドレファレンス Vol.1 入力エラー位置指摘で表示するメッセージ」を参照）を表示します。[Tab] 入力時と [?] 入力時も同様となります。

「^」の指摘箇所とエラーメッセージの説明によって、コマンドまたはパラメータを見直して再度入力してください。入力エラー位置指摘の表示例を「図 5-5 スペルミスをしたときの表示例」および「図 5-6 パラメータ入力途中の表示例」に示します。

図 5-5 スペルミスをしたときの表示例

```
(config)# interface gigabitehernet 1/1
interface gigabitehernet 1/1
      ^
% illegal parameter at '^' marker
(config)# interface gigabitehernet 1/1
```

図 5-6 パラメータ入力途中の表示例

```
(config)# interface gigabitethernet 1/1
(config-if)# speed
speed
  ^
% Incomplete command at '^' marker
(config-if)#
```

5.2.4 コマンド短縮実行

コマンドまたはパラメータを短縮して入力し、入力された文字が一意のコマンドまたはパラメータとして特定できる場合、コマンドを実行します。短縮入力のコマンド実行例を次の図に示します。

図 5-7 短縮入力のコマンド実行例 (show ip arp の短縮入力)

```
> sh ip ar [Enter]
Date 2006/03/15 19:37:02 UTC
Total: 1 entries
  IP Address      Linklayer Address  Netif          Expire      Type
  192.168.0.1     0012.e2d0.e9f5    VLAN0010      3h44m57s   arpa
>
```

なお、短縮実行できるコンフィグレーションコマンドはコンフィグレーションのモードによって異なります。

コンフィグレーションコマンド show

コンフィグレーションの各モードで短縮実行できます。

コンフィグレーションコマンド end, quit, exit, save, write, status, top

グローバルコンフィグレーションモードでだけ短縮実行できます。ほかのモードで短縮実行すると入力エラーになります。

上記以外の各モードのコンフィグレーションコマンド

各モードで一意に特定できたコマンドを短縮実行できます。

また、*を含むパラメータを指定した場合は、それ以降のパラメータについて短縮実行できません。

5.2.5 ヒストリ機能

ヒストリ機能を使用すると、過去に入力したコマンドを簡単な操作で再実行したり、過去に入力したコマンドの一部を変更して再実行したりできます。ヒストリ機能を使用した例を次の図に示します。

図 5-8 ヒストリ機能を使用したコマンド入力の簡略化

```

> ping 192.168.0.1 numeric count 1 ...1
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=31 time=1.329 ms

--- 192.168.0.1 PING Statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max = 1.329/1.329/1.329 ms
> ...2
> ping 192.168.0.1 numeric count 1 ...3
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=31 time=1.225 ms

--- 192.168.0.1 PING Statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max = 1.225/1.225/1.225 ms
> ...4
> ping 192.168.0.2 numeric count 1 ...5
PING 192.168.0.2 (192.168.0.2): 56 data bytes

--- 192.168.0.2 PING Statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
>

```

- 192.168.0.1 に対して ping コマンドを実行します。
- [] キーを入力することで前に入力したコマンドを呼び出せます。
この例の場合,[] キーを 1 回押すと「ping 192.168.0.1 numeric count 1」が表示されるので,
[Enter] キーの入力だけで同じコマンドを再度実行できます。
- 192.168.0.1 に対して ping コマンドを実行します。
- [] キーを入力することで前に入力したコマンドを呼び出し,[] キーおよび [Backspace] キーを
使ってコマンド文字列を編集できます。
この例の場合,[] キーを 1 回押すと「ping 192.168.0.1 numeric count 1」が表示されるので, IP ア
ドレスの「1」の部分で「2」に変更して [Enter] キーを入力しています。
- 192.168.0.2 に対して ping コマンドを実行します。

ヒストリ機能に次の表に示す文字列を使用した場合、コマンド実行前に過去に実行したコマンド文字列に変換したあとにコマンドを実行します。なお、コンフィグレーションコマンドでは、コマンド文字列変換はサポートしていません。

表 5-3 ヒストリのコマンド文字列変換で使える文字一覧

項番	指定	説明
1	!!	直前に実行したコマンドへ変換して実行します。
2	!n	ヒストリ番号 n のコマンドへ変換して実行します。
3	!-n	n 回前のコマンドへ変換して実行します。
4	!str	文字列 str で始まる過去に実行した最新のコマンドへ変換して実行します。
5	^str1^str2	直前に実行したコマンドの文字列 str1 を str2 に置換して実行します。

注

運用コマンド show history で表示される配列番号のこと。

また、過去に実行したコマンドを呼び出して、コマンド文字列を編集したり,[Backspace] キーや [Ctrl] + [C] キーで消去したりしたあと、再度コマンドを呼び出すと、該当コマンドのヒストリを編集したり消去したりできます。

注意

通信ソフトウェアによって方向キー ([], [], [], []) を入力してもコマンドが呼び出されない場合があります。その場合は、通信ソフトウェアのマニュアルなどで設定を確認してください。

5.2.6 パイプ機能

パイプ機能を利用することによって、コマンドの実行結果を別のコマンドに引き継ぐことができます。実行結果を引き継ぐコマンドに grep コマンドを使うことによって、コマンドの実行結果をよりわかりやすくすることができます。「図 5-9 show sessions コマンド実行結果」に show sessions コマンドの実行結果を、「図 5-10 show sessions コマンド実行結果を grep コマンドでフィルタリング」に show sessions コマンドの実行結果を grep コマンドでフィルタリングした結果を示します。

図 5-9 show sessions コマンド実行結果

```
> show sessions
Date 2009/01/07 12:00:00 UTC
operator console ----- 0 Jan 6 14:16
operator aux ----- 1 Jan 6 14:16 (ppp0:200.10.10.1)
operator tty0 ----- 2 Jan 6 14:16 (192.168.3.7)
operator tty1 admin 3 Jan 6 14:16 (192.168.3.7)
```

図 5-10 show sessions コマンド実行結果を grep コマンドでフィルタリング

```
> show sessions | grep admin
operator tty1 admin 3 Jan 6 14:16 (192.168.3.7)
>
```

5.2.7 リダイレクト

リダイレクト機能を利用することによって、コマンドの実行結果をファイルに出力できます。show ip interface コマンドの実行結果をファイルに出力する例を次の図に示します。

図 5-11 show ip interface コマンド実行結果をファイルに出力

```
> show ip interface > show_interface.log
>
```

5.2.8 ページング

コマンドの実行により出力される結果について、表示すべき情報が一画面にすべて表示しきれない場合は、ユーザのキー入力を契機に一画面ごとに区切って表示します。ただし、リダイレクトがあるときにはページングを行いません。なお、ページングはコンフィグレーションコマンド username、または運用コマンド set terminal pager でその機能を有効にしたり無効にしたりできます。

5.2.9 CLI 設定のカスタマイズ

自動ログアウト機能や CLI 機能の一部は、CLI 環境情報としてユーザごとに動作をカスタマイズできます。カスタマイズ可能な CLI 機能と CLI 環境情報を次の表に示します。

表 5-4 カスタマイズ可能な CLI 機能と CLI 環境情報

機能	カスタマイズ内容と初期導入時のデフォルト設定
自動ログアウト	自動ログアウトするまでの時間を設定できます。 初期導入時のデフォルト設定は、60 分です。

5. コマンド操作

機能	カスタマイズ内容と初期導入時のデフォルト設定
ページング	ページングするかどうかを設定できます。 初期導入時のデフォルト設定は、ページングをします。
ヘルプ機能	ヘルプメッセージで表示するコマンドの一覧を設定できます。 初期導入時のデフォルト設定は、運用コマンドのヘルプメッセージを表示する際に、 入力可能なすべての運用コマンドの一覧を表示します。

これらの CLI 環境情報は、ユーザごとに、コンフィグレーションコマンド `username`、または次に示す運用コマンドで設定できます。

- `set exec-timeout`
- `set terminal pager`
- `set terminal help`

コンフィグレーションコマンド `username` による設定は、運用コマンドによる設定よりも優先されます。三つの CLI 環境情報のうち、どれか一つでもコンフィグレーションコマンドで設定した場合、その対象ユーザには、運用コマンドによる設定値は使用されません。コンフィグレーションコマンドの設定値または省略時の初期値で動作します。

運用コマンドによる設定は、コンフィグレーションコマンドによる設定がない場合に使用されます。コンフィグレーションコマンドで一つも CLI 環境情報を設定していないユーザは、運用コマンドによる設定値が使用されます。なお、運用コマンドによる設定では、設定状態を表示できないため、各機能の動作状態で確認してください。

運用コマンドによる設定内容は、コマンド実行直後から動作に反映されます。さらに、コンフィグレーションコマンドによる設定で動作している場合でも、一時的に該当セッションでの動作を変更できます。

なお、運用コマンドによる設定の場合、`adduser` コマンドで `no-flash` パラメータを指定して追加したアカウントのユーザは、装置を再起動したときに、CLI 環境情報が初期導入時のデフォルト設定に戻ります。

運用コマンドで設定した CLI 環境情報を待機系システムに同期させるには、`synchronize` コマンドで `userfile` パラメータまたは `account` パラメータを指定して実行してください。

5.3 CLI の注意事項

5.3.1 ログイン後に運用端末がダウンした場合

ログイン後に運用端末がダウンした場合、本装置内ではログインしたままの状態になっていることがあります。この場合、自動ログアウトを待つか、再度ログインし直して、ログインしたままの状態になっているユーザを運用コマンド `killuser` で削除してください。

5.3.2 CLI の特殊キー操作時にログアウトした場合

[Ctrl] + [C] キー, [Ctrl] + [Z] キー, [Ctrl] + [¥] キーのどれかを押した場合に、ごくまれにログアウトする場合があります。その場合は、再度ログインしてください。

5.3.3 待機系のファイルにアクセスする場合

`/standby` ディレクトリ配下のファイルにアクセスする場合は、次の点に注意してください。

- 補完機能は使用できません。
- 運用コマンド `cd` で、`/standby` 配下のディレクトリに移動しないでください。
- 運用系のファイルにアクセスする場合に比べて、アクセスに時間が掛かります。

6

コンフィグレーション

本装置には、ネットワークの運用環境に合わせて、構成および動作条件などのコンフィグレーションを設定しておく必要があります。この章では、コンフィグレーションを設定するのに必要なことについて説明します。

6.1 コンフィグレーション

6.2 ランニングコンフィグレーションの編集概要

6.3 コンフィグレーションコマンド入力におけるモード遷移

6.4 コンフィグレーションの編集方法

6.5 コンフィグレーションの操作

6.1 コンフィグレーション

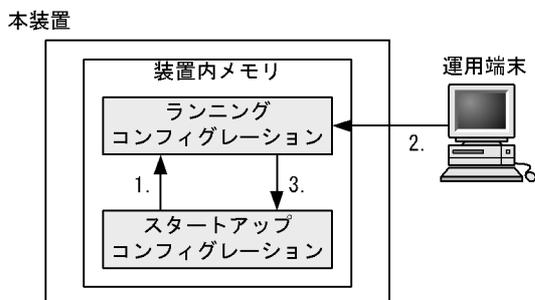
運用開始時または運用中、ネットワークの運用環境に合わせて、本装置に接続するネットワークの構成および動作条件などのコンフィグレーションを設定する必要があります。初期導入時、コンフィグレーションは設定されていません。

6.1.1 起動時のコンフィグレーション

本装置の電源を入れると、装置内メモリ上のスタートアップコンフィグレーションファイルが読み出され、設定されたコンフィグレーションに従って運用を開始します。運用に使用されているコンフィグレーションをランニングコンフィグレーションと呼びます。

なお、スタートアップコンフィグレーションは、直接編集できません。ランニングコンフィグレーションを編集したあとに save(write) コマンドを使用することで、スタートアップコンフィグレーションが更新されます。起動時、および運用中のコンフィグレーションの概要を次の図に示します。

図 6-1 起動時、および運用中のコンフィグレーションの概要



1. 本装置を起動すると、装置内メモリのスタートアップコンフィグレーションが読み出され、ランニングコンフィグレーションとしてロードされる。ランニングコンフィグレーションの内容で運用を開始する。
2. コンフィグレーションを変更した場合は、ランニングコンフィグレーションに反映される。
3. 変更されたランニングコンフィグレーションをスタートアップコンフィグレーションに保存する。

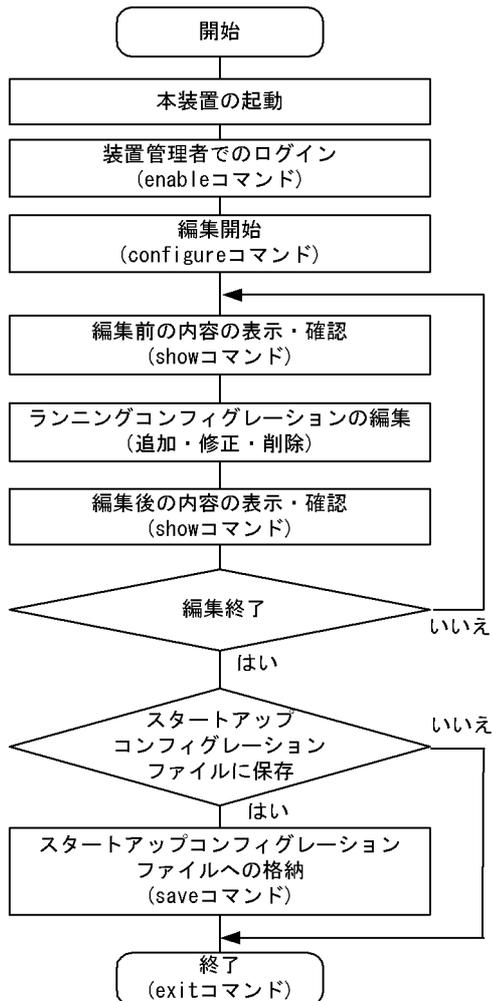
6.1.2 運用中のコンフィグレーション

運用中にコンフィグレーションを編集すると、編集した内容はランニングコンフィグレーションとしてすぐに運用に反映されます。save(write) コマンドを使用することで、ランニングコンフィグレーションが装置内メモリにあるスタートアップコンフィグレーションに保存されます。編集した内容を保存しないで装置を再起動すると、編集した内容が失われるので注意してください。

6.2 ランニングコンフィグレーションの編集概要

初期導入時やネットワーク構成を変更する場合は、ランニングコンフィグレーションを編集します。なお、初期導入時のランニングコンフィグレーションの編集はコンソールから行う必要があります。ランニングコンフィグレーションの編集の流れを次の図に示します。詳細については、「6.4 コンフィグレーションの編集方法」を参照してください。

図 6-2 ランニングコンフィグレーションの編集の流れ



6.3 コンフィグレーションコマンド入力におけるモード遷移

コンフィグレーションは、実行可能なコンフィグレーションモードで編集します。第二階層のコンフィグレーションを編集する場合は、グローバルコンフィグレーションモードで第二階層のコンフィグレーションモードに移行するためのコマンドを実行してモードを移行した上で、コンフィグレーション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のモード遷移の概要を次の図に示します。

図 6-3 コンフィグレーションのモード遷移の概要

グローバル コンフィグレーション モード (第一階層)	モード遷移コマンド	コンフィグレーションの モード (第二階層)	モード遷移コマンド	コンフィグレーションの モード (第三階層)	
config	vlan		config-vlan		
	spanning-tree mst configuration		config-mst		
	interface loopback		config-if		
	interface async		config-if		
	interface mgmt		config-if		
	interface port-channel		config-if		
	interface gigabitethernet		config-if		
	interface range gigabitethernet		config-if-range		
	interface tengigabitethernet		config-if		
	interface range tengigabitethernet		config-if-range		
	interface vlan		config-if		
	interface range vlan		config-if-range		
	axrp		config-axrp		
	gsrp		config-gsrp		
	router rip		config-router	address-family ipv4 vrf	config-router-af
	router ospf		config-router		
	router bgp		config-router	address-family ipv6	config-router-af
				address-family ipv4 vrf	config-router-af
				address-family ipv6 vrf	config-router-af
	ipv6 router rip		config-rtr-rip		
	ipv6 router ospf		config-rtr		

advance access-list	config-adv-acl
ip access-list extended	config-ext-nacl
ip access-list standard	config-std-nacl
ipv6 access-list	config-ipv6-acl
mac access-list extended	config-ext-macl
route-map	config-route-map
advance qos-flow-list	config-adv-qos
ip qos-flow-list	config-ip-qos
ipv6 qos-flow-list	config-ipv6-qos
mac qos-flow-list	config-mac-qos
ip dhcp pool	dhcp-config
ipv6 dhcp pool	config-dhcp
line console	config-line
line vty	config-line
parser view	config-view
auto-config	config-auto-cf
netconf	config-netconf
shaper nif	config-sh-nif
vrf definition	config-vrf
ethernet cfm domain	config-ether-cfm
track-object	config-track-object
policy-list	config-pol
policy-switch-list	config-pol-sw

6.4 コンフィグレーションの編集方法

6.4.1 コンフィグレーション・運用コマンド一覧

コンフィグレーションの編集および操作に関するコンフィグレーションコマンド一覧を次の表に示します。

表 6-1 コンフィグレーションコマンド一覧

コマンド名	説明
end	コンフィグレーションコマンドモードを終了して装置管理者モードに戻ります。
quit(exit)	モードを一つ戻ります。グローバルコンフィグレーションモードで編集の場合は、コンフィグレーションコマンドモードを終了して装置管理者モードに戻ります。
save(write)	編集したコンフィグレーションをスタートアップコンフィグレーションに保存します。
show	編集中のコンフィグレーションを表示します。
status	編集中のコンフィグレーションの状態を表示します。
top	コンフィグレーションコマンドモードの第二階層以下からグローバルコンフィグレーションモード（第一階層）に戻ります。

コンフィグレーションの編集および操作に関する運用コマンド一覧を次の表に示します。

表 6-2 運用コマンド一覧

コマンド名	説明
show running-config	ランニングコンフィグレーションを表示します。
show startup-config	スタートアップコンフィグレーションを表示します。
copy	コンフィグレーションをコピーします。
erase configuration	ランニングコンフィグレーションの内容を初期導入時のものに戻します。
show file	ローカルまたはリモートサーバ上のファイルの内容と行数を表示します。
cd	現在のディレクトリ位置を移動します。
pwd	カレントディレクトリのパス名を表示します。
ls	ファイルおよびディレクトリを表示します。
dir	復元可能な形式で削除された本装置用のファイルの一覧を表示します。
cat	指定されたファイルの内容を表示します。
cp	ファイルをコピーします。
mkdir	新しいディレクトリを作成します。
mv	ファイルの移動およびファイル名の変更をします。
rm	指定したファイルを削除します。
rmdir	指定したディレクトリを削除します。
delete	本装置用のファイルを復元可能な形式で削除します。
undelete	復元可能な形式で削除された本装置用のファイルを復元します。
squeeze	復元可能な形式で削除された本装置用の deleted ファイルを完全に消去します。

6.4.2 configure (configure terminal) コマンド

コンフィグレーションを編集する場合は、enable コマンドを実行して装置管理者モードに移行してください。装置管理者モードで、configure コマンドまたは configure terminal コマンドを入力すると、プロン

プロンプトが「(config)#」になり、ランニングコンフィグレーションの編集が可能となります。ランニングコンフィグレーションの編集開始例を次の図に示します。

図 6-4 ランニングコンフィグレーションの編集開始例

```
> enable          ...1
# configure       ...2
(config)#
```

1. enable コマンドで装置管理者モードに移行します。
2. ランニングコンフィグレーションの編集を開始します。

6.4.3 コンフィグレーションの表示・確認 (show コマンド)

(1) スタートアップコンフィグレーション、ランニングコンフィグレーションの表示・確認

装置管理者モードで運用コマンド show running-config / show startup-config を使用することで、ランニングコンフィグレーションおよびスタートアップコンフィグレーションを表示・確認できます。ランニングコンフィグレーションの表示例を次の図に示します。

図 6-5 ランニングコンフィグレーションの表示例

```
OFFICE01# show running-config          ...1
#default configuration file for XXXXXX-XX
!
hostname "OFFICE01"
!
vlan 1
  name "VLAN0001"
!
vlan 100
  state active
!
vlan 200
  state active
!
interface gigabitethernet 1/1
  switchport mode access
  switchport access vlan 100
!
interface gigabitethernet 1/2
  switchport mode access
  switchport access vlan 200
!
OFFICE01#
```

1. ランニングコンフィグレーションを表示します。

(2) コンフィグレーションの表示・確認

コンフィグレーションモードで show コマンドを使用することで、編集前、編集後のコンフィグレーションを表示・確認できます。コンフィグレーションを表示した例を「図 6-6 コンフィグレーションの内容をすべて表示」～「図 6-9 インタフェースモードで指定のインタフェース情報を表示」に示します。

6. コンフィグレーション

図 6-6 コンフィグレーションの内容をすべて表示

```
OFFICE01(config)# show ...1
#default configuration file for XXXXXX-XX
!
hostname "OFFICE01"
!
vlan 1
  name "VLAN0001"
!
vlan 100
  state active
!
vlan 200
  state active
!
interface gigabitethernet 1/1
  switchport mode access
  switchport access vlan 100
!
interface gigabitethernet 1/2
  switchport mode access
  switchport access vlan 200
!
OFFICE01(config)#
```

1. パラメータを指定しない場合はランニングコンフィグレーションを表示します。

図 6-7 設定済みのすべてのインタフェース情報を表示

```
OFFICE01(config)# show interface gigabitethernet ...1
interface gigabitethernet 1/1
  switchport mode access
  switchport access vlan 100
!
interface gigabitethernet 1/2
  switchport mode access
  switchport access vlan 200
!
OFFICE01(config)#
```

1. ランニングコンフィグレーションのうち、設定済みのすべてのインタフェースを表示します。

図 6-8 指定のインタフェース情報を表示

```
OFFICE01(config)# show interface gigabitethernet 1/1 ...1
!
interface gigabitethernet 1/1
  switchport mode access
  switchport access vlan 100
!
OFFICE01(config)#
```

1. ランニングコンフィグレーションのうち、インタフェース 1/1 を表示します。

図 6-9 インタフェースモードで指定のインタフェース情報を表示

```
OFFICE01(config)# interface gigabitethernet 1/1
OFFICE01(config-if)# show ...1
interface gigabitethernet 1/1
  switchport mode access
  switchport access vlan 100
OFFICE01(config-if)#
```

1. ランニングコンフィグレーションのうち、インタフェース 1/1 を表示します。

6.4.4 コンフィグレーションの追加・変更・削除

(1) コンフィグレーションコマンドの入力

コンフィグレーションコマンドを使用して、コンフィグレーションを編集します。また、コンフィグレーションのコマンド単位での削除は、コンフィグレーションコマンドの先頭に「no」を指定することで実現できます。

ただし、機能の抑止を設定するコマンドでは、コンフィグレーションコマンドの先頭に「no」を指定して設定し、機能の抑止を解除する場合は「no」を外したコンフィグレーションコマンドを入力します。

コンフィグレーションの編集例を「図 6-10 コンフィグレーションの編集例」に、機能の抑止および解除の編集例を「図 6-11 機能の抑止および解除の編集例」に示します。

図 6-10 コンフィグレーションの編集例

```
(config)# vlan 100 ...1
(config-vlan)# state active ...2
(config-vlan)# exit
(config)# interface gigabitethernet 1/1 ...3
(config-if)# switchport mode access ...4
(config-if)# switchport access vlan 100 ...5
(config-if)# exit
(config)#
(config)# vlan 100 ...6
(config-vlan)# state suspend ...7
(config-vlan)# exit
(config)#
(config)# interface gigabitethernet 1/1 ...8
(config-if)# no switchport access vlan ...9
```

1. VLAN 100 をポート VLAN として設定します。
2. VLAN 100 を有効にします。
3. イーサネットインタフェース 1/1 にモードを遷移します。
4. ポート 1/1 にアクセスモードを設定します。
5. アクセス VLAN に 100 を設定します。
6. VLAN 100 にモードを遷移します。
7. VLAN 100 を有効から無効に変更します。
8. イーサネットインタフェース 1/1 にモードを遷移します。
9. 設定されているアクセス VLAN の VLAN ID 100 を削除します。

図 6-11 機能の抑止および解除の編集例

```
(config)# no ip domain lookup          ...1
(config)# ip domain name router.example.com ...2
(config)# ip name-server 192.168.0.1   ...3
(config)# ip domain lookup             ...4
```

1. DNS リゾルバ機能を無効にします。
2. ドメイン名を router.example.com に設定します。
3. ネームサーバを 192.168.0.1 に設定します。
4. DNS リゾルバ機能を有効にします。

(2) 入力コマンドのチェック

コンフィグレーションコマンドを入力すると、入力されたコンフィグレーションに誤りがないかすぐにチェックされます。エラーがない場合は「図 6-12 正常入力時の出力」に示すようにプロンプトが表示されて、コマンドの入力待ちになります。ランニングコンフィグレーションの編集時の場合は、変更した内容がすぐに運用に使用されます。

エラーがある場合は「図 6-13 異常入力時のエラーメッセージ出力」に示すように、入力したコマンドの行の下にエラーの内容を示したエラーメッセージが表示されます。この場合、入力したコンフィグレーションは反映されないため、入力の誤りを正してから再度入力してください。

図 6-12 正常入力時の出力

```
(config)# interface gigabitethernet 1/1
(config-if)# description TokyoOsaka
(config-if)#
```

図 6-13 異常入力時のエラーメッセージ出力

```
(config)# interface tengigabitethernet 1/1
(config-if)# description
description ^
% Incomplete command at '^' marker
(config-if)#
```

6.4.5 コンフィグレーションの運用への反映

コンフィグレーションの変更は、コンフィグレーションコマンドの入力を契機に即時に運用に反映されます。ただし、BGP に関するフィルタ設定の変更内容を運用に反映する場合は、運用コマンド clear ip bgp を実行する必要があります。

運用コマンド clear ip bgp を使用すると、次に示すコマンドで変更した内容を運用に反映できます。

- access-list コマンド
- prefix-list コマンド
- route-map コマンド
- distribute-list in コマンド
- distribute-list out コマンド
- redistribute コマンド
- neighbor in コマンド
- neighbor out コマンド

コマンドの入力例を次の図に示します。

図 6-14 コマンド入力例

```

(config)# ip access-list standard 1 .....(1)
(config-std-nacl)# permit 10.0.0.0 0.255.255.255 .....(2)
(config-std-nacl)# permit 172.16.0.0 0.0.255.255 .....(3)
(config-std-nacl)# exit
(config)# ip prefix-list PEER-OUT seq 10 permit 172.16.1.0/24 ... (4)
(config)# route-map SET-COMM 10 .....(5)
(config-route-map)# match ip address prefix-list PEER-OUT .....(6)
(config-route-map)# set community no-export .....(7)
(config-route-map)# exit
(config)# router bgp 65530
(config-router)# distribute-list 1 in .....(8)
(config-router)# redistribute static .....(9)
(config-router)# neighbor 192.168.1.1 remote-as 65531
(config-router)# neighbor 192.168.1.2 remote-as 65532
(config-router)# neighbor 192.168.1.2 send-community
(config-router)# neighbor 192.168.1.2 route-map SET-COMM out ....(10)
(config-router)# exit
(config)# save
(config)# exit
# clear ip bgp * both .....1

```

1. (1) ~ (10) の変更内容が運用に使用されます。

6.4.6 コンフィグレーションのファイルへの保存 (save コマンド)

save(write) コマンドを使用することで、編集したランニングコンフィグレーションをスタートアップコンフィグレーションファイルに保存できます。コンフィグレーションの保存例を次の図に示します。

図 6-15 コンフィグレーションの保存例

```

# configure .....1
(config)#
:
: .....2
:
!(config)# save .....3
(config)#

```

1. ランニングコンフィグレーションの編集を開始します。
2. コンフィグレーションを変更します。
3. スタートアップコンフィグレーションファイルに保存します。

6.4.7 コンフィグレーションの編集終了 (exit コマンド)

ランニングコンフィグレーションの編集を終了する場合は、グローバルコンフィグレーションモードで exit コマンドを実行します。コンフィグレーションを編集したあと、save コマンドで変更後の内容をスタートアップコンフィグレーションファイルへ保存していない場合は、exit コマンドを実行すると確認のメッセージが表示されます。スタートアップコンフィグレーションファイルに保存しないでコンフィグレーションコマンドモードを終了する場合は「y」を入力してください。「y」以外が入力されるとコンフィグレーションコマンドモードを終了できません。コンフィグレーションの編集終了例を「図 6-16 コンフィグレーションの編集終了例」と「図 6-17 変更内容を保存しない場合のコンフィグレーションの編集終了例」に示します。

6. コンフィグレーション

図 6-16 コンフィグレーションの編集終了例

```
!(config)# save
(config)# exit          ...1
```

1. 編集を終了します。

図 6-17 変更内容を保存しない場合のコンフィグレーションの編集終了例

```
# configure          ...1
(config)#
:
:
:
!(config)# exit
Unsaved changes found! Do you exit "configure" without save ? (y/n): y ...3
!#
```

1. コンフィグレーションの編集を開始します。
2. コンフィグレーションを変更します。
3. 確認メッセージが表示されます。

6.4.8 初期導入時のコンフィグレーションについて

本装置は初期導入時に次のコンフィグレーションを自動生成します。

- デフォルト VLAN
VLAN ID が 1 の VLAN を生成します。
- スパニングツリー
スパニングツリーを PVST + で動作するようにコンフィグレーションを生成します。
- 物理インターフェース
装置に実装されている NIF ボードに合わせて、NIF ボードの実装位置、種別を基に各物理インターフェースのコンフィグレーションを生成します。また、デフォルト VLAN に属するようアクセスポートとして設定します。

6.4.9 コンフィグレーションの編集時の注意事項

(1) 設定できるコンフィグレーションのコマンド数に関する注意事項

設定されたコンフィグレーションはメモリに保持されるため、設定できるコンフィグレーションのコマンド数はメモリ量によって決まります。設定するコンフィグレーションに比べてメモリ量が少なかったり、制限を超えるようなコンフィグレーションを編集したりした場合は、「Maximum number of entries are already defined (config memory shortage). <IP>」または「Maximum number of entries are already defined.<IP>」のメッセージが表示されます。このような場合、むだなコンフィグレーションが設定されていないか確認してください。

(2) コンフィグレーションをコピー & ペーストで入力する際の注意事項

コンフィグレーションをコピー & ペーストで入力する場合、一行に入力できる文字数は 1000 文字、一度に入力できる文字数は 4000 文字未満（スペース、改行を含む）です。4000 文字以上を一度にペーストすると正しくコンフィグレーションを設定できない状態になるので注意してください。

4000 文字を超えるコンフィグレーションを設定する場合は、一行を 1000 文字、一度のペーストを 4000

文字未満で複数回にわけてコピー & ペーストを行ってください。

6.5 コンフィグレーションの操作

この節では、コンフィグレーションのバックアップ、ファイル転送などの操作について説明します。

6.5.1 コンフィグレーションのバックアップ

運用コマンド `copy` を使用することで、コンフィグレーションをリモートサーバや本装置上にバックアップすることができます。ただし、本装置にバックアップ用のコンフィグレーションファイルを格納する場合、スタートアップコンフィグレーションファイルの格納ディレクトリ (`/config`) は指定できません。バックアップ用のコンフィグレーションファイルはログインユーザのホームディレクトリに作成してください。

バックアップできるコンフィグレーションは、スタートアップコンフィグレーションとランニングコンフィグレーションの2種類です。運用中にコンフィグレーションを変更し保存していない場合は、スタートアップコンフィグレーションをバックアップしても、バックアップしたコンフィグレーションファイルの内容は運用中のコンフィグレーションと異なります。それぞれのバックアップ例を次の図に示します。

図 6-18 スタートアップコンフィグレーションのバックアップ例

```
> enable
# copy startup-config ftp://staff@[2001:240:400::101]/backup.cnf
Configuration file copy to ftp://staff@[2001:240:400::101]/backup.cnf?
(y/n): y

Authentication for 2001:240:400::101.
User: staff
Password: xxx                               ...1
transferring...

Data transfer succeeded.
#
```

1. リモートサーバ上のユーザ `staff` のパスワードを入力します。

図 6-19 ランニングコンフィグレーションのバックアップ例

```
> enable
# copy running-config ftp://staff@[2001:240:400::101]/backup.cnf
Configuration file copy to ftp://staff@[2001:240:400::101]/backup.cnf?
(y/n): y

Authentication for 2001:240:400::101.
User: staff
Password: xxx                               ...1
transferring...

Data transfer succeeded.
#
```

1. リモートサーバ上のユーザ `staff` のパスワードを入力します。

6.5.2 バックアップコンフィグレーションファイルの本装置への反映

バックアップコンフィグレーションファイルをスタートアップコンフィグレーションまたはランニングコンフィグレーションに反映する場合は、運用コマンド `copy` を使用します。それぞれの反映例を次の図に示します。

図 6-20 スタートアップコンフィグレーションへの反映例

```

> enable
# copy ftp://staff@[2001:240:400::101]/backup.cnf startup-config
Configuration file copy to startup-config?
(y/n): y

Authentication for 2001:240:400::101.
User: staff
Password: xxx                               ...1
transferring...

Data transfer succeeded.
#

```

1. リモートサーバ上のユーザ staff のパスワードを入力します。

図 6-21 ランニングコンフィグレーションへの反映例

```

> enable
# copy ftp://staff@[2001:240:400::101]/backup.cnf running-config
Configuration file copy to running-config?
(y/n): y

Authentication for 2001:240:400::101.
User: staff
Password: xxx                               ...1
transferring...

Data transfer succeeded.
#

```

1. リモートサーバ上のユーザ staff のパスワードを入力します。

6.5.3 ftp コマンドを使用したファイル転送

リモート運用端末との間でファイル転送をするときは ftp コマンドを使用します。

(1) バックアップコンフィグレーションファイルを本装置に転送する場合

バックアップコンフィグレーションファイルを格納するディレクトリ (/usr/home/operator) にバックアップコンフィグレーションファイルを転送後、運用コマンド copy を使用してスタートアップコンフィグレーションにコピーします。ftp コマンドを使用してバックアップコンフィグレーションファイルを本装置に転送する例を次の図に示します。

図 6-22 バックアップコンフィグレーションファイルの本装置へのファイル転送例 (ftp コマンド)

```

> cd /usr/home/operator
> ftp 192.168.0.1
Connect to 192.168.0.1.
220 FTP server (Version wn-2.4(4) Wed Jan 1 00:00:00 JST 1999) ready.
Name (192.168.0.1:operator): test
331 Password required for test.
Password:xxxxxxx
230 User test logged in.
Remote system type UNIX.
Using binary mode to transfer files.
ftp> get backup.cnf ...1
local: backup.cnf remote: backup.cnf
200 PORT command successful.
150 Opening BINARY mode data connection for backup.cnf (12,345 bytes)
226 Transfer complete.
ftp> bye
221 Goodby
> enable
# copy /usr/home/operator/backup.cnf startup-config ...2
Configuration file copy to startup-config ? (y/n): y ...3
#

```

1. バックアップコンフィグレーションファイルを転送します。
2. backup.cnf のバックアップコンフィグレーションファイルをスタートアップコンフィグレーションに使用します。
3. 入れ替えてよいかどうかの確認です。

(2) バックアップコンフィグレーションファイルをリモート運用端末へ転送する場合

本装置に格納したバックアップコンフィグレーションファイルをリモート運用端末へ転送する例を次の図に示します。

図 6-23 バックアップコンフィグレーションファイルのリモート運用端末へのファイル転送例

```

> cd /usr/home/operator
> enable
# copy running-config backup.cnf ...1
Configuration file copy to /usr/home/operator/backup.cnf? (y/n) : y
# exit
> ftp 192.168.0.1
Connect to 192.168.0.1.
220 FTP server (Version wn-2.4(4) Fri Jan 1 00:00:00 JST 1999) ready.
Name (192.168.0.1:operator): test
331 Password required for test.
Password:xxxxxxx
230 User test logged in.
Remote system type UNIX.
Using binary mode to transfer files.
ftp> put backup.cnf ...2
local: backup.cnf remote: backup.cnf
200 PORT command successful.
150 Opening BINARY mode data connection for backup.cnf (12,345 bytes)
226 Transfer complete.
ftp> bye
221 Goodby
>

```

1. 運用しているコンフィグレーションファイルをバックアップコンフィグレーションファイルへコピーします。
2. バックアップコンフィグレーションファイルを転送します。

6.5.4 MC を使用したファイル転送

MC にファイル転送をするときは cp コマンドを使用します。

(1) バックアップコンフィグレーションファイルを本装置に転送する場合

バックアップコンフィグレーションファイルを格納するディレクトリ (/usr/home/operator) にバックアップコンフィグレーションファイルを MC から転送後、運用コマンド copy を使用してスタートアップコンフィグレーションにコピーします。cp コマンドを使用してバックアップコンフィグレーションファイルを本装置に転送する例を次の図に示します。

図 6-24 バックアップコンフィグレーションファイルの MC から本装置へのファイル転送例 (cp コマンド)

```
> cd /usr/home/operator
> cp mc-file backup.cnf backup.cnf          ...1
> enable
# copy /usr/home/operator/backup.cnf startup-config ...2
Configuration file copy to startup-config? (y/n): y ...3
#
```

1. バックアップコンフィグレーションファイルを MC から転送します。
2. backup.cnf のバックアップコンフィグレーションファイルを運用に使用します。
3. 入れ替えてよいかどうかの確認です。

(2) バックアップコンフィグレーションファイルを MC に転送する場合

本装置に格納したバックアップコンフィグレーションファイルを MC に転送する例を次の図に示します。

図 6-25 バックアップコンフィグレーションファイルの MC へのファイル転送例

```
> cd /usr/home/operator
> enable
# copy running-config backup.cnf          ...1
Configuration file copy to /usr/home/operator/backup.cnf? (y/n) : y
# exit
> cp backup.cnf mc-file backup.cnf       ...2
>
```

1. 運用しているコンフィグレーションファイルをバックアップコンフィグレーションファイルへコピーします。
2. バックアップコンフィグレーションファイルを MC へ転送します。

6.5.5 バックアップコンフィグレーションファイル反映時の注意事項

運用コマンド copy を使用して、バックアップコンフィグレーションファイルをランニングコンフィグレーションにコピーする場合、運用中のポートが再起動しますので、ネットワーク経由でログインしている場合は注意してください。

バックアップコンフィグレーションファイルの内容が本装置の構成と一致していない場合は、バックアップコンフィグレーションファイルの内容を変更してから運用コマンド copy を使用してください。

7

リモート運用端末から本装置へのログイン

この章では、リモート運用端末から本装置へのリモートアクセスについて説明します。

7.1 解説

7.2 コンフィグレーション

7.3 オペレーション

7.1 解説

7.1.1 マネージメントポート接続

マネージメントポート（10BASE-T/100BASE-TX）のツイストペアケーブル（UTP）を使用したインタフェースについて説明します。

（1）接続インタフェース

（a）マネージメントポート機能仕様

マネージメントポートはリモート運用端末を接続するためのインタフェースを提供します。マネージメントポートの機能仕様を次の表に示します。

表 7-1 マネージメントポートの機能仕様

機能概要	仕様
インタフェース種別	10BASE-T および 100BASE-TX
オートネゴシエーション	サポート
AUTO-MDI/MDI-X	サポート
フローコントロール	未サポート
ジャンボフレーム	未サポート
MAC および LLC 副層制御フレーム	Ethernet V2 形式だけ (802.3 形式, そのほかは未サポート)
対象プロトコル	IPv4 / IPv6
フィルタリング	未サポート
QoS	未サポート
マルチキャスト	未サポート

マネージメントポートでは、IPv4 中継および IPv6 中継をするかどうか、コンフィグレーションで選択できます。なお、マネージメントポートに設定できない IPv4 機能および IPv6 機能の仕様を次の表に示します。

表 7-2 マネージメントポートの IPv4/IPv6 機能仕様

機能概要	仕様
MTU	1500（固定）
サブネットブロードキャスト中継	未サポート
ICMP/ICMPv6 リダイレクト	発行
IPv4 ソースルーティング	中継機能が設定されている場合は中継
ProxyARP	未サポート
ローカル ProxyARP	未サポート
ARP 関連パラメータ	再送回数 1 回（固定） 再送間隔 2 秒（固定） 満了時間 14400 秒（固定）
スタティック ARP / NDP	未サポート
VRRP（IPv4/IPv6） / GSRP	未サポート

機能概要	仕様
uRPF	未サポート

(b) 10BASE-T/100BASE-TX 自動認識 (オートネゴシエーション)

マネージメントポートでは、次の自動認識機能 (オートネゴシエーション) および固定接続機能をサポートしています。

- 自動認識・・・10BASE-T, 100BASE-TX
- 固定接続・・・10BASE-T, 100BASE-TX

コンフィグレーションでは次のモードを指定できます。接続するネットワークに合わせて設定してください。本装置のデフォルト値は、オートネゴシエーションとなります。

- オートネゴシエーション
- 100BASE-TX 全二重固定
- 100BASE-TX 半二重固定
- 10BASE-T 全二重固定
- 10BASE-T 半二重固定

(c) マネージメントポートの接続仕様

本装置のコンフィグレーション指定値と相手装置の伝送速度および、全二重および半二重モードの接続仕様は「15.4 10BASE-T/100BASE-TX/1000BASE-T の解説」の「表 15-8 伝送速度および、全二重および半二重モードごとの接続仕様」を参照してください。ただし、マネージメントポートでは、1000BASE-T は使用できません。

(2) オートネゴシエーション

オートネゴシエーションは、伝送速度、および全二重または半二重モード認識について対向装置間でやり取りを行い、接続動作を決定する機能です。

本装置での接続仕様は、「15.4 10BASE-T/100BASE-TX/1000BASE-T の解説」の「表 15-8 伝送速度および、全二重および半二重モードごとの接続仕様」を参照してください。ただし、マネージメントポートでは、1000BASE-T は使用できません。また、本装置ではネゴシエーション解決できなかった場合、リンク接続されるまで接続動作を繰り返し行います。

(3) AUTO-MDI/MDI-X

AUTO-MDI/MDI-X は、MDI と MDI-X を自動的に切り替える機能です。これによって、クロスケーブルまたはストレートケーブルどちらでも通信できるようになります。オートネゴシエーション時だけサポートします。半二重および全二重固定時は MDI となります。MDI/MDI-X のピンマッピングを次の表に示します。

表 7-3 MDI / MDI-X のピンマッピング

RJ45 Pin No.	MDI		MDI-X	
	100BASE-TX	10BASE-T	100BASE-TX	10BASE-T
1	TD +	TD +	RD +	RD +
2	TD -	TD -	RD -	RD -
3	RD +	RD +	TD +	TD +
4	Unused	Unused	Unused	Unused

7. リモート運用端末から本装置へのログイン

RJ45 Pin No.	MDI		MDI-X	
	100BASE-TX	10BASE-T	100BASE-TX	10BASE-T
5	Unused	Unused	Unused	Unused
6	RD -	RD -	TD -	TD -
7	Unused	Unused	Unused	Unused
8	Unused	Unused	Unused	Unused

注 10BASE-Tと100BASE-TXでは、送信（TD）と受信（RD）信号は別々の信号線を使用しています。

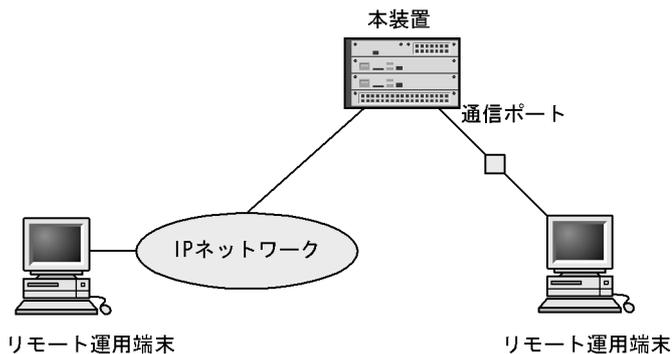
(4) マネージメントポート使用時の注意事項

1. 伝送速度、または全二重および半二重モードが相手装置と不一致の場合、接続できないのでご注意ください。
2. マネージメントポートを100BASE-TXで使用する場合、接続ケーブルはカテゴリ5以上で8芯4対のツイストペアケーブル（UTP）を使用してください。
3. 全二重インタフェースはコリジョン検出とループバック機能を行わないことによって実現しています。このため、10BASE-Tまたは100BASE-TXを全二重インタフェース設定で使用する場合、相手接続インタフェースは必ず全二重に設定して接続してください。
4. マネージメントポートは、リモート運用を主目的としたインタフェースです。マネージメントポートとNIFを経由する通信は250ppsを目安としてください。250ppsを大幅に超える通信環境では、動作が保障できません。

7.1.2 通信用ポート接続

通信用ポートを介して、リモート運用端末から本装置へログインするには、本装置でVLANやIPアドレスなどの設定が必要です。ただし、初期導入時には、VLANやIPアドレスなどの設定が行われていません。そのため、コンソールからログインして、コンフィグレーションを設定する必要があります。

図7-1 リモート運用端末からの本装置へのログイン



7.1.3 ダイアルアップ IP 接続

本装置のシリアル接続ポート（AUX）にダイアルアップ IP 接続でリモート運用端末を接続する手順を次に示します。

(1) 本装置の設定

(a) モデムの準備

あらかじめモデムが自動着信するように設定します。モデムやモデムと AT 互換機を接続するためのストレートケーブルを用意してください。また、本装置ではモデムを設定できないので、PC などに接続して設定してください。

モデムに付属の説明書を参照し、AT コマンドを使用して次の表に示す設定を行ってください。拡張 AT コマンドを持つモデムでは、例で示したコマンドと異なるコマンドを使用する場合があります。

表 7-4 モデムの設定

設定項目	設定内容	指定例 (Hayes 互換 AT コマンドの場合)
CD 信号状態	CD 信号は通常オフで、相手モデムのキャリアを受信するとオンにします。	AT&C1
DTR 信号状態	DTR 信号がオンからオフに変わるとモデムを初期化します。	AT&D3
コマンドエコー	入力したコマンドを DTE に出力しません。	ATE0
フロー制御	DTE と DCE 間のフロー制御を設定します。 • RTS/CTS フロー制御有効 • XON/XOFF フロー制御無効	AT&K3
リザルトコード	リザルトコードを DTE に出力しません。	ATQ1
自動着信	自動着信するまでの呼び出し回数を設定します。	ATS0=2
リセット時の設定	モデム内の不揮発性メモリから設定を読み出します。	AT&Y0
設定の保存	設定をモデム内の不揮発性メモリに保存します。	AT&W0

コマンドを DTE に出力しないようにコマンドエコーを設定すると、コマンドを入力しても文字は表示されません。設定が完了したらモデムに設定内容を保存します。設定保存後に設定内容を表示して確認します。

(例) Hayes 互換 AT コマンドでモデムを自動着信に設定する場合

```
AT&F&C1&D3E0&K3Q1S0=2&W0&Y0&V
```

シリアル接続 (モデム) の場合は、通信ソフトウェアのダイヤル機能を使用してダイヤルします。ダイヤル機能については通信ソフトウェアの説明を参照してください。端末から AT コマンドを使用してダイヤル接続できます。ダイヤル機能を持たない通信ソフトウェアを使用する場合などは AT コマンドでダイヤルしてください。AT コマンドのダイヤル方法についてはモデムのマニュアルを参照してください。

(例) Hayes 互換 AT コマンドでダイヤルする場合

- 公衆回線を使用してトーンで 123-4567 ヘダイヤルする。

```
AT&FE0&S1S0=0S2=255TD123-4567
```

- 構内交換機を使用してトーンで 123-4567 ヘダイヤルする。

```
AT&FX3E0&S1S0=0S2=255TD123-4567
```

- 構内交換機を使用してトーンで 0 をダイヤルして、数秒待ってから 123-4567 ヘダイヤルする。

```
AT&FX3E0&S1S0=0S2=255TD0,123-4567
```

設定したモデムを本装置の AUX ポートに接続します。

7. リモート運用端末から本装置へのログイン

(b) コンフィグレーション設定

本装置で使用する IP アドレスと、リモート運用端末で使用する IP アドレスを設定します。設定するインタフェースは `async` です。

本装置で使用する IP アドレスが 200.10.10.1、リモート運用端末で使用する IP アドレスが 200.10.10.2 の場合、次の図のようにコマンドを実行します。

図 7-2 `async` に関するコンフィグレーション設定例

```
(config)# interface async 1
(config-if)# ip address 200.10.10.1 255.255.255.0
(config-if)# peer default ip address 200.10.10.2
```

(2) リモート運用端末の設定

(a) モデムの準備

本装置にダイヤルアップ IP 接続する運用端末でモデムを使用するための設定方法は、モデムのマニュアルを参照してください。

(b) 接続ソフトの設定

本装置にダイヤルアップ IP 接続する運用端末にダイヤルアップ IP 接続用のソフトをインストールし、次の表のように設定します。

表 7-5 ダイヤルアップ IP 接続設定内容

設定項目	設定内容
サーバの種類	PPP
インターネットプロトコル (TCP/IP)	TCP/IP
IP アドレス	IP アドレスを自動的に取得する
DNS サーバのアドレス	DNS サーバのアドレスを自動的に取得する
認証方式	PAP/ パスワードを暗号化しない
電話番号	本装置に接続するモデムで使用する電話番号

(c) 認証に使用するユーザ名とパスワード

ダイヤルアップ IP 接続の認証に使用するユーザ名とパスワードは、本装置のログインに使用するユーザ名とパスワードを使用します。password コマンドでパスワードを削除してあるユーザ名で認証を行うと、入力したパスワードは無視されます。

(3) 回線接続とログイン

(a) 回線接続

接続ソフトからダイヤルします。

(b) 接続確認

ダイヤルアップ IP 接続を行うと IP アドレスが割り当てられます。ping コマンドなどで宛先アドレスへの通信可否を確認できます。

ダイヤルアップ IP 接続が正しく行われている場合に本装置上で show sessions コマンドを使用すると、ユーザが aux ポートからログインしているように表示され、運用端末で使用している IP アドレスも表示されます。

図 7-3 show sessions コマンド実行例

```
> show sessions
Date 2009/01/07 12:00:00 UTC
gilbert console ----- 0   Jan  6 14:16
john    aux       ----- 1   Jan  6 14:16 (ppp0:200.10.10.2) ... 1
```

1. 「aux」であることを確認します。また、運用端末に割り当てられた IP アドレス (200.10.10.2) が表示されます。

(c) ログイン

リモート運用端末 (リモートログイン) が使用できます。

(4) 回線切断

ダイヤルアップ IP 接続は次の要因で切断されます。

- 運用端末からの切断要求
- 他ログインユーザからの killuser コマンドによるユーザ の強制ログアウト
- 回線障害
- コンフィグレーションコマンド interface async の関連コマンドの変更および削除

注

ここでは AUX ポートからログインしているユーザを指します。

[注意事項]

ダイヤルアップ IP 接続が切断された場合、すぐには再接続できないことがあります。その場合、300 秒程度の間隔を空けてから再接続してください。

7.2 コンフィグレーション

7.2.1 コンフィグレーションコマンド一覧

マネージメントポートのコンフィグレーションコマンド一覧を次の表に示します。

表 7-6 コンフィグレーションコマンド一覧

コマンド名	説明
description	補足説明を設定します。
duplex	マネージメントポートの duplex を設定します。
interface mgmt	マネージメントポートのコンフィグレーションを指定します。
ip routing	マネージメントポートにおける IPv4 のレイヤ 3 中継可否を指定します。
ipv6 routing	マネージメントポートにおける IPv6 のレイヤ 3 中継可否を指定します。
shutdown	マネージメントポートをシャットダウン状態にします。
speed	マネージメントポートの回線速度を設定します。
ip address ¹	マネージメントポートの IPv4 アドレスを指定します。
ipv6 address ²	マネージメントポートの IPv6 アドレスを指定します。
ipv6 enable ²	マネージメントポートの IPv6 機能を有効にします。このコマンドによって、リンクローカルアドレスが自動生成されます。

注 1

「コンフィグレーションコマンドレファレンス Vol.3 2. IPv4・ARP・ICMP」を参照してください。

注 2

「コンフィグレーションコマンドレファレンス Vol.3 16. IPv6・NDP・ICMPv6」を参照してください。

運用端末の接続とリモート操作に関するコンフィグレーションコマンド一覧を次の表に示します。

表 7-7 コンフィグレーションコマンド一覧

コマンド名	説明
ftp-server	リモート運用端末から ftp プロトコルを使用したアクセスを許可します。
line console	コンソール (RS232C) のパラメータを設定します。
line vty	装置への telnet リモートアクセスを許可します。
speed	コンソール (RS232C) の通信速度を設定します。
transport input	リモート運用端末から各種プロトコルを使用したアクセスを規制します。

VLAN の設定、および IPv4/IPv6 インタフェースの設定に関するコンフィグレーションコマンドについては、「19 VLAN」、マニュアル「コンフィグレーションガイド Vol.3 2. IP・ARP・ICMP の設定と運用」、または「コンフィグレーションガイド Vol.3 18. IPv6・NDP・ICMPv6 の設定と運用」を参照してください。

7.2.2 マネージメントポートの設定

(1) マネージメントポートのシャットダウン

[設定のポイント]

マネージメントポートのコンフィグレーションでは、複数のコマンドでコンフィグレーションを設定することがあります。そのとき、コンフィグレーションの設定が完了していない状態でマネージメントポートがリンクアップ状態になると期待した通信ができません。したがって、最初にマネージメントポートをシャットダウンしてから、コンフィグレーションの設定が完了したあとにマネージメントポートのシャットダウンを解除することを推奨します。

[コマンドによる設定]

1. (config)# interface mgmt 0
マネージメントポートの設定を指定します。
2. (config-if)# shutdown
マネージメントポートをシャットダウンします。
3. (config-if)# * * * * *
マネージメントポートに対するコンフィグレーションを設定します。
4. (config-if)# no shutdown
マネージメントポートのシャットダウンを解除します。

[関連事項]

運用コマンド `inactivate` でマネージメントポートの運用を停止することもできます。ただし、`inactivate` コマンドで `inactive` 状態とした場合は、装置を再起動するとマネージメントポートが `active` 状態になります。マネージメントポートをシャットダウンした場合は、装置を再起動してもマネージメントポートは `disable` 状態のままです。マネージメントポートを `active` 状態にするにはコンフィグレーションで `no shutdown` を設定して、シャットダウンを解除する必要があります。

(2) 速度と duplex の設定

本装置と相手装置の伝送速度と duplex を設定できます。デフォルトではオートネゴシエーションで、相手装置と伝送速度および duplex を決定します。

(a) オートネゴシエーションに対応していない相手装置と接続する場合

[設定のポイント]

10BASE-T および 100BASE-TX では、相手装置によってはオートネゴシエーションで接続できない場合があります。その場合は、相手装置に合わせて回線速度と duplex を指定し、固定設定で接続します。

[コマンドによる設定]

1. (config)# interface mgmt 0
(config-if)# shutdown
(config-if)# speed 10
(config-if)# duplex half
相手装置と 10BASE-T 半二重で接続する設定をします。
2. (config)# no shutdown

7. リモート運用端末から本装置へのログイン

(b) オートネゴシエーションでも特定の速度を使用したい場合

[設定のポイント]

本装置は、オートネゴシエーションで接続する場合でも、回線速度を設定できます。オートネゴシエーションに加えて回線速度を設定した場合、相手装置とオートネゴシエーションで接続しても、設定された回線速度にならないときはリンクがアップしません。そのため、意図しない回線速度で接続されることを防止できます。

[コマンドによる設定]

1. (config)# interface mgmt 0
(config-if)# shutdown
(config-if)# speed auto 100

相手装置とオートネゴシエーションで接続しても、100BASE-TX だけで接続するようにします。

2. (config)# no shutdown

[注意事項]

回線速度と duplex は正しい組み合わせで設定してください。オートネゴシエーションの場合は、回線速度と duplex の両方ともにオートネゴシエーションを設定する必要があります。固定設定の場合は、回線速度と duplex の両方を固定設定にする必要があります。正しい組み合わせが設定されていない場合は、オートネゴシエーションで相手装置と接続します。

(3) IPv4 アドレスの設定

[設定のポイント]

マネージメントポートに IPv4 アドレスを設定します。IPv4 アドレスを設定するには、インタフェースコンフィグレーションモードに移行する必要があります。

[コマンドによる設定]

1. (config)# interface mgmt 0

マネージメントポートのインタフェースコンフィグレーションモードに移行します。

2. (config-if)# ip address 192.168.1.1 255.255.255.0

マネージメントポートに IPv4 アドレス 192.168.1.1、サブネットマスク 255.255.255.0 を設定します。

(4) IPv6 アドレスの設定

[設定のポイント]

マネージメントポートに IPv6 アドレスを設定します。ipv6 enable コマンドを設定して、IPv6 機能を有効にする必要があります。ipv6 enable コマンドの設定がない場合、IPv6 設定は無効になります。

[コマンドによる設定]

1. (config)# interface mgmt 0

マネージメントポートのインタフェースコンフィグレーションモードに移行します。

2. (config-if)# ipv6 enable

マネージメントポートに IPv6 アドレス使用可を設定します。

3. `(config-if)# ipv6 address 2001:100::1/64`

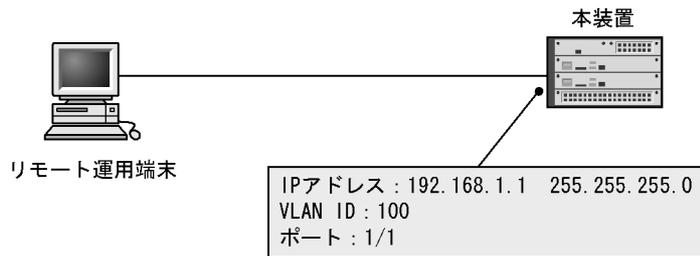
マネージメントポートに IPv6 アドレス 2001:100::1 , プレフィックス長 64 を設定します。

7.2.3 本装置への IP アドレスの設定

[設定のポイント]

リモート運用端末から本装置へアクセスするためには、あらかじめ、接続するインタフェースに対して IP アドレスを設定しておく必要があります。

図 7-4 リモート運用端末との接続例



[コマンドによる設定]

1. `(config)# vlan 100`
`(config-vlan)# exit`

VLAN ID 100 のポート VLAN を作成し、VLAN 100 の VLAN コンフィグレーションモードに移行します。

2. `(config)# interface gigabitethernet 1/1`
`(config-if)# switchport mode access`
`(config-if)# switchport access vlan 100`
`(config-if)# exit`

ポート 1/1 のイーサネットインタフェースコンフィグレーションモードに移行します。ポート 1/1 を VLAN 100 のアクセスポートに設定します。

3. `(config)# interface vlan 100`
`(config-if)# ip address 192.168.1.1 255.255.255.0`
`(config-if)# exit`
`(config)#`

VLAN ID 100 のインタフェースコンフィグレーションモードに移行します。VLAN ID 100 に IPv4 アドレス 192.168.1.1 , サブネットマスク 255.255.255.0 を設定します。

7.2.4 telnet によるログインを許可する

[設定のポイント]

あらかじめ、IP アドレスを設定しておく必要があります。

リモート運用端末から本装置に telnet プロトコルによるリモートログインを許可するには、コンフィグレーションコマンド `line vty` を設定します。

このコンフィグレーションが設定されていない場合、コンソールからだけ本装置にログインできます。

7. リモート運用端末から本装置へのログイン

[コマンドによる設定]

1. (config)# line vty 0 2
(config-line)#

リモート運用端末から本装置への telnet プロトコルによるリモートアクセスを許可します。また、装置に同時にリモートログインできるユーザ数を最大 3 に設定します。

7.2.5 ftp によるログインを許可する

[設定のポイント]

あらかじめ、IP アドレスを設定しておく必要があります。

リモート運用端末から本装置に ftp プロトコルによるリモートアクセスを許可するには、コンフィグレーションコマンド ftp-server を設定します。

このコンフィグレーションが設定されていない場合、ftp プロトコルを用いた本装置へのアクセスはできません。

[コマンドによる設定]

1. (config)# ftp-server

リモート運用端末から本装置への ftp プロトコルによるリモートアクセスを許可します。

7.2.6 VRF での telnet によるログインを許可する【OP-NPAR】

(1) グローバルネットワークを含む全 VRF から telnet によるログインを許可する場合

[設定のポイント]

全 VRF からのアクセスを許可するには、コンフィグレーションコマンド transport input の vrf all パラメータを設定します。この vrf all パラメータが設定されていない場合、グローバルネットワークからのアクセスだけを許可します。

[コマンドによる設定]

1. (config)# line vty 0 2
(config-line)#

リモート運用端末から本装置への telnet プロトコルによるリモートアクセスを許可します。また、装置に同時にリモートログインできるユーザ数を最大 3 に設定します。

2. (config-line)# transport input vrf all telnet
(config-line)#

グローバルネットワークを含む全 VRF で、リモート運用端末から本装置への telnet プロトコルによるリモートアクセスを許可します。

(2) 指定 VRF から telnet によるログインを許可する場合

[設定のポイント]

指定 VRF からのアクセスを許可するには、コンフィグレーションコマンド transport input の vrf パラメータで VRF ID を設定します。この vrf パラメータが設定されていない場合、グローバルネットワークからのアクセスだけを許可します。

[コマンドによる設定]

1. (config)# line vty 0 2

(config-line)#

リモート運用端末から本装置への telnet プロトコルによるリモートアクセスを許可します。また、装置に同時にリモートログインできるユーザ数を最大 3 に設定します。

2. (config-line)# transport input vrf 2 telnet

(config-line)#

VRF 2 で、リモート運用端末から本装置への telnet プロトコルによるリモートアクセスを許可します。なお、グローバルネットワークは含みません。

7.2.7 VRF での ftp によるログインを許可する【OP-NPAR】

(1) グローバルネットワークを含む全 VRF から ftp によるログインを許可する場合

[設定のポイント]

全 VRF からのアクセスを許可するには、コンフィグレーションコマンド ftp-server の vrf all パラメータを設定します。この vrf all パラメータが設定されていない場合、グローバルネットワークからのアクセスだけを許可します。

[コマンドによる設定]

1. (config)# ftp-server vrf all

グローバルネットワークを含む全 VRF で、リモート運用端末から本装置への ftp プロトコルによるリモートアクセスを許可します。

(2) 指定 VRF から ftp によるログインを許可する場合

[設定のポイント]

指定 VRF からのアクセスを許可するには、コンフィグレーションコマンド ftp-server の vrf パラメータで VRF ID を設定します。この vrf パラメータが設定されていない場合、グローバルネットワークからのアクセスだけを許可します。

[コマンドによる設定]

1. (config)# ftp-server vrf 2

VRF 2 で、リモート運用端末から本装置への ftp プロトコルによるリモートアクセスを許可します。なお、グローバルネットワークは含みません。

7.3 オペレーション

7.3.1 運用コマンド一覧

マネージメントポートで使用する運用コマンド一覧を次の表に示します。

表 7-8 運用コマンド一覧

コマンド名	説明
show ip-dual interface ¹	IPv4 および IPv6 インタフェースの状態を表示します。
show ip interface ¹	IPv4 インタフェースの状態を表示します。
show ip arp ¹	ARP エントリ情報を表示します。
clear arp-cache ¹	ダイナミック ARP 情報を削除します。
show netstat(netstat) ¹	ネットワークのステータスを表示します。
clear netstat ¹	ネットワーク統計情報カウンタをクリアします。
clear tcp ¹	TCP コネクションを切断します。
ping ¹	エコーテストを行います。
tracert ¹	経由ルートを表示します。
show ipv6 interface ²	IPv6 インタフェースの状態を表示します。
show ipv6 neighbors ²	NDP 情報を表示します。
clear ipv6 neighbors ²	ダイナミック NDP 情報をクリアします。
ping ipv6 ²	ICMP6 エコーテストを行います。
tracert ipv6 ²	IPv6 経由ルートを表示します。

注 1

「運用コマンドレファレンス Vol.3 2. IPv4・ARP・ICMP」を参照してください。

注 2

「運用コマンドレファレンス Vol.3 9. IPv6・NDP・ICMPv6」を参照してください。

運用端末の接続とリモート操作に関する運用コマンド一覧を次の表に示します。

表 7-9 運用コマンド一覧

コマンド名	説明
set exec-timeout	自動ログアウトが実行されるまでの時間を設定します。
set terminal help	ヘルプメッセージで表示するコマンドの一覧を設定します。
set terminal pager	ページングの実施 / 未実施を設定します。
show history	過去に実行した運用コマンドの履歴を表示します (コンフィグレーションコマンドの履歴は表示しません)。
telnet	指定された IP アドレスのリモート運用端末と仮想端末と接続します。
ftp	本装置と TCP/IP で接続されているリモート端末との間でファイル転送をします。
tftp	本装置と接続されているリモート端末との間で UDP でファイル転送をします。

VLAN の設定，および IPv4/IPv6 インタフェースの設定に関するコンフィグレーションコマンドについては，「19 VLAN」，マニュアル「コンフィグレーションガイド Vol.3 2. IP・ARP・ICMP の設定と運用」，または「コンフィグレーションガイド Vol.3 18. IPv6・NDP・ICMPv6 の設定と運用」を参照してください。

7.3.2 マネージメントポートの確認

(1) IPv4 インタフェースの up/down 確認

IPv4 ネットワークに接続するマネージメントポートに IPv4 アドレスを設定したあとに，show ip interface コマンドを実行し，IPv4 インタフェースの up/down 状態が「UP」であることを確認してください。

図 7-5 「IPv4 インタフェース状態」の表示例

```
> show ip interface summary
MGMT0 : UP 158.215.100.1/24
>
```

7.3.3 リモート運用端末と本装置との通信の確認

本装置とリモート運用端末との通信は，運用コマンド ping や ping ipv6 などを用いて確認できます。詳細は，マニュアル「コンフィグレーションガイド Vol.3 2. IP・ARP・ICMP の設定と運用」，または「コンフィグレーションガイド Vol.3 18. IPv6・NDP・ICMPv6 の設定と運用」を参照してください。

8

ログインセキュリティと RADIUS/ TACACS+

この章では、本装置のログイン制御、ログインセキュリティ、アカウント
リング、および RADIUS/TACACS+ について説明します。

8.1 ログインセキュリティの設定

8.2 RADIUS/TACACS+ の解説

8.3 RADIUS/TACACS+ のコンフィグレーション

8.1 ログインセキュリティの設定

8.1.1 コンフィグレーション・運用コマンド一覧

ログインセキュリティに関するコンフィグレーションコマンド一覧を次の表に示します。

表 8-1 コンフィグレーションコマンド一覧

コマンド名	説明
aaa authentication enable	装置管理者モードへの変更 (enable コマンド) 時に使用する認証方式を指定します。
aaa authentication enable attribute-user-per-method	装置管理者モードへの変更 (enable コマンド) 時の認証に使用するユーザ名属性を変更します。
aaa authentication enable end-by-reject	装置管理者モードへの変更 (enable コマンド) 時の認証で、否認された場合に認証を終了します。
aaa authentication login	リモートログイン時に使用する認証方式を指定します。
aaa authentication login console	コンソール (RS232C) および AUX からのログイン時に aaa authentication login コマンドで指定した認証方式を使用します。
aaa authentication login end-by-reject	ログイン時の認証で、否認された場合に認証を終了します。
aaa authorization commands	RADIUS サーバまたは TACACS+ サーバによるコマンド承認をする場合に指定します。
aaa authorization commands console	コンソール (RS232C) および AUX からのログインの場合に aaa authorization commands コマンドで指定したコマンド承認を行います。
banner	ユーザのログイン前およびログイン後に表示するメッセージを設定します。
commands exec	ローカル (コンフィグレーション) によるコマンド承認で使用するコマンドリストに、コマンド文字列を追加します。
ip access-group	本装置へリモートログインを許可または拒否するリモート運用端末の IPv4 アドレスを指定したアクセスリストを設定します。
ipv6 access-class	本装置へリモートログインを許可または拒否するリモート運用端末の IPv6 アドレスを指定したアクセスリストを設定します。
parser view	ローカル (コンフィグレーション) によるコマンド承認で使用するコマンドリストを生成します。
username	指定ユーザに、ローカル (コンフィグレーション) によるコマンド承認で使用するコマンドリストまたはコマンドクラスを設定します。

ログインセキュリティに関する運用コマンド一覧を次の表に示します。

表 8-2 運用コマンド一覧

コマンド名	説明
adduser	新規ログインユーザ用のアカウントを追加します。
rmuser	adduser コマンドで登録されているログインユーザのアカウントを削除します。
password	ログインユーザのパスワードを変更します。
clear password	ログインユーザのパスワードを削除します。
show sessions	本装置にログインしているユーザを表示します。
show whoami	本装置にログインしているユーザの中で、このコマンドを実行したログインユーザだけを表示します。

コマンド名	説明
killuser	ログイン中のユーザを強制的にログアウトさせます。

8.1.2 ログイン制御の概要

本装置にはローカルログイン（シリアル接続）と IPv4 および IPv6 ネットワーク経由のリモートログイン機能（telnet）があります。

本装置ではログイン時およびログイン中に次に示す制御を行っています。

1. ログイン時に不正アクセスを防止するため、ユーザ ID によるコマンドの使用範囲の制限やパスワードによるチェックを設けています。
2. 複数の運用端末から同時にログインできます。
3. 本装置にログインできるリモートユーザ数は最大 16 ユーザです。なお、コンフィグレーションコマンド line vty でログインできるユーザ数を制限できます。
4. 本装置にアクセスできる IPv4 および IPv6 アドレスをコンフィグレーションコマンド ip access-list standard, ipv6 access-list, access-list, ip access-group, ipv6 access-class で制限できます。
5. 本装置にアクセスできるプロトコル（telnet, ftp）をコンフィグレーションコマンド transport input や ftp-server で制限できます。
6. VRF で本装置にアクセスできる IPv4 および IPv6 アドレスをコンフィグレーションコマンド ip access-list standard, ipv6 access-list, access-list, ip access-group, ipv6 access-class で制限できます。**【OP-NPAR】**
7. VRF で本装置にアクセスできるプロトコル（telnet, ftp）をコンフィグレーションコマンド transport input や ftp-server で制限できます。**【OP-NPAR】**
8. コマンド実行結果はログインした端末だけに表示します。運用メッセージはログインしているすべての運用端末に表示されます。
9. 入力したコマンドとその応答メッセージおよび運用メッセージを運用ログとして収集します。運用ログは運用コマンド show logging で参照できます。
10. キー入力が最大 60 分間ない場合は自動的にログアウトします。
11. 運用コマンド killuser を使用してユーザを強制ログアウトできます。

8.1.3 ログインユーザの作成と削除

adduser コマンドを用いて本装置にログインできるユーザを作成してください。ログインユーザの作成例を次の図に示します。

図 8-1 ユーザ newuser を作成

```
> enable
# adduser newuser
User(empty password) add done. Please setting password.

Changing local password for newuser.
New password:***** ... 1
Retype new password:***** ... 2
# quit
>
```

1. パスワードを入力します（実際には入力文字は表示されません）。
2. 確認のため再度パスワードを入力します（実際には入力文字は表示されません）。

また、使用しなくなったユーザは rmuser コマンドを用いて削除できます。

特に、初期導入時に設定されているログインユーザ "operator" を運用中のログインユーザとして使用しない場合、セキュリティの低下を防ぐため、新しいログインユーザを作成したあとに `rmuser` コマンドで削除することをお勧めします。また、コンフィグレーションコマンド `aaa authentication login` で、RADIUS/TACACS+ を使用したログイン認証ができます。コンフィグレーションの設定例については、「8.3.2 RADIUS サーバによる認証の設定」および「8.3.3 TACACS+ サーバによる認証の設定」を参照してください。

なお、作成したログインユーザ名は忘れないようにしてください。ログインユーザ名を忘れると、デフォルトリスタートで起動してもログインできないので注意してください。

8.1.4 装置管理者モード変更のパスワードの設定

コンフィグレーションコマンドを実行するためには `enable` コマンドで装置管理者モードに変更する必要があります。初期導入時に `enable` コマンドを実行した場合、パスワードは設定されていませんので認証なしで装置管理者モードに変更します。ただし、通常運用中にすべてのユーザがパスワード認証なしで装置管理者モードに変更できるのはセキュリティ上危険ですので、初期導入時にパスワードを設定しておいてください。パスワード設定の実行例を次の図に示します。

図 8-2 初期導入直後の装置管理者モード変更のパスワード設定

```
> enable
# password enable-mode
Changing local password for admin.
New password:
Retype new password:
#
```

また、コンフィグレーションコマンド `aaa authentication enable` で、RADIUS/TACACS+ を使用した認証ができます。コンフィグレーションの設定例については、「8.3.2 RADIUS サーバによる認証の設定」および「8.3.3 TACACS+ サーバによる認証の設定」を参照してください。

8.1.5 リモート運用端末からのログインの許可

コンフィグレーションコマンド `line vty` を設定することで、リモート運用端末から本装置へログインできるようになります。このコンフィグレーションが設定されていない場合、コンソールからだけ本装置にログインできます。リモート運用端末からのログインを許可する設定例を次の図に示します。

図 8-3 リモート運用端末からのログインを許可する設定例

```
(config)# line vty 0 2
(config-line)#
```

また、リモート運用端末から `ftp` プロトコルを用いて、本装置にアクセスする場合には、コンフィグレーションコマンド `ftp-server` を設定する必要があります。本設定を実施しない場合、`ftp` プロトコルを用いた本装置へのアクセスはできません。

図 8-4 ftp プロトコルによるアクセス許可の設定例

```
(config)# ftp-server
(config)#
```

8.1.6 同時にログインできるユーザ数の設定

コンフィグレーションコマンド `line vty` を設定することで、リモート運用端末から本装置へログインできるようになります。line vty コマンドの `<num>` パラメータで、リモートログインできるユーザ数が制限されます。なお、この設定にかかわらず、コンソールからは常にログインできます。2人まで同時にログインを許可する設定例を次の図に示します。

図 8-5 同時にログインできるユーザ数の設定例

```
(config)# line vty 0 1
(config-line)#
```

同時ログインに関する動作概要を次に示します。

複数ユーザが同時にログインすると、ログインしているユーザ数が制限数以下でもログインできない場合があります。

同時にログインできるユーザ数を変更しても、すでにログインしているユーザのセッションが切れることはありません。

8.1.7 リモート運用端末からのログインを許可する IP アドレスの設定

リモート運用端末から本装置へのログインを許可する IP アドレスを設定することで、ログインを制限できます。なお、設定後はリモート運用端末から本装置へのログインの可否を確認してください。

[設定のポイント]

特定のリモート運用端末からだけ、本装置へのアクセスを許可する場合は、コンフィグレーションコマンド `ip access-list standard`、`ipv6 access-list`、`access-list`、`ip access-group`、`ipv6 access-class` であらかじめアクセスを許可する端末の IP アドレスを登録しておく必要があります。アクセスを許可する IPv4 アドレスとサブネットマスク、または IPv6 アドレスとプレフィックスは、合わせて最大 128 個の登録ができます。このコンフィグレーションを実施していない場合、すべてのリモート運用端末から本装置へのアクセスが可能となります。なお、アクセスを許可していない（コンフィグレーションで登録していない）端末からのアクセスがあった場合、すでにログインしているそのほかの端末には、アクセスがあったことを示す "Unknown host address <IP アドレス>" のメッセージが表示されます。アクセスを許可する IP アドレスを変更しても、すでにログインしているユーザのセッションは切れません。

[コマンドによる設定](IPv4 の場合)

1. (config)# ip access-list standard REMOTE
(config-std-nacl)# permit 192.168.0.0 0.0.0.255
(config-std-nacl)# exit

ネットワーク (192.168.0.0/24) からだけログインを許可するアクセスリスト情報 REMOTE を設定します。

2. (config)# line vty 0 2
(config-line)# ip access-group REMOTE in
(config-line)#

line モードに遷移し、アクセスリスト情報 REMOTE を適用し、ネットワーク (192.168.0.0/24) にあるリモート運用端末からだけログインを許可します。


```

3. (config)# show banner login plain-text
#####
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.
#####
(config)#

```

show の際に plain-text パラメータを指定すると、テキスト形式で確認できます。

設定が完了したら、リモート運用端末の telnet または ftp クライアントから本装置へ接続します。接続後、クライアントにメッセージが表示されます。

図 8-6 リモート運用端末から本装置へ接続した例

telnetで接続した場合

```

> telnet 10.10.10.10
Trying 10.10.10.10...
Connected to 10.10.10.10.
Escape character is '^]'.

#####
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.
#####
login:

```

ftpで接続した場合

```

> ftp 10.10.10.10
Connected to 10.10.10.10.
220-
#####
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.
#####
220 10.10.10.10 FTP server (NetBSD-ftpd) ready.
Name (10.10.10.10:staff):

```

8.1.9 VRF でのリモート運用端末からのログインの許可【OP-NPAR】

コンフィグレーションコマンド line vty を設定することで、リモート運用端末から本装置にログインできるようになります。さらに、コンフィグレーションコマンド transport input の vrf パラメータを設定して、VRF からのアクセスを許可します。この vrf パラメータが設定されていない場合、グローバルネットワークからのアクセスだけを許可します。

グローバルネットワークを含む全 VRF で、リモート運用端末から本装置への telnet プロトコルによるリモートアクセスを許可する設定例を次の図に示します。

図 8-7 グローバルネットワークを含む全 VRF でリモート運用端末からのログインを許可する設定例

```

(config)# line vty 0 2
(config-line)# transport input vrf all telnet
(config-line)#

```

指定 VRF で、リモート運用端末から本装置への telnet プロトコルによるリモートアクセスを許可する設

定例を次の図に示します。なお、グローバルネットワークは含みません。

図 8-8 VRF 2 でリモート運用端末からのログインを許可する設定例

```
(config)# line vty 0 2
(config-line)# transport input vrf 2 telnet
(config-line)#
```

また、リモート運用端末から ftp プロトコルを使用して本装置にアクセスする場合には、コンフィグレーションコマンド ftp-server を設定する必要があります。VRF からのアクセスを許可する場合は、vrf パラメータを設定します。この vrf パラメータが設定されていない場合、グローバルネットワークからのアクセスだけを許可します。

グローバルネットワークを含む全 VRF で、リモート運用端末から本装置への ftp プロトコルによるリモートアクセスを許可する設定例を次の図に示します。

図 8-9 グローバルネットワークを含む全 VRF でリモート運用端末から ftp プロトコルによるアクセスを許可する設定例

```
(config)# ftp-server vrf all
(config)#
```

指定 VRF で、リモート運用端末から本装置への ftp プロトコルによるリモートアクセスを許可する設定例を次の図に示します。なお、グローバルネットワークは含みません。

図 8-10 VRF 2 でリモート運用端末から ftp プロトコルによるアクセスを許可する設定例

```
(config)# ftp-server vrf 2
(config)#
```

8.1.10 VRF でのリモート運用端末からのログインを許可する IP アドレスの設定【OP-NPAR】

リモート運用端末から本装置へのログインを許可する IP アドレスをアクセスリストに設定することで、ログインを制限できます。

アクセスリストは、グローバルネットワークや VRF に対して個別に設定しますが、同一のアクセスリストを、グローバルネットワークを含むすべての VRF に適用する設定もできます。また、これらを組み合わせ設定できますが、複数のアクセスリストを使用する場合は、最後のアクセスリストだけ暗黙の廃棄が適用されます。

なお、アクセス元の VRF に対してアクセスリストがどのように適用される（アクセスリストの適用範囲）かは、アクセス元とアクセスリストの設定箇所との関係によって変わります。例として、グローバルネットワーク、VRF 10 および VRF 20 から本装置にアクセスする場合、アクセスリストが設定されている箇所によって、どのアクセスリストが適用されるかを次の表に示します（括弧内が、どのアクセスリストが適用されるかを示しています）。

表 8-3 アクセスリストの適用範囲

アクセスリスト設定箇所	アクセス元 VRF		
	グローバルネットワーク	VRF 10	VRF 20
• global	(global)	-	-

アクセスリスト設定箇所	アクセス元 VRF		
	グローバルネットワーク	VRF 10	VRF 20
<ul style="list-style-type: none"> global VRF 10 	(global)	(VRF 10)	-
<ul style="list-style-type: none"> global VRF 10 VRF ALL 	(global) 適用後 (VRF ALL)	(VRF 10) 適用後 (VRF ALL)	(VRF ALL)

(凡例)

- : アクセスリストは適用されない。したがって、アクセス制限されない。

global : グローバルネットワーク

VRF 10 : VRF 10

VRF ALL : グローバルネットワークを含む全 VRF

注

個別に設定したアクセスリストは、VRF ALL に設定したアクセスリストよりも優先して適用されます。また、アクセスリストを複数使用しているため、個別に設定したアクセスリストの暗黙の廃棄は無視されます。そのため、個別に設定したアクセスリストに一致しない場合は、VRF ALL に設定したアクセスリストが適用されます。VRF ALL に設定したアクセスリストに一致しない場合は、暗黙の廃棄によって制限されます。

なお、設定後はリモート運用端末から本装置へのログインの可否を確認してください。

[設定のポイント]

特定のリモート運用端末からだけ本装置へのアクセスを許可する場合は、アクセスリストを使用します。コンフィギュレーションコマンド `ip access-list standard`、`ipv6 access-list`、`access-list`、`ip access-group`、`ipv6 access-class` で、あらかじめアクセスを許可する端末の IP アドレスを登録しておく必要があります。アクセスを許可する IPv4 アドレスとサブネットマスク、または IPv6 アドレスとプレフィックスは、合わせて最大 128 個の登録ができます。このコンフィギュレーションを設定していない場合、すべてのリモート運用端末から本装置へのアクセスが可能となります。なお、アクセスを許可していない (コンフィギュレーションで登録していない) 端末からのアクセスがあった場合、すでにログインしているそのほかの端末には、アクセスがあったことを示す "Unknown host address <IP アドレス>" のメッセージが表示されます。

設定例を次に示します。まず、グローバルネットワークを含む全 VRF でのリモート運用端末からのログインを制限します。次に、グローバルネットワークと指定 VRF だけ個別にログインを許可します。これによって、特定のネットワークからだけログインを許可します。

[コマンドによる設定]

- ```
(config)# ip access-list standard REMOTE_VRFALL
(config-std-nacl)# deny any
(config-std-nacl)# exit
```

グローバルネットワークを含む全 VRF で、ログインを制限するアクセスリスト REMOTE\_VRFALL を設定します。

- ```
(config)# ip access-list standard REMOTE_GLOBAL
(config-std-nacl)# permit 192.168.0.0 0.0.0.255
(config-std-nacl)# exit
```

グローバルネットワークで、ネットワーク (192.168.0.0/24) からだけログインを許可するアクセスリスト REMOTE_GLOBAL を設定します。

```
3. (config)# ip access-list standard REMOTE_VRF10
   (config-std-nacl)# permit 10.10.10.0 0.0.0.255
   (config-std-nacl)# exit
```

VRF 10 で、ネットワーク (10.10.10.0/24) からだけログインを許可するアクセスリスト REMOTE_VRF10 を設定します。

```
4. (config)# line vty 0 2
   (config-line)# ip access-group REMOTE_VRFALL vrf all in
   (config-line)# ip access-group REMOTE_GLOBAL in
   (config-line)# ip access-group REMOTE_VRF10 vrf 10 in
   (config-line)#
```

line モードに遷移し、グローバルネットワークを含む全 VRF にアクセスリスト REMOTE_VRFALL を、グローバルネットワークにアクセスリスト REMOTE_GLOBAL を、VRF10 にアクセスリスト REMOTE_VRF10 を適用します。

グローバルネットワークでは、ネットワーク (192.168.0.0/24) にあるリモート運用端末からだけログインを許可します。

VRF10 では、ネットワーク (10.10.10.0/24) にあるリモート運用端末からだけログインを許可します。また、その他の VRF ではログインを制限します。

8.2 RADIUS/TACACS+ の解説

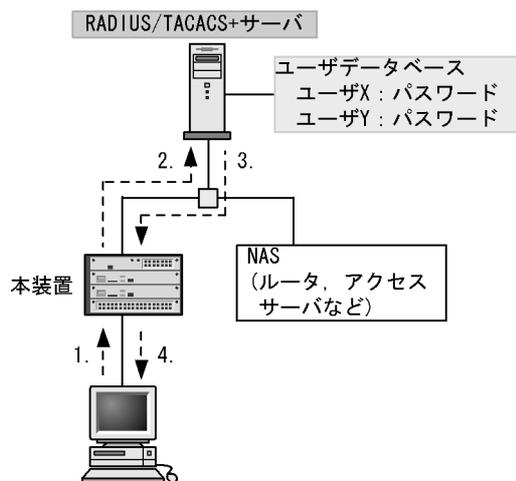
8.2.1 RADIUS/TACACS+ の概要

RADIUS (Remote Authentication Dial In User Service), TACACS+ (Terminal Access Controller Access Control System Plus) とは, NAS (Network Access Server) に対して認証, 承認, およびアカウントリングを提供するプロトコルです。NAS は RADIUS/TACACS+ のクライアントとして動作するリモートアクセスサーバ, ルータなどの装置のことです。NAS は構築されている RADIUS/TACACS+ サーバに対してユーザ認証, コマンド承認, およびアカウントリングなどのサービスを要求します。RADIUS/TACACS+ サーバはその要求に対して, サーバ上に構築された管理情報データベースに基づいて要求に対する応答を返します。本装置は NAS の機能をサポートします。

RADIUS/TACACS+ を使用すると一つの RADIUS/TACACS+ サーバだけで, 複数 NAS でのユーザパスワードなどの認証情報や, コマンド承認情報やアカウントリング情報を一元管理できるようになります。本装置では, RADIUS/TACACS+ サーバに対してユーザ認証, コマンド承認, およびアカウントリングを要求できます。

RADIUS/TACACS+ 認証の流れを次の図に示します。

図 8-11 RADIUS/TACACS+ 認証の流れ



1. リモート運用端末からユーザXが本装置にtelnetを実行する。
2. 本装置はコンフィグレーションで指定したRADIUS/TACACS+サーバに対して認証を要求する。
3. RADIUS/TACACS+サーバはユーザデータベースに基づいてユーザXを認証し, 本装置にユーザXを認証したことを通知する。
4. 本装置はRADIUS/TACACS+認証に基づいて, ユーザXのリモート運用端末からのtelnet許可する。
5. 本装置はコンフィグレーションでコマンド承認を設定した場合, RADIUS/TACACS+サーバに設定してあるコマンドリストに従って, ユーザが投入する運用コマンドを許可/制限する。

8.2.2 RADIUS/TACACS+ の適用機能および範囲

本装置では RADIUS/TACACS+ を, 運用端末からのログイン認証と装置管理者モードへの変更 (enable コマンド) 時の認証, コマンド承認, およびアカウントリングに使用します。また, RADIUS は IEEE802.1X および Web 認証の端末認証にも使用します。RADIUS/TACACS+ 機能のサポート範囲を次

に示します。

(1) RADIUS/TACACS+ の適用範囲

RADIUS/TACACS+ 認証を適用できる操作を次に示します。

- 本装置への telnet (IPv4/IPv6)
- 本装置への ftp (IPv4/IPv6)
- コンソール (RS232C) および AUX からのログイン
- 装置管理者モードへの変更 (enable コマンド)

RADIUS/TACACS+ コマンド承認を適用できる操作を次に示します。

- 本装置への telnet (IPv4/IPv6)
- コンソール (RS232C) および AUX からのログイン

RADIUS/TACACS+ アカウンティングを適用できる操作を次に示します。

- 本装置への telnet (IPv4/IPv6) によるログイン・ログアウト
- 本装置への ftp (IPv4/IPv6) によるログイン・ログアウト
- コンソール (RS232C) および AUX からのログイン・ログアウト
- CLI でのコマンド入力 (TACACS+ だけサポート)
- システム操作パネルでのコマンド入力 (TACACS+ だけサポート)

(2) RADIUS のサポート範囲

RADIUS サーバに対して、本装置がサポートする NAS 機能を次の表に示します。

表 8-4 RADIUS のサポート範囲

分類	内容
文書全体	NAS に関する記述だけを対象にします。
パケットタイプ	ログイン認証, 装置管理者モードへの変更 (enable コマンド) 時の認証, コマンド承認で使用する次のタイプ <ul style="list-style-type: none"> • Access-Request (送信) • Access-Accept (受信) • Access-Reject (受信) アカウンティングで使用する次のタイプ <ul style="list-style-type: none"> • Accounting-Request (送信) • Accounting-Response (受信)

分類	内容
属性	<p>ログイン認証と装置管理者モードへの変更 (enable コマンド) 時の認証で使用する次の属性</p> <ul style="list-style-type: none"> • User-Name • User-Password • Service-Type • NAS-IP-Address • NAS-IPv6-Address • NAS-Identifier • Reply-Message <p>コマンド承認で使用する次の属性</p> <ul style="list-style-type: none"> • Class • Vendor-Specific(Vendor-ID=21839) <p>アカウントングで使用する次の属性</p> <ul style="list-style-type: none"> • User-Name • NAS-IP-Address • NAS-IPv6-Address • NAS-Port • NAS-Port-Type • Service-Type • Calling-Station-Id • Acct-Status-Type • Acct-Delay-Time • Acct-Session-Id • Acct-Authentic • Acct-Session-Time

(a) 使用する RADIUS 属性の内容

使用する RADIUS 属性の内容を次の表に示します。

RADIUS サーバを利用してコマンド承認する場合は、認証時に下の表に示すような Class や Vendor-Specific を返すようにあらかじめ RADIUS サーバを設定しておく必要があります。RADIUS サーバには、ベンダー固有属性を登録 (dictionary ファイルなどに設定) してください。コマンド承認の属性詳細については、「8.2.4 RADIUS/TACACS+/ ローカルを使用したコマンド承認」を参照してください。

表 8-5 使用する RADIUS 属性の内容

属性名	属性値	パケットタイプ	内容
User-Name	1	Access-Request Accounting-Request	認証するユーザの名前。 ログイン認証の場合は、ログインユーザ名を送信します。 装置管理者モードへの変更 (enable コマンド) 時の認証の場合は、「表 8-10 設定するユーザ名属性」に従ってユーザ名を送信します。
User-Password	2	Access-Request	認証ユーザのパスワード。送信時には暗号化されます。
Service-Type	6	Access-Request Accounting-Request	Login(値=1)。Administrative(値=6、ただしパケットタイプが Access-Request の場合だけ使用)。Access-Accept および Access-Reject に添付された場合は無視します。
NAS-IP-Address	4	Access-Request Accounting-Request	本装置の IP アドレス。ローカルアドレスが設定されている場合はローカルアドレス、ローカルアドレスが設定されていない場合は送信インタフェースの IP アドレスになります。

属性名	属性値	パケットタイプ	内容
NAS-IPv6-Address	95	Access-Request Accounting-Request	本装置の IPv6 アドレス。ローカルアドレスが設定されている場合はローカルアドレス、ローカルアドレスが設定されていない場合は送信インタフェースの IPv6 アドレスになります。ただし、IPv6 リンクローカルアドレスで通信する場合は、ローカルアドレス設定の有無にかかわらず送信インタフェースの IPv6 リンクローカルアドレスになります。
NAS-Identifier	32	Access-Request Accounting-Request	本装置の装置名。装置名が設定されていない場合は添付されません。
Reply-Message	18	Access-Accept Access-Reject Accounting-Response	サーバからのメッセージ。添付されている場合は、運用ログとして出力されます。
Class	25	Access-Accept	ログインクラス。コマンド承認で適用します。
Vendor-Specific	26	Access-Accept	ログインリスト。コマンド承認で適用します。
NAS-Port	5	Accounting-Request	ユーザが接続されている NAS のポート番号を指します。本装置では、tty ポート番号を格納します。ただし、ftp の場合は 100 を格納します。
NAS-Port-Type	61	Accounting-Request	NAS に接続した方法を指します。本装置では、telnet/ftp は Virtual(5)、コンソール/AUX は Async(0) を格納します。
Calling-Station-Id	31	Accounting-Request	利用者の識別 ID を指します。本装置では、telnet/ftp はクライアントの IPv4/IPv6 アドレス、コンソールは " console "、AUX は " aux " を格納します。
Acct-Status-Type	40	Accounting-Request	Accounting-Request がどのタイミングで送信されたかを指します。本装置では、ユーザのログイン時に Start(1)、ログアウト時に Stop(2) を格納します。
Acct-Delay-Time	41	Accounting-Request	送信する必要があるイベント発生から Accounting-Request を送信するまでにかかった時間 (秒) を格納します。
Acct-Session-Id	44	Accounting-Request	セッションを識別するための文字列を指します。本装置では、セッションのプロセス ID を格納します。
Acct-Authentic	45	Accounting-Request	ユーザがどのように認証されたかを指します。本装置では、RADIUS(1)、Local(2)、Remote(3) の 3 種類を格納します。
Acct-Session-Time	46	Accounting-Request (Acct-Status-Type が Stop の場合だけ)	ユーザがサービスを利用した時間 (秒) を指します。本装置では、ユーザがログイン後ログアウトするまでの時間 (秒) を格納します。

- Access-Request パケット
本装置が送信するパケットには、この表で示す以外の属性は添付しません。
- Access-Accept, Access-Reject, Accounting-Response パケット
この表で示す以外の属性が添付されていた場合、本装置ではそれらの属性を無視します。

(3) TACACS+ のサポート範囲

TACACS+ サーバに対して、本装置がサポートする NAS 機能を次の表に示します。

表 8-6 TACACS+ のサポート範囲

分類		内容
パケットタイプ		ログイン認証と装置管理者モードへの変更 (enable コマンド) 時の認証で使用する次のタイプ <ul style="list-style-type: none"> • Authentication Start (送信) • Authentication Reply (受信) • Authentication Continue (送信) コマンド承認で使用する次のタイプ <ul style="list-style-type: none"> • Authorization Request (送信) • Authorization Response (受信) アカウンティングで使用する次のタイプ <ul style="list-style-type: none"> • Accounting Request (送信) • Accounting Reply (受信)
ログイン認証	属性	<ul style="list-style-type: none"> • User • Password • priv-lvl
装置管理者モードへの変更 (enable コマンド) 時の認証		
コマンド承認	service	<ul style="list-style-type: none"> • taclogin
	属性	<ul style="list-style-type: none"> • class • allow-commands • deny-commands
アカウンティング	flag	<ul style="list-style-type: none"> • TAC_PLUS_ACCT_FLAG_START • TAC_PLUS_ACCT_FLAG_STOP
	属性	<ul style="list-style-type: none"> • task_id • start_time • stop_time • elapsed_time • timezone • service • priv-lvl • cmd

(a) 使用する TACACS+ 属性の内容

使用する TACACS+ 属性の内容を次の表に示します。

TACACS+ サーバを利用してコマンド承認する場合は、認証時に class または allow-commands や deny-commands 属性とサービスを返すように TACACS+ サーバ側で設定します。コマンド承認の属性詳細については、「8.2.4 RADIUS/TACACS+/ ローカルを使用したコマンド承認」に示します。

表 8-7 使用する TACACS+ 属性の内容

service	属性	説明
-	User	認証するユーザの名前。 ログイン認証の場合は、ログインユーザ名を送信します。 装置管理者モードへの変更 (enable コマンド) 時の認証の場合は、「表 8-10 設定するユーザ名属性」に従ってユーザ名を送信します。
	Password	認証ユーザのパスワード。送信時には暗号化されます。

service	属性	説明
	priv-lvl	認証するユーザの特権レベル。 ログイン認証の場合、1 を使用します。装置管理者モードへの変更 (enable コマンド) 時の認証の場合、15 を使用します。
taclogin	class	コマンドクラス
	allow-commands	許可コマンドリスト
	deny-commands	制限コマンドリスト

(凡例) - : 該当なし

アカウントティング時に使用する TACACS+ flag を次の表に示します。

表 8-8 TACACS+ アカウントティング flag 一覧

flag	内容
TAC_PLUS_ACCT_FLAG_START	アカウントティング START パケットを示します。ただし、aaa コンフィグレーションで送信契機に stop-only を指定している場合は、アカウントティング START パケットは送信しません。
TAC_PLUS_ACCT_FLAG_STOP	アカウントティング STOP パケットを示します。ただし、aaa コンフィグレーションで送信契機に stop-only を指定している場合は、このアカウントティング STOP パケットだけを送信します。

アカウントティング時に使用する TACACS+ 属性 (Attribute-Value) の内容を次の表に示します。

表 8-9 TACACS+ アカウントティング Attribute-Value 一覧

Attribute	Value
task_id	イベントごとに割り当てられる ID です。本装置ではアカウントティングイベントのプロセス ID を格納します。
start_time	イベントを開始した時刻です。本装置ではアカウントティングイベントが開始された時刻を格納します。この属性は次のイベントで格納されます。 <ul style="list-style-type: none"> 送信契機 start-stop 指定時のログイン時、コマンド実行前 送信契機 stop-only 指定時のコマンド実行前
stop_time	イベントを終了した時刻です。本装置ではアカウントティングイベントが終了した時刻を格納します。この属性は次のイベントで格納されます。 <ul style="list-style-type: none"> 送信契機 start-stop 指定時のログアウト時、コマンド実行後 送信契機 stop-only 指定時のログアウト時
elapsed_time	イベント開始からの経過時間 (秒) です。本装置ではアカウントティングイベントの開始から終了までの時間 (秒) を格納します。この属性は次のイベントで格納されます。 <ul style="list-style-type: none"> 送信契機 start-stop 指定時のログアウト時、コマンド実行後 送信契機 stop-only 指定時のログアウト時
timezone	タイムゾーン文字列を格納します。
service	文字列 " shell " を格納します。
priv-lvl	コマンドアカウントティング設定時に、入力されたコマンドが運用コマンドの場合は 1、コンフィグレーションコマンドの場合は 15 を格納します。
cmd	コマンドアカウントティング設定時に、入力されたコマンド文字列 (最大 250 文字) を格納します。

8.2.3 RADIUS/TACACS+ を使用した認証

RADIUS/TACACS+ を使用した認証方法について説明します。

(1) 認証サービスの選択

ログイン認証および装置管理者モードへの変更（enable コマンド）時の認証に使用するサービスは複数指定できます。指定できるサービスは RADIUS，TACACS+ および adduser/password コマンドによる本装置単体でのログインセキュリティ機能です。

これらの認証方式は単独でも同時でも指定できます。同時に指定された場合に先に指定された方式で認証に失敗したときの認証サービスの選択動作を，次に示す end-by-reject を設定するコンフィグレーションコマンドで変更できます。

ログイン認証の場合

```
aaa authentication login end-by-reject
```

装置管理者モードへの変更（enable コマンド）時の認証の場合

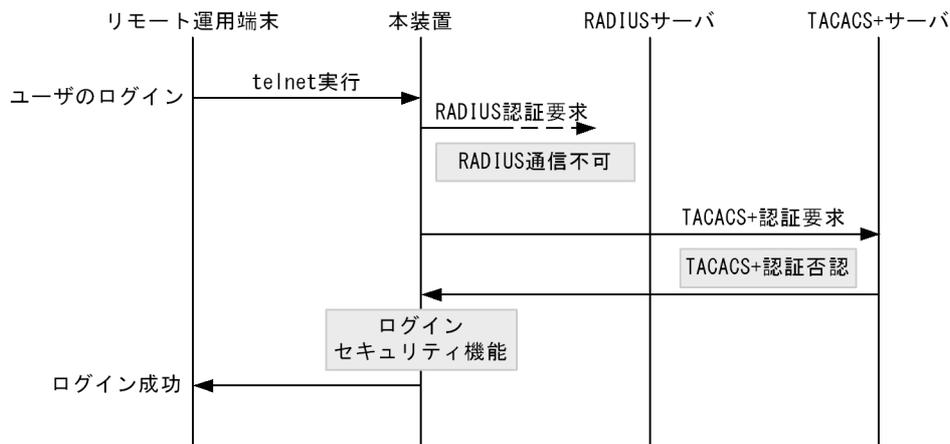
```
aaa authentication enable end-by-reject
```

(a) end-by-reject 未設定時

end-by-reject 未設定時の認証サービスの選択について説明します。end-by-reject 未設定時は，先に指定された方式で認証に失敗した場合に，その失敗の理由に関係なく，次に指定された方式で認証できます。

例として，コンフィグレーションで認証方式に RADIUS，TACACS+，単体でのログインセキュリティの順番で指定し，それぞれの認証結果が RADIUS サーバ通信不可，TACACS+ サーバ認証否認，ログインセキュリティ機能認証成功となる場合の認証方式シーケンスを次の図に示します。

図 8-12 認証方式シーケンス（end-by-reject 未設定時）



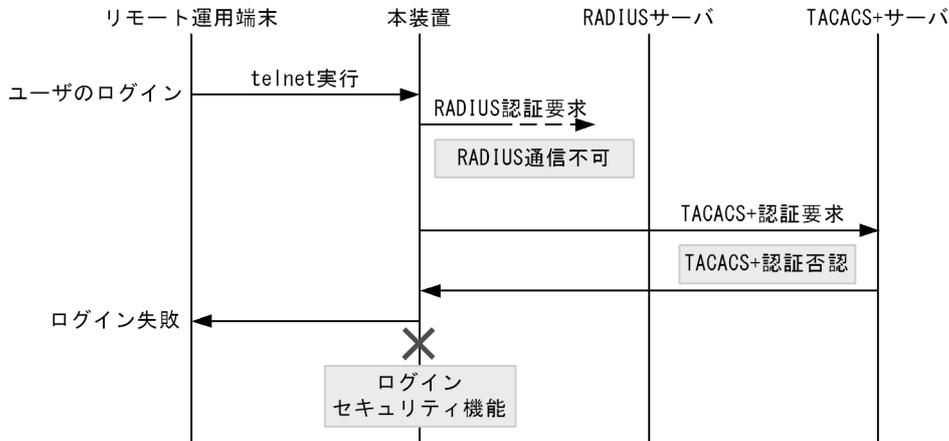
この図で端末からユーザが本装置に telnet を実行すると，RADIUS サーバに対し本装置から RADIUS 認証を要求します。RADIUS サーバとの通信不可によって RADIUS サーバでの認証に失敗すると，次に TACACS+ サーバに対し本装置から TACACS+ 認証を要求します。TACACS+ 認証否認によって TACACS+ サーバでの認証に失敗すると，次に本装置のログインセキュリティ機能での認証を実行します。ここで認証に成功し，ユーザは本装置へのログインに成功します。

(b) end-by-reject 設定時

end-by-reject 設定時の認証サービスの選択について説明します。end-by-reject 設定時は，先に指定された方式で認証否認された場合に，次に指定された方式で認証を行いません。否認された時点で認証を終了し，一連の認証が失敗となります。通信不可などの異常によって認証が失敗した場合だけ，次に指定された方式で認証できます。

例として、コンフィグレーションで認証方式に RADIUS, TACACS+, 単体でのログインセキュリティの順番で指定し、それぞれの認証結果が RADIUS サーバ通信不可, TACACS+ サーバ認証否認となる場合の認証方式シーケンスを次の図に示します。

図 8-13 認証方式シーケンス (end-by-reject 設定時)



この図で端末からユーザが本装置に telnet を実行すると、RADIUS サーバに対し本装置から RADIUS 認証を要求します。RADIUS サーバとの通信不可によって RADIUS サーバでの認証に失敗すると、次に TACACS+ サーバに対し本装置から TACACS+ 認証を要求します。TACACS+ 認証否認によって TACACS+ サーバでの認証に失敗すると、この時点で一連の認証が失敗となり、認証を終了します。次に指定されている本装置のログインセキュリティ機能での認証を実行しません。その結果、ユーザは本装置へのログインに失敗します。

(2) RADIUS/TACACS+ サーバの選択

RADIUS サーバ, TACACS+ サーバはそれぞれ最大四つまで指定できます。一つのサーバと通信できず、認証サービスが受けられない場合は、順次これらのサーバへの接続を試行します。

また、RADIUS サーバ, TACACS+ サーバをホスト名で指定したときに、複数のアドレスが解決できた場合は、優先順序に従い、アドレスを一つだけ決定し、RADIUS サーバ, TACACS+ サーバと通信します。

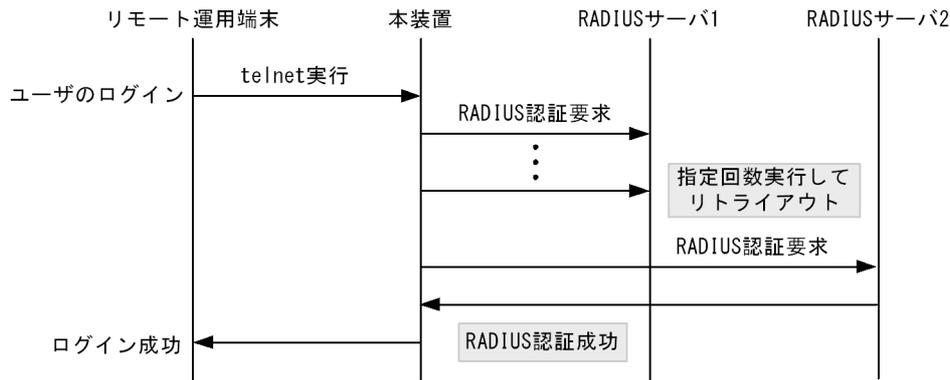
優先順序についての詳細は、「10 ホスト名と DNS 10.1 解説」を参照してください。

注意

DNS サーバを使用してホスト名を解決する場合、DNS サーバとの通信に時間が掛かることがあります。このため、RADIUS サーバ, TACACS+ サーバは IP アドレスで指定することをお勧めします。

RADIUS/TACACS+ サーバと通信不可を判断するタイムアウト時間を設定できます。デフォルト値は 5 秒です。また、各 RADIUS サーバでタイムアウトした場合は、再接続を試行します。この再試行回数も設定でき、デフォルト値は 3 回です。このため、ログイン方式として RADIUS が使用できないと判断するまでの最大時間は、タイムアウト時間×リトライ回数×RADIUS サーバ設定数になります。なお、各 TACACS+ サーバでタイムアウトした場合は、再接続を試行しません。このため、ログイン方式として TACACS+ が使用できないと判断するまでの最大時間は、タイムアウト時間×TACACS+ サーバ設定数になります。RADIUS サーバ選択のシーケンスを次の図に示します。

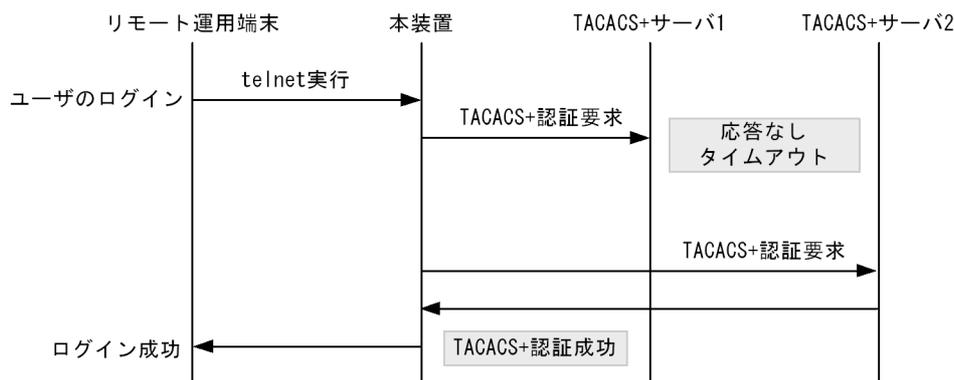
図 8-14 RADIUS サーバ選択のシーケンス



この図でリモート運用端末からユーザが本装置に telnet を実行すると、RADIUS サーバ 1 に対し本装置から RADIUS 認証を要求します。RADIUS サーバ 1 と通信できなかった場合は、続いて RADIUS サーバ 2 に対して RADIUS 認証を実行します。ここで認証に成功し、ユーザは本装置へのログインに成功します。

TACACS+ サーバ選択のシーケンスを次の図に示します。

図 8-15 TACACS+ サーバ選択のシーケンス



この図でリモート運用端末からユーザが本装置に telnet を実行すると、TACACS+ サーバ 1 に対し本装置から TACACS+ 認証を要求します。TACACS+ サーバ 1 と通信できなかった場合は、続いて TACACS+ サーバ 2 に対して TACACS+ 認証を実行します。ここで認証に成功し、ユーザは本装置へのログインに成功します。

(3) RADIUS/TACACS+ サーバへの登録情報

(a) ログイン認証を使用する場合

RADIUS/TACACS+ サーバにユーザ名およびパスワードを登録します。RADIUS/TACACS+ サーバへ登録するユーザ名には次に示す 2 種類があります。

- 本装置に adduser コマンドを使用して登録済みのユーザ名
本装置に登録されたユーザ情報を使用してログイン処理を行います。
- 本装置に未登録のユーザ名
次に示す共通のユーザ情報でログイン処理を行います。
 - ユーザ ID : remote_user

- ホームディレクトリ：/usr/home/remote_user

本装置に未登録のユーザでログインした場合の注意点を示します。

- ファイルの管理
ファイルを作成した場合、すべて remote_user 管理となって、別のユーザでも、作成したファイルの読み込みおよび書き込みができます。重要なファイルは ftp など外部に保管するなど、ファイルの管理に注意してください。

(b) 装置管理者モードへの変更 (enable コマンド) 時の認証を使用する場合

装置管理者モードへの変更 (enable コマンド) 用に、次のユーザ情報を登録してください。

- ユーザ名
本装置ではユーザ名属性として、次の表に示すユーザ名をサーバに送信します。送信するユーザ名はコンフィグレーションコマンドで変更できます。対応するユーザ名をサーバに登録してください。

表 8-10 設定するユーザ名属性

コマンド名	ユーザ名	
	RADIUS 認証	TACACS+ 認証
設定なし	admin	admin
aaa authentication enable attribute-user-per-method	\$enab15\$	ログインユーザ名

- 特権レベル
特権レベルは 15 で固定です。

ただし、使用するサーバによっては、送信したユーザ名属性に関係なく特定のユーザ名 (例えば \$enab15\$) を使用する場合や、特権レベルの登録が不要な場合などがあります。詳細については、使用するサーバのマニュアルを確認してください。

8.2.4 RADIUS/TACACS+/ ローカルを使用したコマンド承認

RADIUS/TACACS+/ ローカル (コンフィグレーション) を使用したコマンド承認方法について説明します。

(1) コマンド承認の概要

RADIUS サーバ、TACACS+ サーバ、またはローカルパスワードによる認証の上ログインしたユーザに対し、使用できる運用コマンドの種類を制限することができます。これをコマンド承認と呼びます。使用できる運用コマンドは、RADIUS サーバまたは TACACS+ サーバから取得する、コマンドクラスおよびコマンドリスト、またはコンフィグレーションで設定したコマンドクラスおよびコマンドリストに従い制御を行います。また、制限した運用コマンドは、CLI の補完機能で補完候補として表示しません。なお、<option> や <Host Name> などの、<> で囲まれたパラメータ部分の値や文字列を含んだ運用コマンドを、許可するコマンドリストに指定した場合は、<> 部分は補完候補として表示しません。

図 8-16 RADIUS/TACACS+ サーバによるログイン認証，コマンド承認

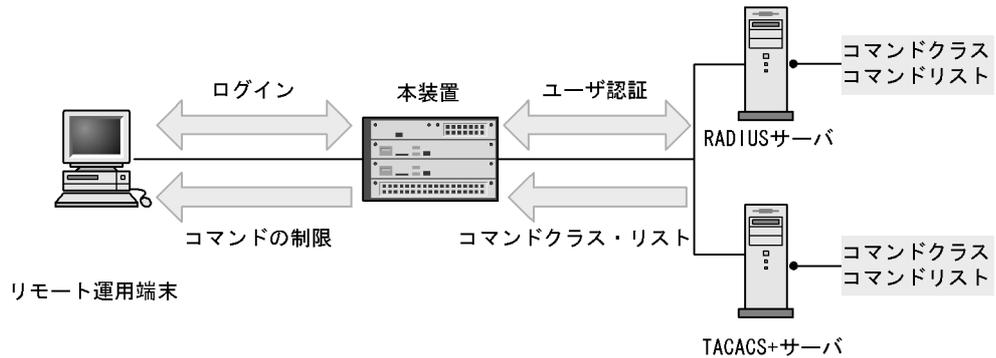
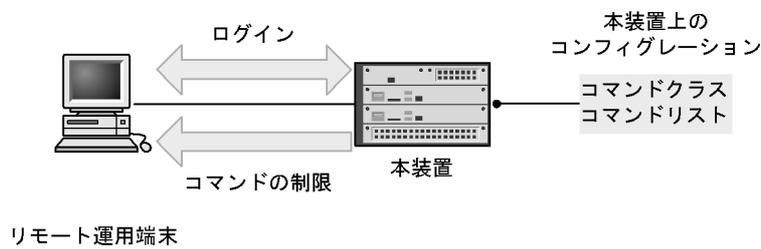


図 8-17 ローカルによるログイン認証，コマンド承認



本装置の aaa コンフィギュレーションでコマンド承認を設定すると，RADIUS/TACACS+ 指定時は，ログイン認証と同時に，サーバからコマンドリストを取得します。ローカル指定時は，ログイン認証と同時に，コンフィギュレーションで設定されたコマンドリストを使用します。本装置ではこれらのコマンドリストに従ってログイン後の運用コマンドを許可/制限します。

図 8-18 RADIUS/TACACS+ サーバによるコマンド承認のシーケンス

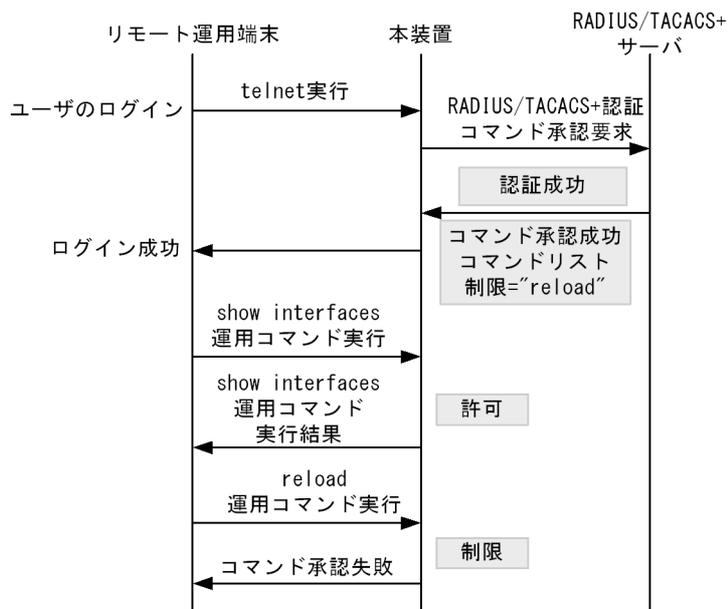
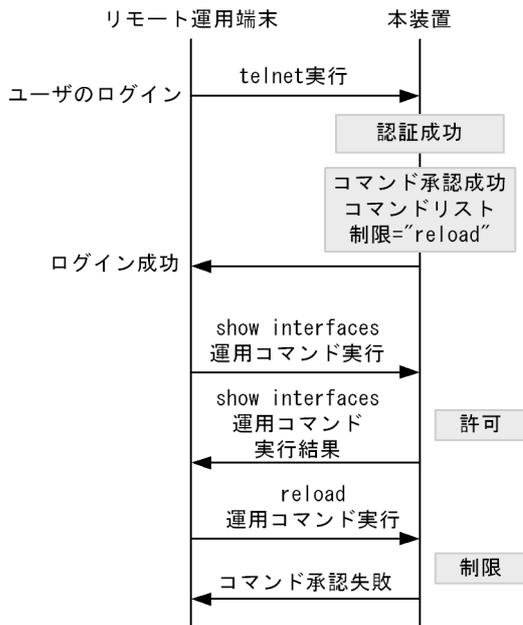


図 8-19 ローカルコマンド承認のシーケンス



「図 8-18 RADIUS/TACACS+ サーバによるコマンド承認のシーケンス」で端末からユーザが本装置に telnet を実行すると、RADIUS/TACACS+ サーバに対し本装置から認証、コマンド承認を要求します。認証成功時に RADIUS/TACACS+ サーバからコマンドリストを取得し、ユーザは本装置にログインします。

「図 8-19 ローカルコマンド承認のシーケンス」で端末からユーザが本装置に telnet を実行すると、ローカル認証を行います。認証成功時にコンフィグレーションからコマンドリストを取得し、ユーザは本装置にログインします。

ログイン後、ユーザは本装置で運用コマンド show interfaces などを実行できますが、reload 運用コマンドはコマンドリストによって制限されているため実行できません。

! 注意事項

RADIUS/TACACS+ サーバのコマンドリストの設定を変更した場合またはコンフィグレーションのコマンドリストを変更した場合は、次のログイン認証後から反映されます。

(2) RADIUS/TACACS+/ ローカルコマンド承認設定手順

RADIUS/TACACS+ によるコマンド承認を使用するためには、次の手順で RADIUS/TACACS+ サーバや本装置を設定します。

1. コマンド制限のポリシーを決める。
各ユーザに対し、運用コマンドの中で、制限・許可するコマンドのポリシーを決めます。
2. コマンドリストを指定する。
コマンドクラス以外に、許可/制限コマンドリストとして、許可コマンドと制限コマンドをそれぞれ指定できます。
3. RADIUS/TACACS+ サーバを設定する。
決定したコマンド制限ポリシーを基に、RADIUS または TACACS+ のリモート認証サーバに、コマンド制限のための設定を行います。
4. 本装置のリモート認証を設定する。

本装置で RADIUS または TACACS+ サーバのコンフィグレーション設定と aaa コンフィグレーション設定を行います。

5. コマンド承認の動作を確認する。

RADIUS/TACACS+ を使用したリモート運用端末から本装置へログインし、確認を行います。

ローカルコマンド承認を使用するためには、次の手順で本装置を設定します。

1. コマンド制限のポリシーを決める。

各ユーザに対し、運用コマンドの中で、制限・許可するコマンドのポリシーを決めます。

2. コマンドリストを作成する。

コマンドクラス以外に、コマンドリストとして許可コマンドと制限コマンドをそれぞれ指定できます。

決定したコマンド制限ポリシーを基に、コマンドリストのコンフィグレーション設定を行います。

なお、コマンドクラスだけを使用する場合は作成不要です。

3. ユーザにコマンドクラスまたはコマンドリストを割り当てる。

各ユーザに対し、コマンドクラスまたはコマンドリストを割り当てる username コンフィグレーション設定を行います。

その後、aaa コンフィグレーション設定を行います。

4. コマンド承認の動作を確認する。

本装置へローカル認証でログインし確認を行います。

(3) コマンド制限のポリシー決定

各ユーザに対し、運用コマンドの中で、制限・許可するコマンドのポリシーを決めます。ここでは、各ユーザがログインしたときに、あるコマンド群は許可し、それ以外のコマンドは制限するなどを決めます。ポリシーは、「(5) RADIUS/TACACS+/ ローカルコマンド承認の設定」で設定します。

コマンド制限・許可の対象となるのは、運用コマンドです。マニュアル未掲載のデバッグコマンド (ps コマンドなど) は対象外で、常に制限されます (許可が必要な場合は、次に説明するコマンドクラスで root を指定してコマンド無制限クラスとしてください)。なお、logout, exit, quit, disable, end, set terminal, show whoami, who am i コマンドに関しては常に許可されます。

本装置には、あらかじめ「コマンドクラス」として、次に示すポリシーが定義されています。規定のコマンドクラスを選択することで、そのクラスの応じたコマンド制限を行うことができます。

表 8-11 コマンドクラス一覧

コマンドクラス	許可コマンド	制限コマンド
root 全コマンド無制限クラス	従来どおりすべてのコマンド (マニュアル未掲載のデバッグコマンドを含む)	なし
allcommand 運用コマンド無制限クラス	すべての運用コマンド "all"	なし (マニュアル未掲載のデバッグコマンドは不可)
noconfig コンフィグレーション変更制限クラス (コンフィグレーションコマンド指定も制限します)	制限以外の運用コマンド	"config, copy, erase configuration"
nomanage ユーザ管理コマンド制限クラス	制限以外の運用コマンド	"adduser, rmuser, clear password, password, killuser"
noenable 装置管理者モードコマンド制限クラス	制限以外の運用コマンド	"enable"

また、コマンドクラス以外に、許可コマンドリストと制限コマンドリストをそれぞれ指定することもできます。

(4) コマンドリストの指定方法について

コマンドクラス以外に、許可/制限コマンドリストとして、許可コマンドと制限コマンドをそれぞれ指定できます。コマンドを指定する場合は、各コマンドリストに設定対象のコマンド文字列をスペースも意識して指定します。複数指定する場合はコンマ(,)で区切って並べます。なお、ローカルコマンド承認では、コマンド文字列をコンフィグレーションコマンド `commands exec` で一つずつ設定します。本装置では、その設定されたコマンド文字列をコンマ(,)で連結したものをコマンドリストとして使用します。

コマンドリストで指定されたコマンド文字列と、ユーザが入力したコマンドの先頭部分とが、合致するかどうかを判定します(前方一致)。なお、特別な文字列として、`all` を指定できます。`all` は運用コマンドすべてを意味します。

判定時に、許可コマンドリストと制限コマンドリストの両方に合致した場合は、合致したコマンド文字数が多い方の動作を採用します(ただし、`all` 指定は文字数を 1 とします)。その際、許可コマンドリストと制限コマンドリストに同じコマンド文字列が指定されていた場合は、許可として判定されます。

また、コマンドクラスと許可/制限コマンドリストを同時に指定した場合は、コマンドクラスごとに規定されているコマンドリスト(「表 8-11 コマンドクラス一覧」中の" "で囲まれているコマンドリストに対応)と許可/制限コマンドリストを合わせて判定を行います。なお、コマンドクラスに `root` を指定した場合、許可/制限コマンドクラスの設定は無効となり、マニュアル未掲載のデバッグコマンド(`ps` コマンドなど)を含むすべてのコマンドが実行できるようになります。

例 1 ~ 7 にある各コマンドリストを設定した場合、本装置でどのようなコマンドが許可/制限されるかを示します。

(例 1)

許可コマンドリストだけを設定した場合、設定されたコマンドだけが実行を許可されます。

表 8-12 コマンドリスト例 1

コマンドリスト	指定コマンド	判定
許可コマンドリスト="show ,ping" 制限コマンドリスト 設定なし	show ip arp	許可
	ping ipv6 ::1	許可
	reload	制限

(例 2)

許可コマンドリストと制限コマンドリストの両方に合致した場合は、合致したコマンド文字数が多い方の動作とします(ただし、`all` 指定は文字数 1 とします)。

表 8-13 コマンドリスト例 2

コマンドリスト	指定コマンド	判定
許可コマンドリスト="show ,ping ipv6" 制限コマンドリスト="show ip,ping"	show system	許可
	show ipv6 neighbors	制限
	ping ipv6 ::1	許可
	ping 10.10.10.10	制限

(例 3)

許可コマンドリストと制限コマンドリストの両方を設定し、両方に合致しない場合は、許可として判

定されます。

表 8-14 コマンドリスト例 3

コマンドリスト	指定コマンド	判定
許可コマンドリスト ="show" 制限コマンドリスト ="reload"	ping 10.10.10.10	許可
	reload	制限

(例 4)

許可コマンドリストと制限コマンドリストに同じコマンド文字列が指定されている場合は、許可として判定されます。

表 8-15 コマンドリスト例 4

コマンドリスト	指定コマンド	判定
許可コマンドリスト ="show" 制限コマンドリスト ="show,ping"	show system	許可
	ping ipv6 ::1	制限

(例 5)

コマンドリストをまったく設定しなかった場合は、logout などのコマンド以外はすべて制限されます。

表 8-16 コマンドリスト例 5

コマンドリスト	指定コマンド	判定
許可コマンドリスト 設定なし 制限コマンドリスト 設定なし	すべて	制限
	logout , exit , quit , disable , end , set terminal , show whoami , who am i	許可

(例 6)

クラスとして root を指定した場合は、従来どおりすべてのコマンドが実行可能となります。なお、コマンドクラスに root を指定した場合、許可 / 制限コマンドクラスの制限は無効となり、マニュアル未掲載のデバッグコマンド (ps コマンドなど) を含むすべてのコマンドが実行可能となります。

表 8-17 コマンドリスト例 6

コマンドリスト	指定コマンド	判定
コマンドクラス ="root"	すべて (マニュアル未掲載のデバッグコマンドを含む)	許可

(例 7)

制限コマンドリストだけを設定した場合は、リストに合致しない運用コマンドはすべて許可となります。

表 8-18 コマンドリスト例 7

コマンドリスト	指定コマンド	判定
許可コマンドリスト 設定なし 制限コマンドリスト = "reload"	reload 以外の運用コマンドすべて	許可
	reload	制限

本マニュアルでは、例として次表のようなポリシーでコマンド制限を行います。

表 8-19 コマンド制限のポリシー例

ユーザ名	コマンドクラス	許可コマンド	制限コマンド
staff	allcommand	運用コマンドすべて	なし
guest	なし	制限以外の運用コマンドすべて許可	reload ... inactivate ... enable ...
test	なし	show ip ... (show ipv6 ... は制限)	許可以外、すべて制限

注 ...は任意のパラメータを意味します (show ip ...は show ip arp など)。

(5) RADIUS/TACACS+/ ローカルコマンド承認の設定

「表 8-19 コマンド制限のポリシー例」で決定したコマンド制限ポリシーを基に、RADIUS または TACACS+ のリモート認証サーバでは、通常のログイン認証の設定以外に、以下の属性値を使用したコマンド制限のための設定を行います。

なお、サーバ側でコマンド承認の設定を行っていない場合、ユーザが認証されログインできても logout, exit, quit, disable, end, set terminal, show whoami, who am i 以外のすべてのコマンドが制限され、コマンドを実行できなくなりますのでご注意ください。その場合は、コンソールからログインしてください。

また、コンフィグレーションコマンド aaa authorization commands console によってコンソールもコマンド承認の対象となっている場合は、デフォルトリスタート後、ログインしてください。

RADIUS サーバを使用する場合

RADIUS サーバを利用してコマンド制限する場合は、認証時に以下のような属性を返すようにサーバで設定します。

表 8-20 RADIUS 設定属性一覧

属性	ベンダー固有属性	値
25 Class	-	クラス 次の文字列のどれか一つを指定します。 root, allcommand, noconfig, nomanage, noenable
26 Vendor-Specific Vendor-Id: 21839	ALAXALA-Allow-Commands Vendor type: 101	許可コマンドリスト 許可するコマンドの前方一致文字列をコンマ(,)で区切って指定します。空白も区別します。 運用コマンドすべては "all" を指定します。 許可コマンドリストだけ設定した場合は、許可コマンドリスト以外のコマンドはすべて制限となります。 (例: ALAXALA-Allow-Commands="show ,ping ,telnet ")

属性	ベンダー固有属性	値
	ALAXALA-Deny-Commands Vendor type: 102	制限コマンドリスト 制限するコマンドの前方一致文字列をコンマ(,)で区切って指定します。空白も区別します。 運用コマンドすべては "all" を指定します。 制限コマンドリストだけ設定した場合は、制限コマンドリスト以外はすべて許可となります。 (例: ALAXALA-Deny-Commands="enable,reload,inactivate")

(凡例) - : 該当なし

RADIUS サーバには、上記のベンダー固有属性を登録 (dictionary ファイルなどに設定) してください。

図 8-20 RADIUS サーバでのベンダー固有属性の dictionary ファイル登録例

```
VENDOR          ALAXALA          21839
ATTRIBUTE       ALAXALA-Allow-Commands 101    string  ALAXALA
ATTRIBUTE       ALAXALA-Deny-Commands  102    string  ALAXALA
```

「表 8-19 コマンド制限のポリシー例」で決定したポリシーを一般的な RADIUS サーバに設定する場合、以下のような設定例になります。

図 8-21 RADIUS サーバ設定例

```
staff Password = "*****"
      Class = "allcommand" ... 1

guest Password = "*****"
      Alaxala-Deny-Commands = "enable,reload,inactivate" ... 2

test Password = "*****"
      Alaxala-Allow-Commands = "show ip " ... 3
```

注 ***** の部分には各ユーザのパスワードを設定します。

1. クラス "allcommand" で運用コマンドすべてを許可します。
2. enable , reload , および inactivate で始まるコマンドを制限します。
allow-commands が指定されていないため、ほかのコマンドは許可となります。
3. 空白の有無が意味を持ちます。
"show ip" の後ろに空白があるため、show ip arp などのコマンドは許可されますが、show ipv6 neighbors などのコマンドは許可されません。
ほかのコマンドはすべて制限となります。

注意

- 本装置では Class エントリを複数受信した場合、1 個目の Class を認識し 2 個目以降の Class エントリは無効となります。

図 8-22 複数 Class エントリ設定例

```
Class = "noenable" ... 1
Class = "allcommand"
```

1. 本装置では一つ目の noenable だけ有効となります。

- 本装置では Class エントリに複数のクラス名を記述した場合、1 個目のクラス名を認識し 2 個目以降のクラス名は無効となります。例えば、class="nomanage,noenable" と記述した場合、nomanage だけが有効になります。
- ALAXALA-Deny-Commands, ALAXALA-Allow-Commands のそれぞれにおいて、同一属性のエントリを複数受信した場合、一つの属性につきコンマ(,)と空白も含み 1024 文字までを認識し、1025 文字以降は受信しても無効となります。なお、下記の例のように同一属性を複数エントリ記述し、本装置で 2 個目以降のエントリを受信した場合にはエントリ先頭に自動的にコンマ(,)を設定します。

図 8-23 複数 Deny-Commands エントリ設定例

```
ALAXALA-Deny-Commands = "inactivate,reload"           ... 1
ALAXALA-Deny-Commands = "activate,test,....."         ... 1
```

1. 本装置では下線の部分を合計 1024 文字まで認識します。

上記の Deny-Commands を受信した場合は、下記のように 2 個目のエントリ先頭である activate コマンドの前にコンマ(,)が自動的に設定されます。

```
Deny-Commands = "inactivate,reload,activate,test,....."
```

TACACS+ サーバを使用する場合

TACACS+ サーバを使用してコマンド制限をする場合は、TACACS+ サーバで承認の設定として以下のような属性 - 値のペアを設定します。

表 8-21 TACACS+ 設定属性一覧

service	属性	値
taclogin	class	コマンドクラス 次の文字列のどれかを指定 root, allcommand, noconfig, nomanage, noenable
	allow-commands	許可コマンドリスト 許可するコマンドの前方一致文字列をコンマ(,)で区切って指定します。空白も区別します。 運用コマンドすべては "all" を指定します。 許可コマンドリストだけ設定した場合は、許可コマンドリスト以外のコマンドはすべて制限となります。 (例: allow-commands="show ,ping ,telnet ")
	deny-commands	制限コマンドリスト 制限するコマンドの前方一致文字列をコンマ(,)で区切って指定します。空白も区別します。 運用コマンドすべては "all" を指定します。制限コマンドリストだけ設定した場合は、制限コマンドリスト以外はすべて許可となります。 (例: deny-commands="enable,reload,inactivate")

「表 8-19 コマンド制限のポリシー例」で決定したポリシーを一般的な TACACS+ サーバに設定する場合、以下のような設定ファイルイメージになります。

図 8-24 TACACS+ サーバの設定例

```

user=staff {
  login = cleartext "*****"
  service = taclogin {
    class = "allcommand"
  }
}

user=guest {
  login = cleartext "*****"
  service = taclogin {
    deny-commands = "enable,reload,inactivate"
  }
}

user=test {
  login = cleartext "*****"
  service = taclogin {
    allow-commands = "show ip "
  }
}

```

注 ***** の部分には各ユーザのパスワードを設定します。

1. service 名は taclogin と設定します。
クラス "allcommand" で運用コマンドすべてを許可します。
2. enable, reload, および inactivate で始まるコマンドを制限します。
allow-commands が指定されていないため、ほかのコマンドは許可となります。
3. 空白の有無が意味を持ちます。
"show ip" の後ろに空白があるため、show ip arp などのコマンドは許可されますが、show ipv6 neighbors などのコマンドは許可されません。
ほかのコマンドはすべて制限となります。

注意

- 本装置では class エントリに複数のクラス名を記述した場合、1 個目のクラス名を認識し 2 個目以降のクラス名は無効となります。例えば class="nomanage,noenable" と記述した場合、nomanage だけが有効になります。
- deny-commands, allow-commands のそれぞれにおいて、一つの属性につきコンマ(,)と空白も含み 1024 文字までを認識し、1025 文字以降は受信しても無効となります。

ローカルコマンド承認を使用する場合

「表 8-19 コマンド制限のポリシー例」で決定したポリシーをローカルコマンド承認で設定する場合、次のようなコンフィグレーションの設定になります。

図 8-25 コンフィグレーションの設定例

```

username guest view guest_view
username staff view-class allcommand          ... 1
username test view test_view
!
parser view guest_view
  commands exec exclude all "enable"          ... 2
  commands exec exclude all "inactivate"      ... 2
  commands exec exclude all "reload"         ... 2
!
parser view test_view
  commands exec include all "show ip "        ... 3
!
aaa authentication login default local
aaa authorization commands default local

```

1. ユーザ "staff" に対し、クラス "allcommand" で運用コマンドすべてを許可します。
2. enable , inactivate , および reload で始まるコマンドを制限します。
 commands exec include が指定されていないため、ほかのコマンドは許可となります。
3. 空白の有無が意味を持ちます。
 "show ip " の後ろに空白があるため、show ip arp などのコマンドは許可されますが、show ipv6 neighbors などのコマンドは許可されません。
 ほかのコマンドはすべて制限となります。

(a) ログインしての確認

設定が完了した後、RADIUS/TACACS+ ローカルを使用したりリモート運用端末から本装置へのログインを行います。ログイン後、show whoami コマンドでコマンドリストが設定されていること、コマンドを実行して制限・許可していることを確認してください。

図 8-26 staff がログイン後の確認例

```

> show whoami
Date 2009/01/07 12:00:00 UTC
staff ttyp0 ----- 2 Jan 6 14:17 (10.10.10.10)

Home-directory: /usr/home/staff
Authentication: TACACS+ (Server 192.168.10.1)
Class: allcommand
  Allow: "all"
  Deny : -----
Command-list: -----
>
> show clock
Wed Jan 7 12:00:10 UTC 2009
> /bin/date
% Command not authorized.
>

```

図 8-27 guest がログイン後の確認例

```

>show whoami
Date 2009/01/07 12:00:00 UTC
guest ttyp0 ----- 2 Jan 6 14:17 (10.10.10.20)

Home-directory: /usr/home/guest
Authentication: RADIUS (Server 192.168.10.1)
Class: -----
Command-list:
    Allow: -----
    Deny : "enable,reload,inactivate"
>
> show clock
Wed Jan 7 12:00:10 UTC 2009
> reload
% Command not authorized.
>

```

図 8-28 test がログイン後の確認例

```

>show whoami
Date 2009/01/07 12:00:00 UTC
test ttyp0 ----- 2 Jan 6 14:17 (10.10.10.30)

Home-directory: /usr/home/test
Authentication: LOCAL
Class: -----
Command-list:
    Allow: "show ip "
    Deny : -----
>
> show ip arp
***コマンド実行されます***
> show ipv6 neighbors
% Command not authorized.
>

```

8.2.5 RADIUS/TACACS+ を使用したアカウントिंग

RADIUS/TACACS+ を使用したアカウントिंग方法について説明します。

(1) アカウントिंगの指定

本装置の RADIUS/TACACS+ コンフィグレーションと aaa accounting コンフィグレーションのアカウントिंगを設定すると、運用端末から本装置へのログイン・ログアウト時に RADIUS または TACACS+ サーバへアカウントング情報を送信します。また、本装置へのコマンド入力時に TACACS+ サーバへアカウントング情報を送信します。

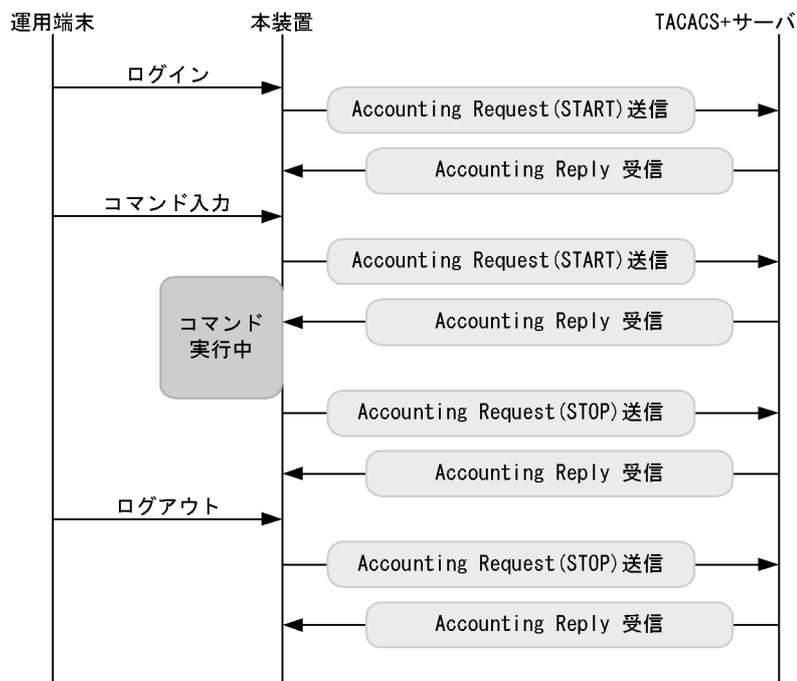
アカウントングの設定は、ログインとログアウトのイベントを送信するログインアカウントング指定と、コマンド入力のイベントを送信するコマンドアカウントング指定があります。コマンドアカウントングは TACACS+ だけでサポートしています。

それぞれのアカウントングに対して、アカウントング START と STOP を両方送信するモード (start-stop) と STOP だけを送信するモード (stop-only) を選択できます。さらに、コマンドアカウントングに対しては、入力したコマンドをすべて送信するモードとコンフィグレーションだけを送信するモードを選択できます。また、設定された各 RADIUS/TACACS+ サーバに対して、通常はどこかのサーバでアカウントングが成功するまで順に送信しますが、成功したかどうかにかかわらずすべてのサーバへ順に送信するモード (broadcast) も選択できます。

(2) アカウンティングの流れ

ログインアカウンティングとコマンドアカウンティングの両方を START-STOP 送信モードで TACACS+ サーバへ送信する設定をした場合のシーケンスを次の図に示します。

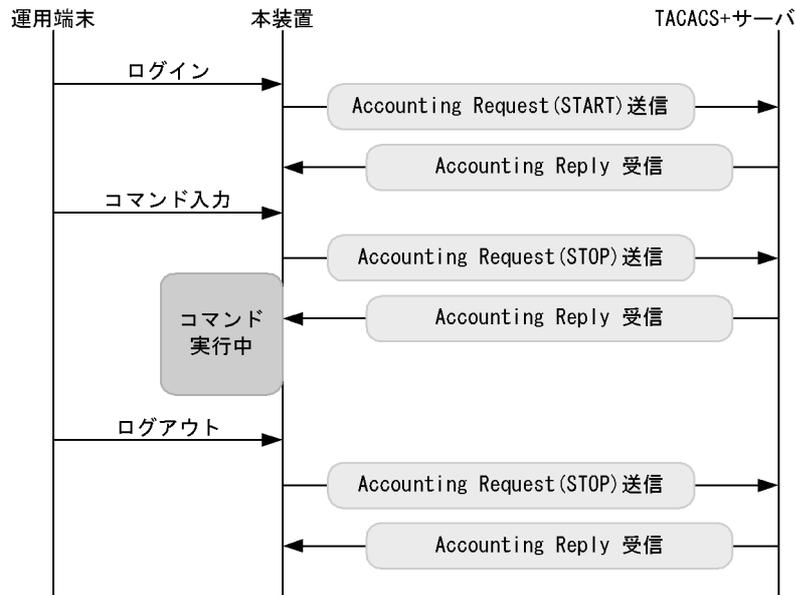
図 8-29 TACACS+ アカウンティングのシーケンス (ログイン・コマンドアカウンティングの START-STOP 送信モード時)



この図で運用端末から本装置にログインが成功すると、本装置から TACACS+ サーバに対しユーザ情報や時刻などのアカウンティング情報を送信します。また、コマンドの入力前後にも本装置から TACACS+ サーバに対し入力したコマンド情報などのアカウンティング情報を送信します。最後に、ログアウト時には、ログインしていた時間などの情報を送信します。

ログインアカウンティングは START-STOP 送信モードのまま、コマンドアカウンティングだけを STOP-ONLY 送信モードして TACACS+ サーバへ送信する設定をした場合のシーケンスを次の図に示します。

図 8-30 TACACS+ アカウンティングのシーケンス (ログインアカウンティング START-STOP, コマンドアカウンティング STOP-ONLY 送信モード時)



「図 8-29 TACACS+ アカウンティングのシーケンス (ログイン・コマンドアカウンティングの START-STOP 送信モード時)」の例と比べると、ログイン・ログアウトでのアカウンティング動作は同じですが、コマンドアカウンティングで STOP-ONLY を指定している場合、コマンドの入力前にだけ本装置から TACACS+ サーバに対し入力したコマンド情報などのアカウンティング情報を送信します。

(3) アカウンティングの注意事項

RADIUS/TACACS+ コンフィグレーション, aaa accounting コンフィグレーションのアカウンティングの設定や interface loopback コンフィグレーションで IPv4 装置アドレスを変更した場合は、送受信途中や未送信のアカウンティングイベントと統計情報はクリアされ、新しい設定で動作します。

多数のユーザが、コマンドを連続して入力したり、ログイン・ログアウトを繰り返したりした場合、アカウンティングイベントが大量に発生するため、一部のイベントでアカウンティングできないことがあります。

アカウンティングイベントの大量な発生による本装置・サーバ・ネットワークへの負担を避けるためにも、コマンドアカウンティングは STOP-ONLY で設定することをお勧めします。また、正常に通信できない RADIUS/TACACS+ サーバは指定しないでください。

運用コマンド clear accounting でアカウンティング統計情報をクリアする場合、clear accounting コマンドの入力時点で各サーバへの送受信途中のアカウンティングイベントがあるときは、そのイベントの送受信終了後に、各サーバへの送受信統計のカウンタを開始します。

DNS サーバを使用してホスト名を解決する場合、DNS サーバとの通信に時間が掛かることがあります。このため、RADIUS サーバおよび TACACS+ サーバは IP アドレスで指定することをお勧めします。

8.2.6 RADIUS/TACACS+ との接続

(1) RADIUS サーバとの接続

(a) RADIUS サーバでの本装置の識別

RADIUS プロトコルでは NAS を識別するキーとして、要求パケットの発信元 IP アドレスを使用するように規定されています。本装置では要求パケットの発信元 IP アドレスに次に示すアドレスを使用します。

- コンフィグレーションコマンド `interface loopback 0` のローカルアドレスが設定されている場合は、ローカルアドレスを発信元 IP アドレスとして使用します。
- ローカルアドレスが設定されていない場合は、送信インタフェースの IP アドレスを使用します。

このため、ローカルアドレスが設定されている場合は、RADIUS サーバに本装置を登録するためにローカルアドレスで指定した IP アドレスを使用する必要があります。これによって、RADIUS サーバと通信するインタフェースが特定できない場合は、ローカルアドレスを設定することで RADIUS サーバを確実に識別できる本装置の情報を登録できるようになります。

(b) RADIUS サーバのメッセージ

RADIUS サーバは応答に Reply-Message 属性を添付して要求元にメッセージを送付する場合があります。本装置では、RADIUS サーバからの Reply-Message 属性の内容を運用ログに出力します。RADIUS サーバとの認証に失敗する場合は、運用ログを参照してください。

(c) RADIUS サーバのポート番号

RADIUS の認証サービスのポート番号は、RFC2865 で 1812 と規定されています。本装置では特に指定しないかぎり、RADIUS サーバへの要求に 1812 のポート番号を使用します。しかし、一部の RADIUS サーバで 1812 ではなく初期の実装時に使用されていた 1645 のポート番号を使用している場合があります。このときはコンフィグレーション `radius-server host` の `auth-port` パラメータで 1645 を指定してください。なお、`auth-port` パラメータでは 1 ~ 65535 の任意の値が指定できますので、RADIUS サーバが任意のポート番号で待ち受けできる場合にも対応できます。

(2) TACACS+ サーバとの接続

(a) TACACS+ サーバの設定

- 本装置と TACACS+ サーバを接続する場合は、Service と属性名などに注意してください。TACACS+ サーバの属性については、「8.2.4 RADIUS/TACACS+/ ローカルを使用したコマンド承認」を参照してください。
- コンフィグレーションコマンド `interface loopback 0` のローカルアドレスが設定されている場合は、ローカルアドレスを発信元 IP アドレスとして使用します。

8.3 RADIUS/TACACS+ のコンフィグレーション

8.3.1 コンフィグレーションコマンド一覧

RADIUS/TACACS+, アカウンティングに関するコンフィグレーションコマンド一覧を次の表に示します。

表 8-22 コンフィグレーションコマンド一覧 (RADIUS)

コマンド名	説明
radius-server host	認証, 承認, アカウンティングに使用する RADIUS サーバを設定します。
radius-server key	認証, 承認, アカウンティングに使用する RADIUS サーバ鍵を設定します。
radius-server retransmit	認証, 承認, アカウンティングに使用する RADIUS サーバへの再送回数を設定します。
radius-server timeout	認証, 承認, アカウンティングに使用する RADIUS サーバの応答タイムアウト値を設定します。

表 8-23 コンフィグレーションコマンド一覧 (TACACS+)

コマンド名	説明
tacacs-server host	認証, 承認, アカウンティングに使用する TACACS+ サーバを設定します。
tacacs-server key	認証, 承認, アカウンティングに使用する TACACS+ サーバの共有秘密鍵を設定します。
tacacs-server timeout	認証, 承認, アカウンティングに使用する TACACS+ サーバの応答タイムアウト値を設定します。

表 8-24 コンフィグレーションコマンド一覧 (アカウンティング)

コマンド名	説明
aaa accounting commands	コマンドアカウンティングを行うときに設定します。
aaa accounting exec	ログイン・ログアウトアカウンティングを行うときに設定します。

8.3.2 RADIUS サーバによる認証の設定

(1) ログイン認証の設定例

[設定のポイント]

RADIUS サーバ, およびローカル認証を行う設定例を示します。RADIUS サーバとの通信不可などの異常によって認証に失敗した場合だけローカル認証を行うように設定します。なお, 否認によって認証に失敗した場合には, その時点で一連の認証を終了し, ローカル認証を行いません。あらかじめ, 通常のリモートアクセスに必要な設定を行っておく必要があります。

[コマンドによる設定]

1. (config)# aaa authentication login default group radius local
ログイン時に使用する認証方式を RADIUS 認証, ローカル認証の順に設定します。
2. (config)# aaa authentication login end-by-reject
RADIUS 認証で否認された場合には, その時点で一連の認証を終了し, ローカル認証を行わないよう

に設定します。

3. (config)# radius-server host 192.168.10.1 key "039fk11f84kxm3"
RADIUS 認証に使用するサーバ 192.168.10.1 の IP アドレスと共有鍵を設定します。

(2) 装置管理者モードへの変更 (enable コマンド) 時の認証の設定例

[設定のポイント]

RADIUS サーバ、およびローカル認証を行う設定例を示します。RADIUS サーバとの通信不可などの異常によって認証に失敗した場合だけローカル認証を行うように設定します。なお、否認によって認証に失敗した場合には、その時点で一連の認証を終了し、ローカル認証を行いません。また、RADIUS 認証時のユーザ名属性として \$enab15\$ を送信するように設定します。

[コマンドによる設定]

1. (config)# aaa authentication enable default group radius enable
装置管理者モードへの変更 (enable コマンド) 時に使用する認証方式を RADIUS 認証、ローカル認証の順に設定します。
2. (config)# aaa authentication enable end-by-reject
RADIUS 認証で否認された場合には、その時点で一連の認証を終了し、ローカル認証を行わないように設定します。
3. (config)# aaa authentication enable attribute-user-per-method
RADIUS 認証時のユーザ名属性として \$enab15\$ を送信するように設定します。
4. (config)# radius-server host 192.168.10.1 key "039fk11f84kxm3"
RADIUS 認証に使用するサーバ 192.168.10.1 の IP アドレスと共有鍵を設定します。

8.3.3 TACACS+ サーバによる認証の設定

(1) ログイン認証の設定例

[設定のポイント]

TACACS+ サーバおよびローカル認証を行う設定例を示します。TACACS+ サーバとの通信不可などの異常によって認証に失敗した場合だけローカル認証を行うように設定します。なお、否認によって認証に失敗した場合には、その時点で一連の認証を終了し、ローカル認証を行いません。あらかじめ、通常のリモートアクセスに必要な設定を行っておく必要があります。

[コマンドによる設定]

1. (config)# aaa authentication login default group tacacs+ local
ログイン時に使用する認証方式を TACACS+ 認証、ローカル認証の順に設定します。
2. (config)# aaa authentication login end-by-reject
TACACS+ 認証で否認された場合には、その時点で一連の認証を終了し、ローカル認証を行わないように設定します。
3. (config)# tacacs-server host 192.168.10.1 key "4h8dlir9r-w2"

TACACS+ 認証に使用するサーバ 192.168.10.1 の IP アドレスと共有鍵を設定します。

(2) 装置管理者モードへの変更 (enable コマンド) 時の認証の設定例

[設定のポイント]

TACACS+ サーバおよびローカル認証を行う設定例を示します。TACACS+ サーバとの通信不可などの異常によって認証に失敗した場合だけローカル認証を行うように設定します。なお、否認によって認証に失敗した場合には、その時点で一連の認証を終了し、ローカル認証を行いません。また、TACACS+ 認証時のユーザ名属性としてログインユーザ名を送信するように設定します。

[コマンドによる設定]

1. (config)# aaa authentication enable default group tacacs+ enable
装置管理者モードへの変更 (enable コマンド) 時に使用する認証方式を TACACS+ 認証、ローカル認証の順に設定します。
2. (config)# aaa authentication enable end-by-reject
TACACS+ 認証で否認された場合には、その時点で一連の認証を終了し、ローカル認証を行わないように設定します。
3. (config)# aaa authentication enable attribute-user-per-method
TACACS+ 認証時のユーザ名属性としてログインユーザ名を送信するように設定します。
4. (config)# tacacs-server host 192.168.10.1 key "4h8dlir9r-w2"
TACACS+ 認証に使用するサーバ 192.168.10.1 の IP アドレスと共有鍵を設定します。

8.3.4 RADIUS/TACACS+/ ローカルによるコマンド承認の設定

(1) RADIUS サーバによるコマンド承認の設定例

[設定のポイント]

RADIUS サーバによるコマンド承認を行う設定例を示します。
あらかじめ、RADIUS 認証を使用する設定を行ってください。

[コマンドによる設定]

1. (config)# aaa authentication login default group radius local
(config)# radius-server host 192.168.10.1 key "RaD#001"
あらかじめ、RADIUS サーバによる認証の設定を行います。
2. (config)# aaa authorization commands default group radius
RADIUS サーバを使用して、コマンド承認を行います。

[注意事項]

本設定後にユーザが RADIUS 認証されてログインしたとき、RADIUS サーバ側でコマンド承認の設定がされていなかった場合は、コマンドがすべて制限されて実行できなくなります。設定ミスなどでコマンドの実行ができない場合は、コンソールからログインして修正してください。なお、コンフィグレーションコマンド aaa authorization commands console によってコンソールもコマンド承認の対

象となっている場合は、デフォルトリスタート後、ログインして修正してください。

(2) TACACS+ サーバによるコマンド承認の設定例

[設定のポイント]

TACACS+ サーバによるコマンド承認を行う設定例を示します。

あらかじめ、TACACS+ 認証を使用する設定を行ってください。

[コマンドによる設定]

1. (config)# aaa authentication login default group tacacs+ local

(config)# tacacs-server host 192.168.10.1 key "TaC#001"

あらかじめ、TACACS+ サーバによる認証の設定を行います。

2. (config)# aaa authorization commands default group tacacs+

TACACS+ サーバを使用して、コマンド承認を行います。

[注意事項]

本設定後にユーザが TACACS+ 認証されてログインしたとき、TACACS+ サーバ側でコマンド承認の設定がされていなかった場合は、コマンドがすべて制限されて実行できなくなります。設定ミスなどでコマンドの実行ができない場合は、コンソールからログインして修正してください。なお、コンフィグレーションコマンド aaa authorization commands console によってコンソールもコマンド承認の対象となっている場合は、デフォルトリスタート後、ログインして修正してください。

(3) ローカルコマンド承認の設定例

[設定のポイント]

ローカルコマンド承認を行う設定例を示します。

あらかじめ、ユーザ名とそれに対応したコマンドクラス (username view-class) またはコマンドリスト (username view · parser view · commands exec) の設定を行ってください。

また、ローカルパスワード認証を使用する設定を行ってください。

[コマンドによる設定]

1. (config)# parser view Local_001

(config-view)# commands exec include all "show"

(config-view)# commands exec exclude all "reload"

コマンドリストを使用する場合は、あらかじめコマンドリストの設定を行います。

なお、コマンドクラスだけを使用する場合は、コマンドリストの設定は必要ありません。

2. (config)# username user001 view Local_001

(config)# username user001 view-class noenable

指定ユーザにコマンドクラスまたはコマンドリストの設定を行います。

なお、コマンドクラスとコマンドリストを同時に設定することもできます。

3. (config)# aaa authentication login default local

ローカルパスワードによる認証の設定を行います。

4. (config)# aaa authorization commands default local

ローカル認証を使用して、コマンド承認を行います。

[注意事項]

ローカルコマンド承認を設定すると、ローカル認証でログインしたすべてのユーザに適用されますので、設定に漏れがないようご注意ください。
 コマンドクラスまたはコマンドリストの設定がされていないユーザは、コマンドがすべて制限されて実行できなくなります。
 設定誤りなどでコマンドの実行ができない場合は、コンソールからログインして修正してください。
 なお、コンフィグレーションコマンド `aaa authorization commands console` によってコンソールもコマンド承認の対象となっている場合は、デフォルトリスタート後、ログインして修正してください。

8.3.5 RADIUS/TACACS+ によるログイン・ログアウトアカウントティングの設定

(1) RADIUS サーバによるログイン・ログアウトアカウントティングの設定例

[設定のポイント]

RADIUS サーバによるログイン・ログアウトアカウントティングを行う設定例を示します。あらかじめ、アカウントティング送信先となる RADIUS サーバホスト側の設定を行ってください。

[コマンドによる設定]

1. `(config)# radius-server host 192.168.10.1 key "RaD#001"`
 あらかじめ、RADIUS サーバの設定を行います。
2. `(config)# aaa accounting exec default start-stop group radius`
 ログイン・ログアウトアカウントティングの設定を行います。

[注意事項]

`radius-server` コンフィグレーションの設定がされていない状態で `aaa accounting exec` を設定した場合、ユーザがログイン・ログアウトしたときに `System accounting failed` という運用ログが表示されます。使用する `radius-server` コンフィグレーションを設定してください。

(2) TACACS+ サーバによるログイン・ログアウトアカウントティングの設定例

[設定のポイント]

TACACS+ サーバによるログイン・ログアウトアカウントティングを行う設定例を示します。あらかじめ、アカウントティング送信先となる TACACS+ サーバホスト側の設定を行ってください。

[コマンドによる設定]

1. `(config)# tacacs-server host 192.168.10.1 key "TaC#001"`
 あらかじめ、TACACS+ サーバの設定を行います。
2. `(config)# aaa accounting exec default start-stop group tacacs+`
 ログイン・ログアウトアカウントティングの設定を行います。

[注意事項]

`tacacs-server` コンフィグレーションの設定がされていない状態で `aaa accounting exec` を設定した場合、ユーザがログイン・ログアウトしたときに `System accounting failed` という運用ログが表示されます。使用する `tacacs-server` コンフィグレーションを設定してください。

8.3.6 TACACS+ サーバによるコマンドアカウントिंगの設定

(1) TACACS+ サーバによるコマンドアカウントिंगの設定例

[設定のポイント]

TACACS+ サーバによるコマンドアカウントングを行う設定例を示します。
あらかじめ、アカウントング送信先となる TACACS+ サーバホスト側の設定を行ってください。

[コマンドによる設定]

1. (config)# tacacs-server host 192.168.10.1 key "TaC#001"
TACACS+ サーバの設定を行います。
2. (config)# aaa accounting commands 0-15 default start-stop group tacacs+
コマンドアカウントングを設定します。

[注意事項]

tacacs-server コンフィグレーションの設定がされていない状態で aaa accounting commands を設定した場合、ユーザがコマンドを入力したときに System accounting failed という運用ログが表示されます。使用する tacacs-server コンフィグレーションを設定してください。

9

時刻の設定と NTP

この章では、時刻の設定と NTP について説明します。

9.1 時刻の設定と NTP 確認

9.1 時刻の設定とNTP確認

時刻は、本装置の初期導入時に設定してください。時刻は、本装置のログ情報や各種ファイルの作成時刻などに付与される情報です。運用開始時には正確な時刻を本装置に設定してください。運用コマンド `set clock` で時刻を設定できます。

また、このほかに、NTP プロトコルを使用して、ネットワーク上の NTP サーバと時刻の同期を行えます。なお、本装置は RFC1305 NTP バージョン 3 に準拠しています。

9.1.1 コンフィグレーションコマンド・運用コマンド一覧

時刻設定および NTP に関するコンフィグレーションコマンド一覧を次の表に示します。

表 9-1 コンフィグレーションコマンド一覧

コマンド名	説明
<code>clock timezone</code>	タイムゾーンを設定します。
<code>ntp access-group</code>	アクセスグループを作成し、IPv4 アドレスフィルタによって、NTP サービスへのアクセスを許可または制限できます。
<code>ntp authenticate</code>	NTP 認証機能を有効化します。
<code>ntp authentication-key</code>	認証鍵を設定します。
<code>ntp broadcast</code>	インタフェースごとにブロードキャストで NTP パケットを送信し、ほかの装置が本装置に同期化するように設定します。
<code>ntp broadcast client</code>	接続したサブネット上の装置からの NTP ブロードキャストメッセージを受け付けるための設定をします。
<code>ntp broadcastdelay</code>	NTP ブロードキャストサーバと本装置間で予測される遅延時間を指定します。
<code>ntp master</code>	ローカルタイムサーバの設定を指定します。
<code>ntp peer</code>	NTP サーバに、シンメトリック・アクティブ/パッシブモードを構成します。
<code>ntp server</code>	NTP サーバをクライアントモードに設定し、クライアントサーバモードを構成します。
<code>ntp trusted-key</code>	ほかの装置と同期化する場合に、セキュリティ目的の認証をするように鍵番号を設定します。

時刻設定および NTP に関する運用コマンド一覧を次の表に示します。

表 9-2 運用コマンド一覧

コマンド名	説明
<code>set clock</code>	日付、時刻を表示、設定します。
<code>show clock</code>	現在設定されている日付、時刻を表示します。
<code>show ntp associations</code>	接続されている NTP サーバの動作状態を表示します。
<code>restart ntp</code>	ローカル NTP サーバを再起動します。

9.1.2 システムクロックの設定

[設定のポイント]

日本時間として時刻を設定する場合は、あらかじめコンフィグレーションコマンド `clock timezone` でタイムゾーンに JST、UTC からのオフセットを +9 に設定する必要があります。

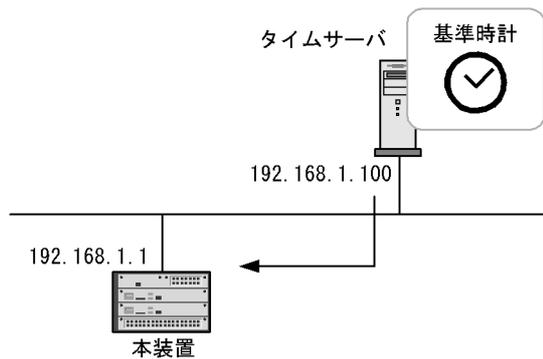
[コマンドによる設定]

1. `(config)# clock timezone JST +9`
日本時間として、タイムゾーンに JST、UTC からのオフセットを +9 に設定します。
2. `(config)# save`
`(config)# exit`
保存し、コンフィグレーションモードから装置管理者モードに移行します。
3. `# set clock 0603221530`
`Wed Mar 22 15:30:00 2006 JST`
2006 年 3 月 22 日 15 時 30 分に時刻を設定します。

9.1.3 NTP によるタイムサーバと時刻同期の設定

NTP 機能を用いて、本装置の時刻をタイムサーバの時刻に同期させます。

図 9-1 NTP 構成図 (タイムサーバへの時刻の同期)



[設定のポイント]

タイムサーバを複数設定した場合の本装置の同期先は、`ntp server` コマンドの `prefer` パラメータを指定されたタイムサーバが選択されます。また、`prefer` パラメータが指定されなかった場合は、タイムサーバの `stratum` 値が最も小さいタイムサーバが選択され、すべての `stratum` 値が同じ場合の同期先は任意となります。

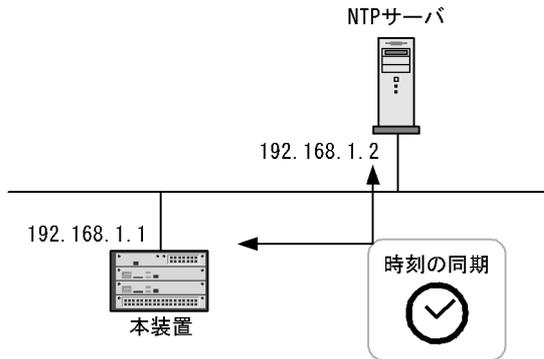
[コマンドによる設定]

1. `(config)# ntp server 192.168.1.100`
IP アドレス 192.168.1.100 のタイムサーバに本装置を同期させます。

9.1.4 NTP サーバとの時刻同期の設定

NTP 機能を用いて、本装置の時刻と NTP サーバの時刻をお互いに調整しながら、同期させます。

図 9-2 NTP 構成図 (NTP サーバとの時刻の同期)



[設定のポイント]

複数の NTP サーバと本装置を同期する場合には、ntp peer コマンドを用いて複数設定する必要があります。

NTP サーバを複数設定した場合の本装置の同期先は、ntp peer コマンドの prefer パラメータを指定された NTP サーバが選択されます。また、prefer パラメータが指定されなかった場合は、NTP サーバの stratum 値が最も小さい NTP サーバが選択され、すべての stratum 値が同じ場合の同期先は任意となります。

[コマンドによる設定]

1. (config)# ntp peer 192.168.1.2
IP アドレス 192.168.1.2 の NTP サーバとの間を peer 関係として設定します。

9.1.5 NTP 認証の設定

[設定のポイント]

NTP 機能でほかの装置と時刻の同期を行う場合に、セキュリティ目的の認証を行います。

[コマンドによる設定]

1. (config)# ntp authenticate
NTP 認証機能を有効化します。
2. (config)# ntp authentication-key 1 md5 NtP#001
NTP 認証鍵として、鍵番号 1 に「NtP#001」を設定します。
3. (config)# ntp trusted-key 1
NTP 認証に使用する鍵番号 1 を指定します。

9.1.6 VRF での NTP による時刻同期の設定【OP-NPAR】

NTP 機能を用いて、VRF に存在する NTP サーバや NTP クライアントに対して時刻を同期させる設定をします。

[設定のポイント]

NTP 機能を用いて、本装置の時刻を任意の VRF に存在する NTP サーバに同期させます。また、本

装置の時刻が NTP サーバに同期している場合、グローバルネットワークを含む全 VRF に存在する複数の NTP クライアントに本装置の時刻を配布できます。

同期の対象にする NTP サーバと NTP クライアントの VRF が異なる場合、NTP クライアントに対して、本装置の参照先ホストをローカルタイムサーバとして通知します。

[コマンドによる設定]

1. (config)# ntp server vrf 10 192.168.1.100
VRF 10 に存在する IP アドレス 192.168.1.100 の NTP サーバに、本装置の時刻を同期させます。構成はクライアントサーバモードです。
2. (config)# ntp peer vrf 10 192.168.1.100
VRF 10 に存在する IP アドレス 192.168.1.100 の NTP サーバと本装置の時刻を同期させます。構成はシメトリック・アクティブ/パッシブモードです。
3. (config)# ntp broadcast client
NTP ブロードキャストメッセージで本装置の時刻を同期させます。グローバルネットワークを含む全 VRF 上のサブネットを対象にして、NTP サーバからの NTP ブロードキャストメッセージを受信します。
4. (config)# interface vlan 100
(config-if)# vrf forwarding 20
(config-if)# ip address 192.168.10.1 255.255.255.0
(config-if)# ntp broadcast
VRF が指定されたインタフェースに対して NTP ブロードキャストの設定をします。本装置の時刻が NTP サーバに同期すると、VRF20, 192.168.10.0, サブネットマスク 255.255.255.0 のネットワークに NTP ブロードキャストパケットを送信します。

9.1.7 時刻変更に関する注意事項

- 本装置で収集している統計情報の CPU 使用率は、時刻が変更された時点で 0 にクリアされます。
- スケジューリングによる省電力機能の使用時に時刻補正した場合、補正した時間分（最大で 30 分）経過するまで、スケジュールが反映されないことがあります。【AX6700S】【AX6600S】

9.1.8 時刻の確認

本装置に設定されている時刻情報は、運用コマンド show clock で確認できます。次の図に例を示します。

図 9-3 時刻の確認

```
> show clock
Wed Mar 22 15:30:00 2006 JST
>
```

また、NTP プロトコルを使用して、ネットワーク上の NTP サーバと時刻の同期を行っている場合、運用コマンド show ntp associations で動作状態を確認できます。次の図に例を示します。

図 9-4 NTP サーバの動作状態の確認

```
> show ntp associations [Enter]キーを押す
Date 2009/01/23 12:00:00 UTC
  remote          refid          st t when poll reach  delay  offset  disp
=====
*timesvr    192.168.1.100    3 u   1  64  377    0.89  -2.827  0.27
>
```

10

ホスト名と DNS

この章では、ホスト名と DNS の解説と操作方法について説明します。

10.1 解説

10.2 コンフィグレーション

10.1 解説

本装置では、ネットワーク上の装置を識別するためにホスト名情報を設定できます。設定したホスト名情報は、本装置のログ情報などのコンフィグレーションを設定するときにネットワーク上のほかの装置を指定する名称として使用できます。本装置で使用するホスト名情報は次に示す方法で設定できます。

- コンフィグレーションコマンド `ip host / ipv6 host` で個別に指定する方法
- DNS リゾルバ機能を使用してネットワーク上の DNS サーバに問い合わせる方法

コンフィグレーションコマンド `ip host / ipv6 host` を使用して設定する場合は、使用するホスト名ごとに IP アドレスとの対応を明示的に設定する必要があります。DNS リゾルバを使用する場合は、ネットワーク上の DNS サーバで管理されている名称を問い合わせるため、本装置で参照するホスト名ごとに IP アドレスを設定する必要がなくなります。

コンフィグレーションコマンド `ip host / ipv6 host` と DNS リゾルバ機能の両方が設定されている場合、`ip host / ipv6 host` で設定されているホスト名が優先されます。コンフィグレーションコマンド `ip host / ipv6 host` または DNS リゾルバ機能を使用して、IPv4 と IPv6 で同一のホスト名を設定している場合、IPv4 が優先されます。

本装置の DNS リゾルバ機能は RFC1034 および RFC1035 に準拠しています。

10.2 コンフィグレーション

10.2.1 コンフィグレーションコマンド一覧

ホスト名・DNS に関するコンフィグレーションコマンド一覧を次の表に示します。

表 10-1 コンフィグレーションコマンド一覧

コマンド名	説明
ip domain lookup	DNS リゾルバ機能を無効化または有効化します。
ip domain name	DNS リゾルバで使用するドメイン名を設定します。
ip host	IPv4 アドレスに付与するホスト名情報を設定します。
ip name-server	DNS リゾルバが参照するネームサーバを設定します。
ipv6 host	IPv6 アドレスに付与するホスト名情報を設定します。

10.2.2 ホスト名の設定

(1) IPv4 アドレスに付与するホスト名の設定

[設定のポイント]

IPv4 アドレスに付与するホスト名を設定します。

[コマンドによる設定]

1. (config)# ip host WORKPC1 192.168.0.1

IPv4 アドレス 192.168.0.1 の装置にホスト名 WORKPC1 を設定します。

(2) IPv6 アドレスに付与するホスト名の設定

[設定のポイント]

IPv6 アドレスに付与するホスト名を設定します。

[コマンドによる設定]

1. (config)# ipv6 host WORKPC2 3ffe:501:811:ff45::87ff:fec0:3890

IPv6 アドレス 3ffe:501:811:ff45::87ff:fec0:3890 の装置にホスト名 WORKPC2 を設定します。

10.2.3 DNS の設定

(1) DNS リゾルバの設定

[設定のポイント]

DNS リゾルバで使用するドメイン名および DNS リゾルバが参照するネームサーバを設定します。

DNS リゾルバ機能はデフォルトで有効なため、ネームサーバが設定された時点から機能します。

[コマンドによる設定]

1. (config)# ip domain name router.example.com

ドメイン名を router.example.com に設定します。

2. (config)# ip nameserver 192.168.0.1
ネームサーバを 192.168.0.1 に設定します。

(2) DNS リゾルバ機能の無効化

[設定のポイント]

DNS リゾルバ機能を無効にします。

[コマンドによる設定]

1. (config)# no ip domain lookup
DNS リゾルバ機能を無効にします。

11 装置の管理

この章では，本装置を導入した際，および本装置を管理する上で必要な作業について説明します。

11.1 システム操作パネル

11.2 装置の状態確認，および運用形態に関する設定

11.3 運用情報のバックアップ・リストア

11.4 装置の温度監視

11.5 障害時の復旧

11.1 システム操作パネル

システム操作パネルはBCUボード、CSUボード、およびMSUボードに搭載されていて、装置情報の表示や動作指示、障害情報を表示できます。

システム操作パネルは、[BACK]キー（◀）、[ENTR]キー（ ）、[FWRD]キー（▶）の三つの操作キーと16桁×2行のLCDを持ちます。システム操作パネルは、装置に発生した障害情報を表示する機能のほかに、システム操作パネルのキーを操作して階層構造のメニューをたどることにより、装置情報の表示や動作指示、障害情報を表示できます。

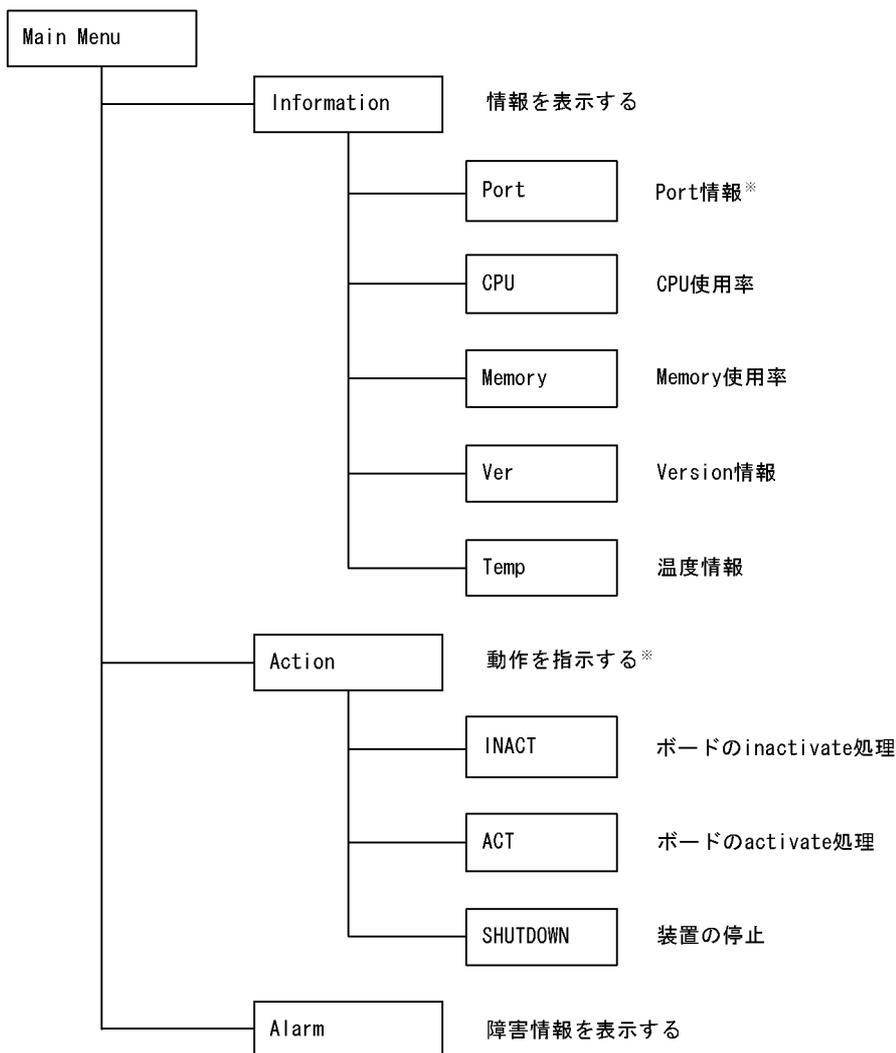
システム操作パネルの基本操作は、[BACK]キーおよび[FWRD]キーで項目を選択して、[ENTR]キーで決定します。例えば、ボードのinactivate処理をしたい場合には、<Main Menu>で「Action」を選択して[ENTR]キーを押し、続いて<ACTION>で「INACT」を選択して[ENTR]キーを押しします。

11.1.1 メニュー構造

<Main Menu> 以下のメニュー構造を次の図に示します。

メニューを操作していて、現在メニューのどの表示をしているかわからなくなった場合は、[ENTR]キーを何回か押すと<Main Menu>に戻ります。また、操作キーを操作しないで一定時間が経過しても<Main Menu>に戻ります。

図 11-1 メニュー構造



注※ 待機系BCU、待機系CSUおよび待機系MSUでは操作できません

11.1.2 Port 情報の表示

Port の情報表示では、選択した Port 番号のインタフェースの状態を表示します。

<INFORMATION> で「Port」を選択して [ENTR] キーを押すと、NIF 番号選択画面を表示します。

(1) NIF 番号選択

表示する Port の NIF 番号を選択する画面で [FWRD] キーを押していくと、選択できる NIF 番号を昇順に表示します。NIF が正常状態でない場合、その NIF 番号の表示はスキップします。[BACK] キーでは [FWRD] キーと逆の順序で NIF 番号を表示します。情報を表示したい NIF 番号を選択し、[ENTR] キーで決定すると Port 情報表示画面を表示します。

図 11-2 NIF 番号選択の表示例



(2) Port 情報表示

Port 情報表示画面では、物理インタフェースの状態を表示します。[FWRD] キーを押すと、次の Port の情報を表示します。[BACK] キーでは、逆順となります。正常な NIF が複数ある場合は、[FWRD] キーおよび [BACK] キーで NIF をまたいで Port 情報を表示することもできます。

[ENTR] キーを押すと、<Main Menu> に戻ります。

図 11-3 Port 情報の表示例



表 11-1 Port 情報の表示内容

分類	名称	意味
Port 状態	active up	運用中 (正常動作中)
	active down	運用中 (回線障害発生中)
	initialize	初期化中またはネゴシエーション確立待ち
	test	回線テスト中
	fault	障害中
	inactive	inactivate コマンドによる運用停止状態
	disable	shutdown コマンドによる運用停止状態
Port 種別	10BASE-T	
	100BASE-TX	
	1000BASE-T	
	1000BASE-SX	
	1000BASE-SX2	
	1000BASE-LX	
	1000BASE-LH	
	1000BASE-LHB	
	1000BASE-BX10-D	
	1000BASE-BX10-U	
	1000BASE-BX40-D	
	1000BASE-BX40-U	
	10GBASE-LR	
	10GBASE-ER	
	10GBASE-SR	
10GBASE-ZR		

分類	名称	意味
全二重 / 半二重	full	全二重
	half	半二重
	full (auto)	全二重 (自動認識)
	half (auto)	半二重 (自動認識)

11.1.3 CPU 使用率の表示

CPU 使用率を表示します。

<INFORMATION> で「CPU」を選択して [ENTR] キーを押すと、CPU の使用率画面を表示します。

(1) CPU 使用率

CPU 使用率を 2% 刻みの横棒グラフで表示します。表示は 1 秒ごとに最新の状況に更新します。

図 11-4 CPU 使用率の表示例



[FWRD] キーおよび [BACK] キーを押しても、表示内容は変わりません。

[ENTR] キーを押すと、<Main Menu> に戻ります。

表 11-2 CPU 使用率の表示内容

表示項目	表示内容
CPU average	CPU 使用率を 1 秒単位で集計した平均値 (%)

11.1.4 メモリ使用率の表示

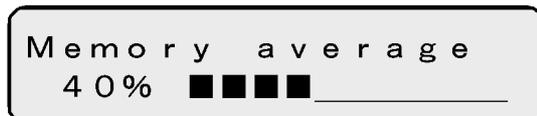
メモリ使用率を表示します。

<INFORMATION> で「Memory」を選択して [ENTR] キーを押すと、メモリの使用率画面を表示します。

(1) メモリ使用率

メモリ使用率を 2% 刻みの横棒グラフで表示します。表示は 1 秒ごとに最新の状況に更新します。

図 11-5 メモリ使用率の表示例



[FWRD] キーおよび [BACK] キーを押しても、表示内容は変わりません。

[ENTR] キーを押すと、<Main Menu> に戻ります。

表 11-3 メモリ使用率の表示内容

表示項目	表示内容
Memory average	実装メモリの使用率 (%)

11.1.5 バージョンの表示

本装置に組み込まれているソフトウェアと実装されているボードの情報を表示します。

<INFORMATION> で「Ver」を選択して [ENTR] キーを押すと、バージョン表示画面を表示します。

(1) バージョン表示

型名表示中に [ENTR] キーを押すと、シリアルナンバー表示に切り替わります。シリアルナンバー表示中に [ENTR] キーを押すと、稼働時間表示に切り替わります。稼働時間表示は、稼働時間の合計である「Runtime Total」と、Caution 状態での稼働時間の合計である「Runtime Caution」を、5 秒ごとに切り替えて表示します。[FWRD] キーまたは [BACK] キーを押すと、型名表示となり、表示対象が切り替わります。

稼働時間表示中、装置のシリアルナンバー表示中およびソフトウェアバージョン表示中は、[ENTR] キーを押すことによって <Main Menu> に戻ります。ボードの型名表示中は 3 回、装置の型名表示中、ソフトウェア型名表示中およびボードのシリアルナンバー表示中は 2 回、[ENTR] キーを押すことによって <Main Menu> メニューに戻ります。

表 11-4 バージョン表示の表示項目一覧【AX6700S】

表示対象	型名表示	シリアルナンバー表示	稼働時間表示
モデル	装置の型名	装置のシリアルナンバー	-
ソフトウェア	ソフトウェア型名	ソフトウェアバージョン	-
ボード	BCU ボードの型名	BCU ボードのシリアルナンバー	BCU ボードの稼働時間
	BSU ボードの型名	BSU ボードのシリアルナンバー	BSU ボードの稼働時間
	NIF ボードの型名	NIF ボードのシリアルナンバー	NIF ボードの稼働時間
電源機構	電源機構の型名	電源機構のシリアルナンバー	電源機構の稼働時間
ファンユニット	ファンユニットの型名	ファンユニットのシリアルナンバー	ファンユニットの稼働時間

(凡例) - : 該当なし

表 11-5 バージョン表示の表示項目一覧【AX6600S】

表示対象	型名表示	シリアルナンバー表示	稼働時間表示
モデル	装置の型名	装置のシリアルナンバー	-
ソフトウェア	ソフトウェア型名	ソフトウェアバージョン	-
ボード	CSU ボードの型名	CSU ボードのシリアルナンバー	CSU ボードの稼働時間
	NIF ボードの型名	NIF ボードのシリアルナンバー	NIF ボードの稼働時間
電源機構	電源機構の型名	電源機構のシリアルナンバー	電源機構の稼働時間
ファンユニット	ファンユニットの型名	ファンユニットのシリアルナンバー	ファンユニットの稼働時間

(凡例) - : 該当なし

表 11-6 バージョン表示の表示項目一覧【AX6300S】

表示対象	型名表示	シリアルナンバー表示	稼働時間表示
モデル	装置の型名	装置のシリアルナンバー	-
ソフトウェア	ソフトウェア型名	ソフトウェアバージョン	-
ボード	MSU ボードの型名	MSU ボードのシリアルナンバー	MSU ボードの稼働時間
	NIF ボードの型名	NIF ボードのシリアルナンバー	NIF ボードの稼働時間
電源機構	電源機構の型名	電源機構のシリアルナンバー	電源機構の稼働時間
ファンユニット	ファンユニットの型名	ファンユニットのシリアルナンバー	ファンユニットの稼働時間

(凡例) - : 該当なし

図 11-6 モデルの表示例

```
MODEL
AX-6300-S08
```

表 11-7 モデルの表示内容

表示位置	表示内容
上段	「MODEL」固定
下段	装置の型名

図 11-7 ソフトウェア型名の表示例

```
OS-SE
AX-P6300-S2
```

表 11-8 ソフトウェア型名の表示内容

表示位置	表示内容
上段	ソフトウェア略称
下段	ソフトウェア型名

注 ソフトウェア型名は、自系の情報を表示します。

図 11-8 ソフトウェアバージョンの表示例

```
OS-SE
Ver. 10.2
```

表 11-9 ソフトウェアバージョンの表示内容

表示位置	表示内容
上段	ソフトウェア略称

表示位置	表示内容
下段	ソフトウェアバージョン

注 ソフトウェアバージョンは、自系の情報を表示します。

図 11-9 ボード型名の表示例 (NIF)

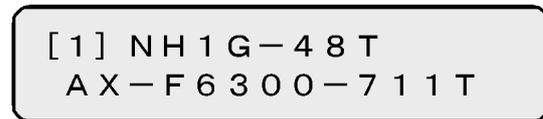


表 11-10 ボード型名の表示内容

表示位置	表示内容
上段	ボードの実装スロット番号, ボード略称
下段	ボード型名

図 11-10 シリアルナンバーの表示例



表 11-11 シリアルナンバーの表示内容

表示位置	表示内容
上段	シリアルナンバー 12 桁目まで
下段	シリアルナンバー 13 桁目以降

図 11-11 稼働時間の表示例



表 11-12 稼働時間の表示内容

表示位置	表示内容
上段	「Runtime Total」: 稼働時間の累計 「Runtime Caution」: Caution 状態での稼働時間の累計
下段	稼働時間

11.1.6 温度情報の表示

装置の温度情報を表示します。

<INFORMATION> で「Temp」を選択して [ENTR] キーを押すと、温度表示画面を表示します。

(1) 温度表示

装置代表温度を表示します。装置代表温度とは、装置内に複数ある温度測定部位のうちで、最も優先度の高い部位で測定した温度値です。

図 11-12 温度表示の表示例



[FWRD] キーおよび [BACK] キーを押しても、表示内容は変わりません。

[ENTR] キーを押すと、<Main Menu> に戻ります。

表 11-13 温度のステータス

温度のステータス	表示内容
Normal	正常
Caution	注意 (高温または低温)
Critical	警告

表 11-14 温度値とステータス変化

温度値	障害 / 回復動作
2	注意検出 (低温)
5	注意回復 (低温)
40	注意回復 (高温)
43	注意検出 (高温)
55	警告回復
58	警告検出

11.1.7 ボードの交換

電源を ON にしたまま、システム操作パネルからボードの交換を指示できます。交換できるボードは、次のとおりです。

- 待機系 BCU ボード
- BSU ボード
- 待機系 CSU ボード
- 待機系 MSU ボード
- NIF ボード

電源を ON にしたまま、各ボードを交換する手順の概略を次に示します。

1. システム操作パネルから INACT 指示を実行して、ボードを inactive 状態にする
2. 1. で inactive 状態にしたボードの取り外し
3. 交換用ボードの取り付け
4. システム操作パネルから ACT 指示を実行して、ボードを active 状態にする

ボード交換の詳細な手順については、マニュアル「ハードウェア取扱説明書」を参照してください。

(1) ボード交換の選択

ボードを inactivate する場合

<ACTION> で「INACT」を選択して [ENTR] キーを押すと、inactivate するボードの選択画面を表示します。

ボードを activate する場合

<ACTION> で「ACT」を選択して [ENTR] キーを押すと、activate するボードの選択画面を表示します。

(2) ほかの情報表示の抑制

ボードの交換の動作指示を行っている間は、障害情報は表示しません。

(3) inactivate の操作

図 11-13 inactivate の操作手順【AX6700S】

<ACTION>で「INACT」を選択

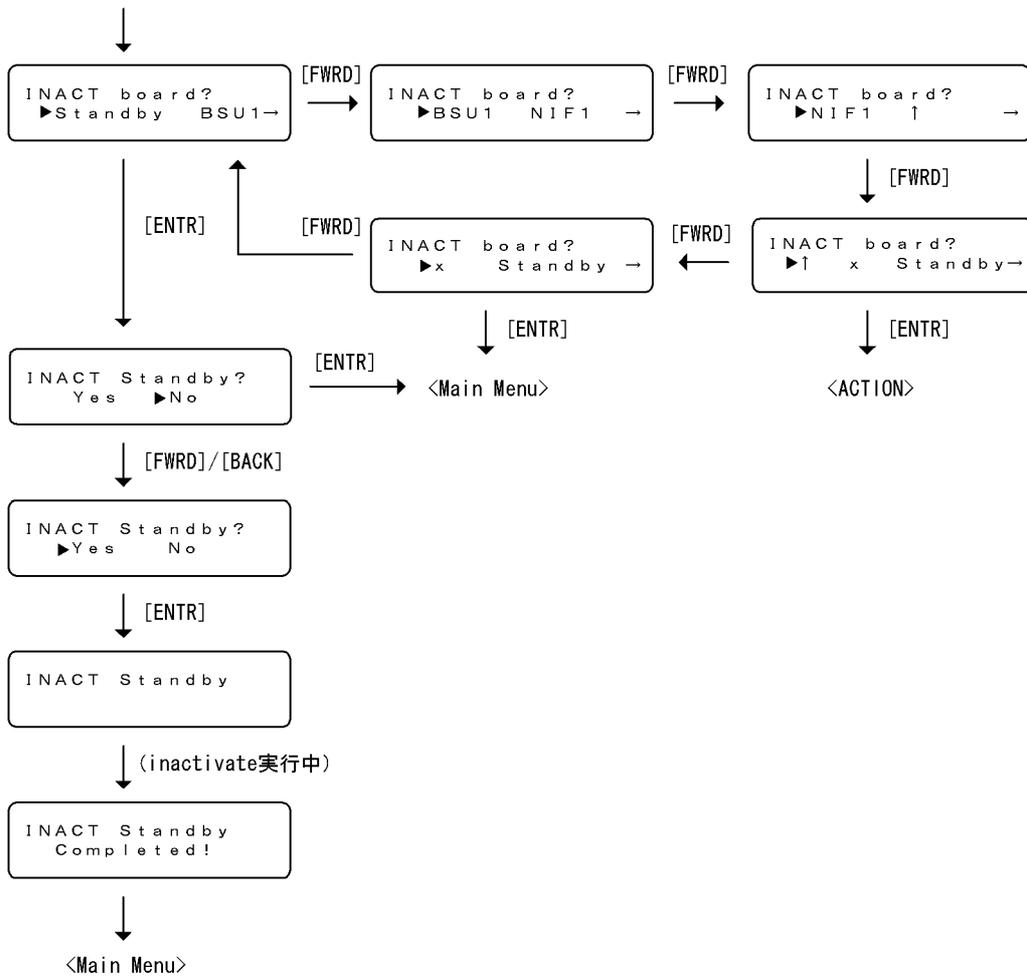
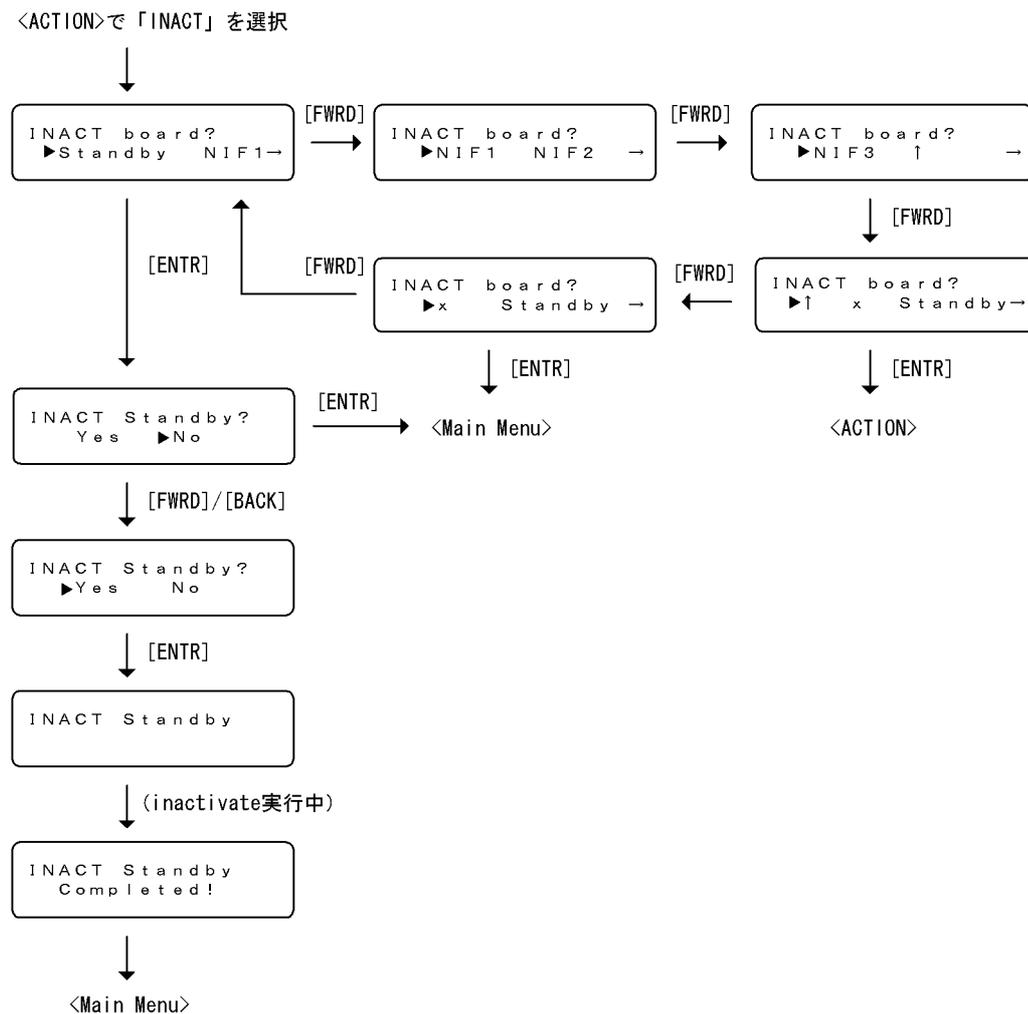


図 11-14 inactivate の操作手順【AX6600S】【AX6300S】



(4) activate の操作

図 11-15 activate の操作手順【AX6700S】

<ACTION>で「ACT」を選択

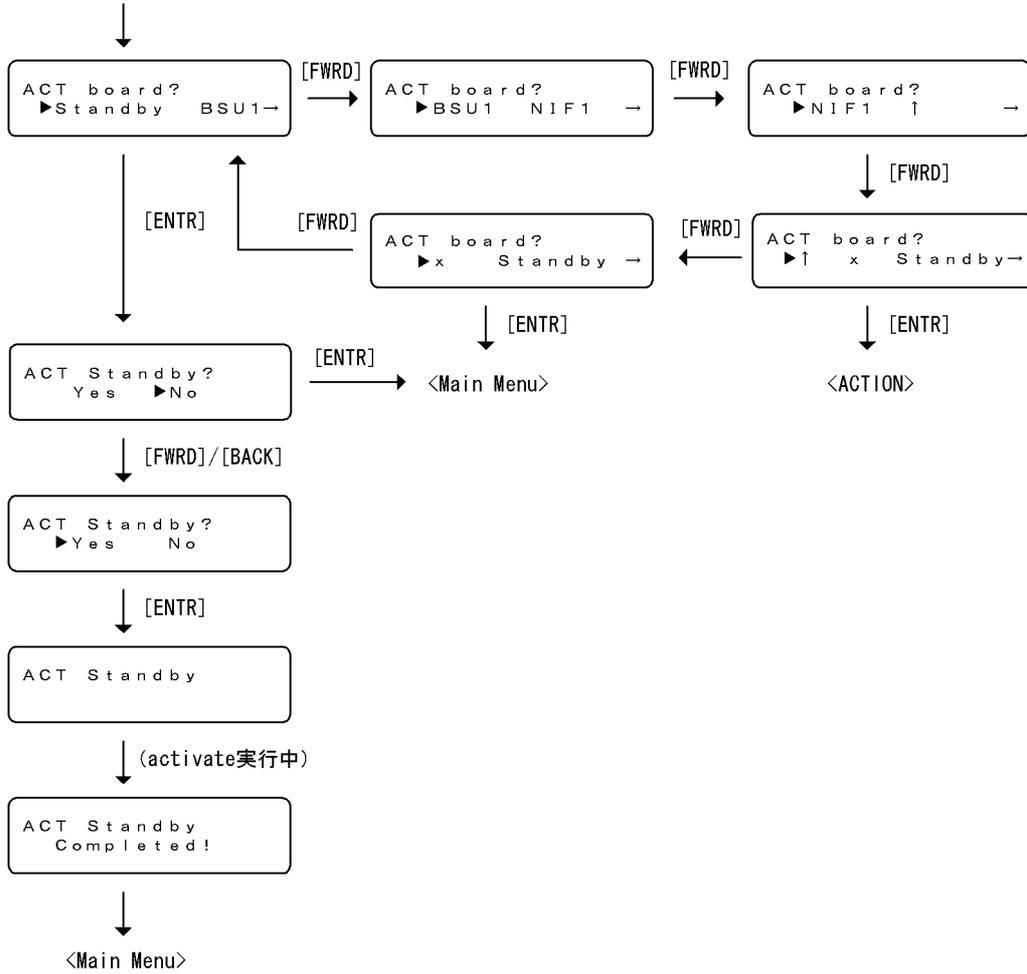
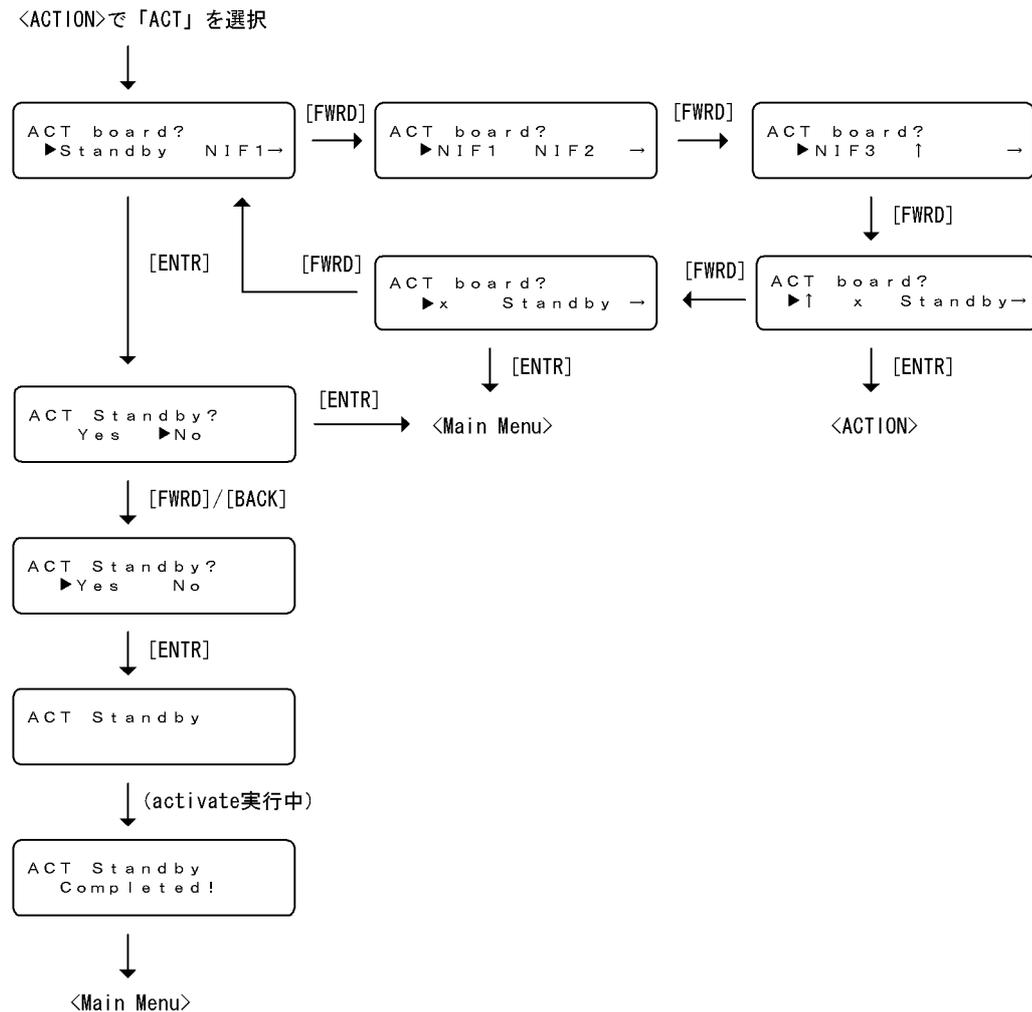


図 11-16 activate の操作手順【AX6600S】【AX6300S】



(5) コンフィグレーションについて

NIF ボードの交換を実施し、交換前と交換後で異なる NIF ボードに交換した場合、交換前と交換後で物理インタフェースの種別が異なるコンフィグレーションについては、交換後の NIF ボードに対応した物理インタフェースのコンフィグレーションに自動的に変更されます。その際、変更前に設定されていた物理インタフェースに関連するコンフィグレーションは削除されます。

11.1.8 装置の停止

システム操作パネルから装置の停止を指示できます。システム操作パネルから装置を停止した場合、装置を再度起動するには、電源スイッチを一度 OFF にしてから ON にしてください。

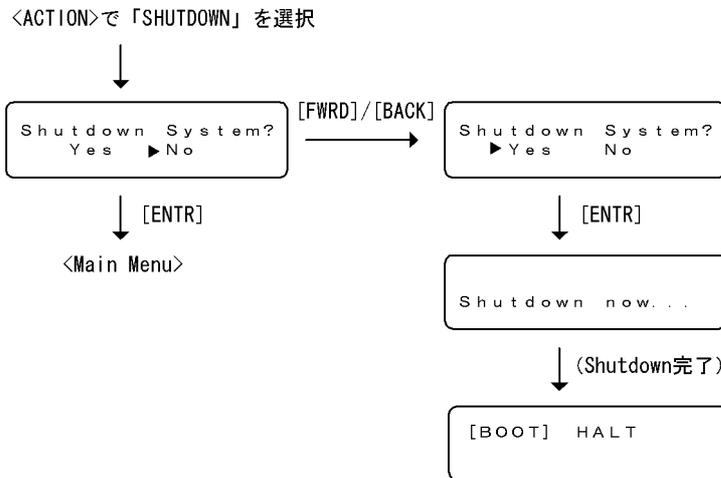
<ACTION> で「SHUTDOWN」を選択して [ENTR] キーを押すと、装置の停止の確認画面を表示します。

(1) ほかの情報表示の抑制

装置の停止の動作指示を行っている間は、障害情報は表示しません。

(2) 装置の停止の操作

図 11-17 装置の停止の操作手順



11.1.9 障害の表示

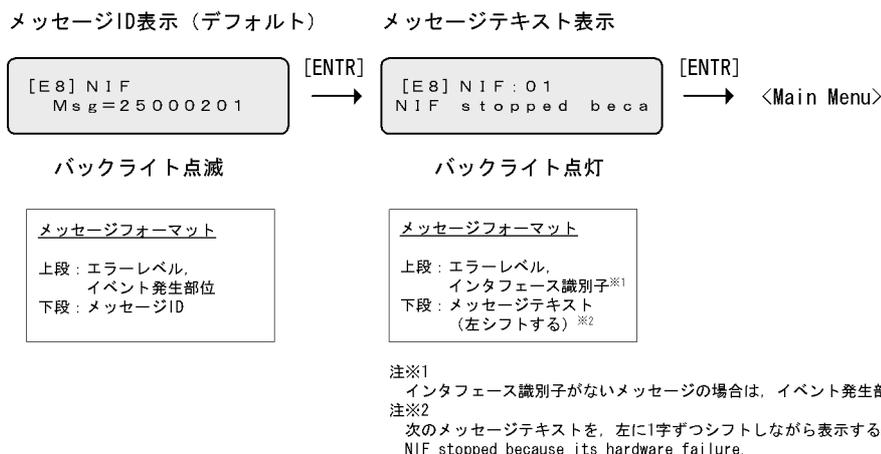
装置内で故障が発生した場合、および装置内で故障が発生中に <Main Menu> から「Alarm」を選択した場合、故障部位または機能の切り分けを行うためにシステム操作パネルに障害を表示します。BCU ボード、CSU ボードまたは MSU ボード上の SYSTEM LED が赤点灯している場合は、装置障害が発生していることを示す障害表示を行います。また、SYSTEM LED が橙点灯している場合は、装置の部分障害が発生していることを示す障害表示を行います。

障害表示は、エラーレベル E9、E8、E7、E6、E5 の障害に対して行い、エラーレベルの高い障害を優先的に表示します。障害個所が修復されると、障害表示は自動的に消えます。

(1) 障害表示

障害が発生すると、エラーレベルとともにイベント発生部位とメッセージ ID を、バックライトを点滅させながら表示します。[ENTR] キーを押すと、インタフェース識別子とその障害のメッセージテキストをバックライト点灯で表示します。再度、[ENTR] キーを押すと、<Main Menu> を表示します。メッセージテキストは、画面左側に移動しながら繰り返し表示します。

図 11-18 障害表示の表示例 (NIF でハードウェア障害を検出した例)



(2) 障害表示中のメニューの表示

障害表示中、装置情報の表示や動作指示を行うために <Main Menu> を表示するには、メッセージ ID 表示の場合は [ENTR] キーを 2 回、メッセージテキスト表示の場合は [ENTR] キーを 1 回押します。

次の場合、メニュー表示から障害表示へ戻ります。

- 動作指示以外の状態で、障害が発生した場合
- <Main Menu> で 10 秒間経った状態で、障害状態が解除されていない場合
- <Main Menu> から「Alarm」が選択された場合

(3) ほかの情報表示との関係

ほかの情報表示を行っている場合でも、障害が発生した場合は障害表示を優先して表示します。ただし、動作指示を行っている場合は、障害が発生しても障害表示を行いません。動作指示が終了したあと、障害表示を行います。

(4) 多重障害時の障害表示

多重障害が発生している場合は、エラーレベルを囲む括弧を【】で表示します。多重障害時には、[FWRD] キーまたは [BACK] キーを押すごとに、表示モードを維持しながらほかの障害表示を順次行います。例えば、メッセージ ID 表示をしている場合はほかのメッセージ ID 表示を行い、メッセージテキスト表示をしている場合はほかのメッセージテキスト表示を行います。表示中の障害表示が発生している障害の中でエラーレベルが最上位のものでない場合は、表示してから 30 秒後にエラーレベルが最上位の障害表示に戻ります。

図 11-19 多重障害時の障害表示



11.1.10 NIF ポートの LED 確認

運用系システムのシステム操作パネルの操作キーを操作すると、NIF ポートの LED 消灯を設定している場合でも、NIF ポートの LED が点灯して、ポートの動作状態を確認できます。なお、点灯した LED は、

キー操作のあと 60 秒後に消灯します。

11.2 装置の状態確認，および運用形態に関する設定

11.2.1 コンフィグレーション・運用コマンド一覧

装置を管理する上で必要なコンフィグレーションコマンド，および運用コマンドの一覧を次の表に示します。

表 11-15 コンフィグレーションコマンド一覧

コマンド名	説明
fldm prefer	装置のフロー系テーブルエントリ数の配分パターンを設定します。
fwdm prefer	装置の経路系テーブルエントリ数の配分パターンを設定します。
system fan mode	ファンの運転モードを設定します。
system hardware-mode	装置のハードウェアモードを設定します。
system recovery	no system recovery コマンドを設定すると，装置の障害が発生した際に，障害部位の復旧処理を行わないようにし，障害発生以降に障害部位を停止したままにします。
system temperature-warning-level	装置の入気温度が指定温度を超えた場合に運用メッセージを出力します。

表 11-16 運用コマンド一覧（ソフトウェアバージョンと装置状態の確認）

コマンド名	説明
show version	本装置に組み込まれているソフトウェアや実装されているボードの情報を表示します。
show system	本装置の運用状態を表示します。
clear control-counter	障害による装置再起動回数および部分再起動回数を 0 クリアします。
show environment	筐体のファン，電源機構，温度の状態と累積稼働時間を表示します。
reload	装置を再起動します。
show tech-support	テクニカルサポートで必要となるハードウェアおよびソフトウェアの状態に関する情報を表示します。
show tcpdump	本装置に対して送受信されるパケットをモニタします。

表 11-17 運用コマンド一覧（装置内メモリと MC の確認）

コマンド名	説明
show flash	装置内メモリの使用状態を表示します。
show mc	MC の形式と使用状態を表示します。
format mc	MC を本装置用のフォーマットで初期化します。

表 11-18 運用コマンド一覧（ログ情報の確認）

コマンド名	説明
show logging	本装置で収集しているログを表示します。
clear logging	本装置で収集しているログを消去します。
show logging console	set logging console コマンドで設定された内容を表示します。
set logging console	システムメッセージの画面表示をイベントレベル単位で制御します。

表 11-19 運用コマンド一覧（リソース情報とダンプ情報の確認）

コマンド名	説明
show cpu	CPU 使用率を表示します。
show processes	装置の現在実行中のプロセスの情報を表示します。
show memory	装置の現在使用中のメモリの情報を表示します。
df	ディスクの空き領域を表示します。
du	ディレクトリ内のファイル容量を表示します。
erase dumpfile	ダンプファイルを消去します。
show dumpfile	ダンプファイル格納ディレクトリに格納されているダンプファイルの一覧を表示します。

11.2.2 ソフトウェアバージョンの確認

運用コマンド `show version` で本装置に組み込まれているソフトウェアの情報を確認できます。次の図に例を示します。

図 11-20 ソフトウェア情報の確認

```
> show version software
Date 2006/03/25 15:11:20 UTC
S/W: OS-SE Ver. 10.2
>
```

11.2.3 装置の状態確認

運用コマンド `show system` で装置の動作状態や搭載メモリ量などを確認できます。次の図に例を示します。

図 11-21 装置の状態確認

```

> show system
Date 2006/07/18 18:36:57 UTC
System: AX6308S, OS-SE Ver. 10.2
Node : Name=System Name
      Contact=Contact Address
      Locate=Location
      Elapsed time : 2days 03:25:01
      Machine ID : 0012.e220.5100
      Device redundancy cpu status : duplex
      Power control : normal
      Power redundancy-mode : check is executed
      PS1 = active
      PS2 = active
      PS3 = notconnect
      PS4 = notconnect
      PS5 = notconnect
      PS6 = notconnect
      Fan:active No = FAN1(1), FAN1(2), FAN1(3),
                    FAN2(4), FAN2(5), FAN2(6),
                    FAN3(7), FAN3(8), FAN3(9)
                    Speed = normal

MSU1 : active
      CPU:AX-F6300-51A [MSU-1A , 80200020]
      Boot : 2006/07/18 18:35:42 , power on , 0 times restart
      PSP : active
      Lamp : STATUS LED=green , ACTIVE LED=green , SYSTEM1 LED=green
      System operation panel : No error
      Board : CPU=PowerPC 667MHz , Memory=1,048,576kB(1024MB)
      Management port: active up
              10BASE-T half(auto) , 0012.e220.3401
      Temperature : normal(27degree)
      Flash :
              user area  config area  dump area  area total
      used  63,470kB      91kB      6,326kB    69,887kB
      free  29,872kB      19,318kB  14,734kB   63,924kB
      total 93,342kB      19,409kB  21,060kB   133,811kB
      MC : enabled
              Manufacture ID : 00000003
              19,343kB used
              103,616kB free
              122,959kB total

MSU2 : standby
      CPU:AX-F6300-51A [MSU-1A , 80200020]
      Boot : 2006/07/18 18:36:25 , power on , 0 times restart
      PSP : standby
      Lamp : STATUS LED=green , ACTIVE LED=light off , SYSTEM1 LED=green
      System operation panel : No error
      Board : CPU=PowerPC 667MHz , Memory=1,048,576kB(1024MB)
      Management port: unused
      Temperature : normal(25degree)
      Flash :
              user area  config area  dump area  area total
      used  62,699kB      91kB      4,800kB    67,590kB
      free  30,643kB      19,318kB  16,260kB   66,221kB
      total 93,342kB      19,409kB  21,060kB   133,811kB
      MC : enabled
              Manufacture ID : 00000003
              22,863kB used
              100,096kB free
              122,959kB total

Forwarding Database Management
      fwdm : ipv4-uni standard
              IPv4 Unicast resources  Used/Max: 0 / 65536
              IPv4 Multicast resources Used/Max: 0 / 0

```

```

IPv6 Unicast resources    Used/Max:      0 /      0
IPv6 Multicast resources Used/Max:      0 /      0
MAC Address resources    Used/Max:      0 / 24576
  MAC Address (Learned) used           :      0
  MAC Address (Static) used            :      0
  MAC Address (IEEE 802.1X/Web/MAC) used :      0
  MAC Address (not Learned/ARP,NDP resolved) used :      0
  VLAN config used                   :      0
Shared resources          Used/Max:      0B/1638400B
  IPv4 Unicast Single-path used :      0B
  IPv4 Unicast Multi-path used  :      0B
  IPv6 Unicast Single-path used :      0B
  IPv6 Unicast Multi-path used  :      0B
  IPv4 Multicast used           :      0B
  IPv6 Multicast used           :      0B
  IPv4 Policy Based Routing used:      0B
  IPv6 Policy Based Routing used:      0B
  Policy Based Switching used   :      0B
  VLAN config used              :      0B
  IGMP/MLD Snooping used       :      0B
Flow Database Management
  Filter resources            Used/Max:    1856/   4000
    MAC :      239  IPv4 :    1046  IPv6 :     571
  QoS resources               Used/Max:    1206/   4000
    MAC :      18  IPv4 :     814  IPv6 :     374

```

>

運用コマンド show environment でファン、電源機構、温度の状態、累積稼働時間を確認できます。ファンの運転モードはコンフィグレーションコマンド system fan mode で設定できます。次の図に例を示します。

図 11-22 装置の環境状態確認

```

> show environment
Date 2011/07/20 18:00:00 UTC

Fan environment
  FAN1(1) : active    FAN1(2) : active    FAN1(3) : active
  FAN2(4) : active    FAN2(5) : active    FAN2(6) : active
  FAN3(7) : active    FAN3(8) : active    FAN3(9) : active
  FAN4(10): active   FAN4(11): active   FAN4(12): active
  Speed   : normal
  Mode    : 2 (cool)

Power environment
  Power supply type : AC
  PS1 : active      PS2 : active      PS3 : active      PS4 : active
  PS5 : notconnect PS6 : notconnect PS7 : notconnect PS8 : notconnect

Temperature environment
  BCU1 Temperature : 36 degrees C
  BCU2 Temperature : 37 degrees C
  BSU1 Temperature : 32 degrees C
  BSU2 Temperature : 34 degrees C
  BSU3 Temperature : 31 degrees C
  NIF1 Temperature : 34 degrees C
  NIF2 Temperature : 32 degrees C
  NIF3 Temperature : 31 degrees C
  NIF4 Temperature : 30 degrees C
  NIF5 notconnect
  NIF6 notconnect
  NIF7 notconnect
  NIF8 notconnect
  Warning level : normal

Accumulated running time
      total          caution
BCU1 : 365 days and 18 hours : 10 days and 8 hours
BCU2 : 365 days and 18 hours : 10 days and 8 hours
BSU1 : 365 days and 18 hours : 10 days and 8 hours
BSU2 : 365 days and 18 hours : 10 days and 8 hours
BSU3 : 85 days and 18 hours : 0 days and 18 hours
NIF1 : 365 days and 18 hours : 10 days and 8 hours
NIF2 : 365 days and 18 hours : 10 days and 8 hours
NIF3 : 128 days and 20 hours : 1 days and 4 hours
NIF4 : 85 days and 11 hours : 0 days and 18 hours
NIF5 : notconnect
NIF6 : notconnect
NIF7 : notconnect
NIF8 : notconnect
PS1 : 365 days and 18 hours : 10 days and 8 hours
PS2 : 365 days and 18 hours : 10 days and 8 hours
PS3 : 128 days and 20 hours : 1 days and 4 hours
PS4 : 128 days and 20 hours : 1 days and 4 hours
PS5 : notconnect
PS6 : notconnect
PS7 : notconnect
PS8 : notconnect
FAN1 : 365 days and 18 hours : 10 days and 8 hours
FAN2 : 128 days and 20 hours : 1 days and 4 hours
FAN3 : 365 days and 18 hours : 10 days and 8 hours
FAN4 : 365 days and 18 hours : 10 days and 8 hours
>

```

運用コマンド show environment の temperature-logging パラメータで温度履歴情報を確認できます。次の図に例を示します。

図 11-23 温度履歴情報の確認

```
> show environment temperature-logging
Date 2011/07/20 17:00:00 UTC
Date      0:00  6:00 12:00 18:00
2011/07/20  24.3  24.2  26.0
2011/07/19  21.8  25.1  26.0  24.0
2011/07/18  25.6      -  26.0  24.0
2011/07/17  21.0      -  26.0  24.0
2011/07/16  24.0  23.5  26.0  24.0
2011/07/15  22.2  24.9  26.0  24.0
2011/07/14      -      -  26.0  24.0
>
```

11.2.4 装置内メモリの確認

運用コマンド `show flash` で装置内メモリ上のファイルシステムの使用状況を確認できます。もし、使用量が合計容量の 95% を超える場合は、マニュアル「トラブルシューティングガイド」を参照して対応してください。次の図に例を示します。

図 11-24 Flash 容量の確認

```
>show flash
Date 2006/07/18 18:45:14 UTC
Flash :
      user area   config area   dump area   area total
used   62,699kB      91kB       4,800kB     67,590kB
free   30,643kB     19,318kB    16,260kB    66,221kB
total  93,342kB     19,409kB    21,060kB    133,811kB
>
```

11.2.5 運用メッセージの出力抑止と確認

装置の状態が変化した場合、本装置は動作情報や障害情報などを運用メッセージとしてコンソールやリモート運用端末に表示します。例えば、回線が障害状態から回復した場合は回線が回復したメッセージを、回線が障害になって運用を停止した場合は回線が障害になったメッセージを表示します。運用メッセージの詳細については、マニュアル「メッセージ・ログレファレンス 2. ルーティングのイベント情報」を参照してください。

運用端末に出力される運用メッセージは、運用コマンド `set logging console` を使用することでイベントレベル単位で出力を抑止できます。また、その抑止内容については、運用コマンド `show logging console` で確認できます。イベントレベルが E5 以下の運用メッセージの運用端末への出力抑止の設定例を次に示します。

図 11-25 運用メッセージの出力抑止の設定例

```
> set logging console disable E5
> show logging console
System message mode : E5
>
```

注意

多数の運用メッセージが連続して発生した際は、コンソールやリモート運用端末上には一部しか表示しませんので、運用コマンド `show logging` で確認してください。

11.2.6 運用ログ情報の確認

運用メッセージは運用端末に出力するほか、運用ログとして装置内に保存します。この情報で装置の運用

状態や障害の発生を管理できます。

運用ログは装置運用中に発生した事象（イベント）を発生順に記録したログ情報で、運用メッセージと同様の内容が格納されます。運用ログとして格納する情報には次に示すものがあります。

- オペレータの操作および応答メッセージ
- 運用メッセージ

種別ログは装置内で発生した障害や警告についての運用ログ情報をメッセージ ID ごとに分類した上で、同事象が最初に発生した日時および最後に発生した日時と累積回数をまとめた情報です。

これらのログは装置内にテキスト形式で格納されており、運用コマンド `show logging` で確認できます。また、`grep` を使用してパターン文字列の指定を実施することで、特定のログ情報だけを表示することもできます。例えば、障害に関するログは `show logging | grep EVT` や `show logging | grep ERR` の実行でまとめて表示できます。障害に関するログの表示例を次の図に示します。

図 11-26 障害に関するログ表示

```
> show logging | grep EVT
:
(途中省略)
:
EVT 08/10 20:39:38 E3 SOFTWARE 00005002 1001:000000000000 Login operator from
LOGHOST1 (ttypl).
EVT 08/10 20:41:43 E3 SOFTWARE 00005003 1001:000000000000 Logout operator from
LOGHOST1 (ttypl).
:
(以下省略)
:
>
```

11.2.7 テーブルエントリの配分パターンの設定

本装置では、ネットワーク構成に合わせて適切なテーブルエントリ数の配分パターンを選べます。配分パターンは経路系テーブルエントリとフロー系テーブルエントリがあり、それぞれコンフィグレーションコマンド `fwdm prefer` とコンフィグレーションコマンド `fldm prefer` で指定できます。

なお、各配分パターンと各テーブルのエントリ数に関する情報は、運用コマンド `show system` で確認できます。

テーブル容量種別を次の表に示します。

表 11-20 経路系テーブル容量

テーブル容量	対応 BSU	対応 CSU	対応 MSU
standard	BSU-LA	CSU-1A	MSU-1A, MSU-1A1
extended	BSU-LB	CSU-1B	MSU-1B, MSU-1B1

表 11-21 フロー系テーブル容量

テーブル容量	対応 BSU	対応 CSU	対応 MSU
standard	BSU-LA	CSU-1A	MSU-1A, MSU-1A1
standard-advance			
extended	BSU-LB	CSU-1B	MSU-1B, MSU-1B1
extended-advance			

注 フロー検出拡張モードを使用する場合に指定します。

(1) 経路系エントリテーブル

経路系エントリテーブルの配分パターンを次の表に示します。

表 11-22 経路系テーブルエントリ配分パターン

パターン名称	意味
default	全エントリ混在
ipv4-uni	IPv4 ユニキャスト主体, マルチキャスト, IPv6 無し
ipv4-ipv6-uni	IPv4 ユニキャスト /IPv6 ユニキャスト主体, マルチキャスト無し
vlan	L2 主体, マルチキャスト無し

注 デフォルトのパターン

AX6700S の経路系テーブルエントリ数の配分パターンについては、「3.2 AX6700S の収容条件【AX6700S】」の「表 3-10 standard の経路系テーブルエントリ数」および「表 3-11 extended の経路系テーブルエントリ数」を参照してください。

AX6600S の経路系テーブルエントリ数の配分パターンについては、「3.4 AX6600S の収容条件【AX6600S】」の「表 3-117 standard の経路系テーブルエントリ数」および「表 3-118 extended の経路系テーブルエントリ数」を参照してください。

AX6300S の経路系テーブルエントリ数の配分パターンについては、「3.6 AX6300S の収容条件【AX6300S】」の「表 3-224 standard の経路系テーブルエントリ数」および「表 3-225 extended の経路系テーブルエントリ数」を参照してください。

(2) フロー系エントリテーブル

フロー系エントリテーブルの配分パターンを次の表に示します。

表 11-23 standard および standard-advance のフロー系テーブルエントリ配分パターン

パターン名称	意味
default	フィルタ, QoS 均等

注 デフォルトのパターン

表 11-24 extended および extended-advance のフロー系テーブルエントリ配分パターン

パターン名称	意味
default	フィルタ, QoS 均等
filter-only	フィルタ専用
qos-only	QoS 専用
filter	フィルタ主体
qos	QoS 主体

注 デフォルトのパターン

AX6700S のフロー系テーブルエントリ数のテーブル配分パターンについては、「3.2 AX6700S の収容条件【AX6700S】」の「表 3-12 standard のフロー系エントリ数」～「表 3-14 extended および

extended-advance のフロー系エントリ数」を参照してください。

AX6600S のフロー系テーブルエントリ数のテーブル配分パターンについては、「3.4 AX6600S の収容条件【AX6600S】」の「表 3-119 standard のフロー系エントリ数」～「表 3-121 extended および extended-advance のフロー系エントリ数」を参照してください。

AX6300S のフロー系テーブルエントリ数のテーブル配分パターンについては、「3.6 AX6300S の収容条件【AX6300S】」の「表 3-226 standard のフロー系エントリ数」～「表 3-228 extended および extended-advance のフロー系エントリ数」を参照してください。

(3) 経路系エントリテーブルのコンフィグレーション

[設定のポイント]

経路系エントリテーブルの初期状態は default です。本設定を変更すると、AX6700S ではすべての BSU を、AX6600S および AX6300S では PSP を自動的に再起動します。再起動が完了するまでは本装置を経由する通信が停止します。そのため、初期導入時に設定することをお勧めします。

[コマンドによる設定]

1. (config)# fwdm prefer ipv4-uni standard

PSP will be restarted automatically when the selected pattern differs from current pattern.

Do you wish to change pattern (y/n):

コンフィグレーションモードで、経路系エントリテーブルの配分パターンを ipv4-uni に設定します。コンフィグレーションの変更を確認し y を入力すると、AX6700S ではすべての BSU を、AX6600S および AX6300S では PSP を自動的に再起動します。n を入力した場合、コンフィグレーションを変更しません。

(4) フロー系エントリテーブルのコンフィグレーション

[設定のポイント]

フロー系エントリテーブルの初期状態は default です。本設定を変更すると、AX6700S ではすべての BSU を、AX6600S および AX6300S では PSP を自動的に再起動します。再起動が完了するまでは本装置を経由する通信が停止します。そのため、初期導入時に設定することをお勧めします。

[コマンドによる設定]

1. (config)# fldm prefer qos standard

PSP will be restarted automatically when the selected pattern differs from current pattern.

Do you wish to change pattern (y/n):

コンフィグレーションモードで、フロー系エントリテーブルの配分パターンを qos に設定します。コンフィグレーションの変更を確認し y を入力すると、AX6700S ではすべての BSU を、AX6600S および AX6300S では PSP を自動的に再起動します。n を入力した場合、コンフィグレーションを変更しません。

11.2.8 ハードウェアモードの設定

本装置では、使用する機能に合わせてハードウェアモードを設定します。ハードウェアモードは、コンフィグレーションコマンド system hardware-mode で設定できます。

設定できるハードウェアモードの種類を次の表に示します。なお、ハードウェアモードを設定しないと、

サポート機能は使用できません。

表 11-25 ハードウェアモードの種類と対応する機能

ハードウェアモード	サポート機能
アクセスリストロギング対応ハードウェアモード	アクセスリストロギング

注 すべての BCU/CSU/MSU で設定できます。

(1) アクセスリストロギング対応ハードウェアモード

アクセスリストロギングに対応したハードウェアモードです。アクセスリストロギングは、本ハードウェアモードでだけ使用できます。アクセスリストロギングについては、「コンフィグレーションガイド Vol.2 2. アクセスリストロギング」を参照してください。

なお、本モードによる他機能への影響はありません。

[設定のポイント]

本設定を変更すると、ハードウェアモードの反映が完了するまで本装置を経由する通信が停止します。そのため、初期導入時に設定することをお勧めします。

[コマンドによる設定]

1. (config)# system hardware-mode access-log

コンフィグレーションモードで、ハードウェアモードに access-log を設定します。

11.3 運用情報のバックアップ・リストア

装置障害または交換時の運用情報の復旧手順を示します。

BCU/CSU/MSU を二重化している場合には、「11.3.2 BCU/CSU/MSU 二重化時の手順」を実施してください。BCU/CSU/MSU が一重化の場合に確実かつ簡単に行うためには「11.3.3 BCU/CSU/MSU 一重化時の backup/restore コマンドを用いる手順」の手順を実施してください。すべてを手作業で復旧することもできますが、取り扱う情報が複数にわたるため管理が複雑になり、また、完全に復旧できないため、お勧めしません。

11.3.1 運用コマンド一覧

バックアップ・リストアに使用する運用コマンド一覧を次の表に示します。

表 11-26 運用コマンド一覧

コマンド名	説明
backup	稼働中のソフトウェアおよび装置の情報を MC またはリモートの ftp サーバに保存します。
restore	MC およびリモートの ftp サーバに保存している装置情報を本装置に復旧します。

11.3.2 BCU/CSU/MSU 二重化時の手順

交換した BCU/CSU/MSU が待機系で立ち上がっている状態で、次のコマンドによってソフトウェアバージョンおよび設定ファイルを待機系と同期させます。なお、ソフトウェアバージョンが 11.0 以降の場合、運用系と待機系のライセンスキー情報が一致しない状態では、SYSTEM1 LED が橙点灯し、一時的にコマンドによる系切替が抑止されます。

- ppupdate コマンド
ソフトウェアバージョンを同期させます。
- synchronize コマンド
その他の設定ファイルを同期させます。本コマンドで同期する対象には、コンフィグレーション、ユーザアカウント、パスワード、ライセンスキーファイルを含みます。同期したライセンスキーファイルを有効にするには、reload コマンドを使って待機系を再起動する必要があります。

二重化運用時の管理情報の同期処理については、「コンフィグレーションガイド Vol.2 17. BCU/CSU/MSU の冗長化」を参照してください。

なお、BCU/CSU/MSU 二重化時に運用系および待機系の両系 BCU/CSU/MSU を同時に交換した場合には、restore コマンドを使って次の手順で復旧します。

1. restore コマンド実行時に系切替が発生しないよう deactivate standby コマンドで待機系を deactivate 状態にします。
2. 運用系で restore コマンドを実行します。これによって運用系が再起動します。
3. activate standby コマンドで待機系を activate 状態にします。
4. ppupdate コマンドおよび synchronize コマンドで運用系と待機系を同期させます。
5. オプションライセンスを導入している場合、ライセンスキーを反映させるために reload no-dump-image standby コマンドで待機系を再起動します。

11.3.3 BCU/CSU/MSU 一重化時の backup/restore コマンドを用いる手順

(1) 情報のバックアップ

装置が正常に稼働しているときに、backup コマンドを用いてバックアップを作成しておきます。backup コマンドは、装置の稼働に必要な次の情報を一つのファイルにまとめて、MC または外部の FTP サーバに保存します。

これらの情報に変更があった場合、backup コマンドによるバックアップの作成をお勧めします。

- ソフトウェアを稼働中のバージョンにアップデートするためのファイル
- startup-config
- 電源運用モード
- ユーザアカウント/パスワード
- オプションライセンスの有無
- Web 認証データベース
- Web 認証用に登録された認証画面ファイル
- MAC 認証データベース
- IPv6 DHCP サーバ DUID ファイル

backup コマンドでは次に示す情報は保存されないので注意してください。

- show logging コマンドで表示される運用ログ情報など
- 装置内に保存されているダンプファイルなどの障害情報
- ユーザアカウントごとに設けられるホームディレクトリにユーザが作成および保存したファイル

(2) 情報のリストア

backup コマンドで作成されたバックアップファイルから情報を復旧する場合、restore コマンドを用います。

restore コマンドを実行すると、バックアップファイル内に保存されているソフトウェアアップデート用ファイルを用いて装置のソフトウェアをアップデートします。このアップデート作業後、装置は自動的に再起動します。再起動後、復旧された環境になります。

11.4 装置の温度監視

本装置では入気温度を監視して、入気温度が高温注意レベル以上になるとファンを高速回転させます。入気温度が高温注意回復レベル以下に戻ると、ファンを通常回転に戻します。また、入気温度が高温停止レベル以上になると、装置を停止します。

11.4.1 装置入気温度の監視対象

(1) AX6700S の監視対象

BCU の搭載位置と入気温度の監視対象を次の表に示します。

表 11-27 BCU の搭載位置と入気温度の監視対象

BCU 搭載位置		入気温度の監視対象
BCU1	BCU2	
電源 ON	電源 ON	BCU2
電源 ON	停止, 電源 OFF または未搭載	BCU1
停止, 電源 OFF または未搭載	電源 ON	BCU2

(2) AX6600S/AX6300S の監視対象

運用系および待機系の CSU/MSU で測定した温度を入気温度として監視します。

11.4.2 入気温度の監視レベルと動作

入気温度の監視レベルと動作を次の表に示します。

表 11-28 監視レベルと動作

入気温度	監視レベル	システムの動作	ファンの回転
2	低温注意レベル	運用を継続して、ログを出力します。	通常
5	低温注意回復レベル	運用を継続して、ログを出力します。	通常
40	高温注意回復レベル	運用を継続して、ログを出力します。	通常
43	高温注意レベル	運用を継続して、ログを出力します。	高速
55	高温警告回復レベル	運用を継続して、ログを出力します。	高速
58	高温警告レベル	運用を継続して、ログを出力します。	高速
65	高温停止レベル	ログを出力して装置を停止します。自動復旧はしません。	-

(凡例) - : 該当なし

注 AX6600S/AX6300S の場合、運用系で測定した温度でファンを制御します。

高温停止レベル検出時の動作を次に示します。

AX6700S の場合

BCU が一重化の場合

ログを出力して装置を停止します。

BCU が二重化で、BCU1 が運用系の場合

ログを出力して BCU2 を停止（電源 OFF）し、一重化で運用します。

その 5 分後から BCU1 で入気温度の監視を開始して、さらに高温停止レベルを検出した場合、ログを出力して装置を停止します。

BCU が二重化で、BCU2 が運用系の場合

ログを出力して BCU2 を停止（電源 OFF）します。系切替をして BCU1 が運用系となり、一重化で運用します。

その 5 分後から BCU1 で入気温度の監視を開始して、さらに高温停止レベルを検出した場合、ログを出力して装置を停止します。

AX6600S/AX6300S の場合

CSU/MSU が一重化の場合

ログを出力して装置を停止します。

CSU/MSU が二重化で、運用系で検出した場合

ログを出力して運用系を停止します。系切替をして一重化で運用します。

さらに新運用系で高温停止レベルを検出した場合、ログを出力して装置を停止します。

CSU/MSU が二重化で、待機系で検出した場合

ログを出力して待機系を停止し、一重化で運用します。

さらに運用系で高温停止レベルを検出した場合、ログを出力して装置を停止します。

11.5 障害時の復旧

本装置では運用中に障害が発生した場合は自動的に復旧処理をします。障害部位に応じて復旧処理を局所化して行い、復旧処理による影響範囲を狭めることによって、正常運用部分が中断しないようにします。

11.5.1 障害部位と復旧内容

障害発生時、障害の内容によって復旧内容が異なります。障害部位と復旧内容を次の表に示します。

表 11-29 障害部位と復旧内容

障害部位	装置の対応	復旧内容	影響範囲
ポートで検出した障害	自動復旧を無限回行います。	該当するポートの再初期化を行います。	該当するポートを介する通信が中断されます。
ネットワークインタフェースボード障害 (NIF)	自動復旧を 3 回まで行います。 ¹ 自動復旧の回数が 3 回のときに障害が発生すると停止します。ただし、1 時間ごとに自動復旧の回数を初期化して、再度自動復旧を行います。	該当する NIF の再初期化を行います。	該当する NIF が収容する全ポートを介する通信が中断されます。
基本スイッチング機構障害 (BSU)	自動復旧を 3 回まで行います。 ¹ 自動復旧の回数が 3 回のときに障害が発生すると停止します。ただし、1 時間ごとに自動復旧の回数を初期化して、再度自動復旧を行います。	該当する BSU の再初期化を行います。なお、待機系 BSU がある場合は系切替による復旧処理を行います。	BSU を冗長化している場合は通信を維持できます。該当する BSU 以外に運用系の BSU がない場合、全 NIF を介する通信が中断されます。なお、BSU の固定モードを使用している場合は該当する BSU を経由する通信が中断されます。
基本制御機構障害 (BCU)	自動復旧を 6 回まで行います。 ² 自動復旧の回数が 6 回のときに障害が発生すると停止します。ただし、復旧後 1 時間以上運用すると、自動復旧の回数を初期化します。	該当する BCU の再初期化を行います。なお、BCU を冗長化している場合は系切替による復旧処理を行います。	装置内の全ポートを介する通信が中断されます。なお、BCU を冗長化している場合は通信を維持できます。
制御スイッチング機構障害 (CSU)	自動復旧を 6 回まで行います。 ³ 自動復旧の回数が 6 回のときに障害が発生すると停止します。ただし、復旧後 1 時間以上運用すると、自動復旧の回数を初期化します。	該当する CSU の再初期化を行います。なお、CSU を冗長化している場合は系切替による復旧処理を行います。	装置内の全ポートを介する通信が中断されます。なお、CSU を冗長化している場合は通信を維持できます。
管理スイッチング機構障害 (MSU)	自動復旧を 6 回まで行います。 ⁴ 自動復旧の回数が 6 回のときに障害が発生すると停止します。ただし、復旧後 1 時間以上運用すると、自動復旧の回数を初期化します。	該当する MSU の再初期化を行います。なお、MSU を冗長化している場合は系切替による復旧処理を行います。	装置内の全ポートを介する通信が中断されます。なお、MSU を冗長化している場合は通信を維持できます。
装置筐体障害	停止します。	装置の再起動を行います。	装置内の全ポートを介する通信が中断されます。

11. 装置の管理

障害部位	装置の対応	復旧内容	影響範囲
電源機構障害 (PS)	装置の運用に必要な電力が供給されなくなると停止します。なお、電源機構が冗長化されている場合は停止しません。	装置を停止します。なお、電源機構が冗長化されている場合は停止しません。	装置内全ポートを介する通信が中断されます。なお、電源機構が二重化されている場合は通信の中断はありません。
ファン障害	<ol style="list-style-type: none"> ファンユニット内のファンが1個故障した場合、残りのファンを高速にします。 同一ファンユニット内のファンが2個以上故障した場合、残りのファンを高速にし、5分以上その状態が継続すると装置を停止します。 	<ol style="list-style-type: none"> 自動復旧はありません。ファンユニットを交換してください。 装置を停止します。 	<ol style="list-style-type: none"> ファンが高速回転しますが通信に影響はありません。 装置内の全ポートを介する通信が中断されます。

注 1
 コンフィグレーションコマンド `no system recovery` で復旧処理をしない設定にしている場合は、自動復旧を行いません。

注 2
 コンフィグレーションコマンド `no system recovery` で復旧処理をしない設定にしている場合は、障害による BCU 再起動後、該当する BCU で BSU の起動を抑止します。

注 3
 コンフィグレーションコマンド `no system recovery` で復旧処理をしない設定にしている場合は、障害による CSU 再起動後、該当する CSU で PSP の起動を抑止します。

注 4
 コンフィグレーションコマンド `no system recovery` で復旧処理をしない設定にしている場合は、障害による MSU 再起動後、該当する MSU で PSP の起動を抑止します。

12 BSU/NIF の管理

この章では、BSU/NIF を導入した際、および BSU/NIF を管理する上で必要な作業について説明します。

12.1 BSU の状態確認、および運用形態に関する設定【AX6700S】

12.2 NIF の状態確認、および運用形態に関する設定

12.1 BSU の状態確認 , および運用形態に関する設定 【AX6700S】

12.1.1 コンフィグレーション・運用コマンド一覧

BSU を管理する上で必要なコンフィグレーションコマンド一覧 , および運用コマンド一覧を次の表に示します。

表 12-1 コンフィグレーションコマンド一覧

コマンド名	説明
power enable	disable 状態のボードを active 状態にします。また , ボードの電力を OFF にします。

表 12-2 運用コマンド一覧

コマンド名	説明
activate bsu	inactive 状態の BSU を active 状態にします。
inactivate bsu	active 状態の BSU を inactive 状態にします。また , BSU の電力を OFF にします。
show system	BSU の運用状態を表示します。

注

「運用コマンドレファレンス Vol.1 9. ソフトウェアバージョンと装置状態の確認」を参照してください。

12.1.2 ボードの disable 設定

未使用のボードに disable 設定をします。また , ボードの電力を OFF します。

[設定のポイント]

未使用の BSU を disable に設定します。また , ボードの電力を OFF にします。

[コマンドによる設定]

1. (config)# no power enable bsu 1

コンフィグレーションモードで , BSU 番号 1 のボードを disable 設定します。

12.1.3 BSU の状態確認

運用コマンド show system で BSU の動作状態を確認できます。次の図に例を示します。

図 12-1 BSU の状態確認

```
> show system
Date 2006/06/13 06:35:27 UTC
System: AX6700S-S08, OS-SE Ver. 10.3
.
.
.
BSU1 : Active AX-F6700-3LA [BSU-LA]
      :
BSU2 : Active AX-F6700-3LA [BSU-LA]
      :
BSU3 : standby hot AX-F6700-3LA [BSU-LA]
      :
>
```

12.2 NIF の状態確認，および運用形態に関する設定

12.2.1 コンフィグレーション・運用コマンド一覧

NIF を管理する上で必要なコンフィグレーションコマンド一覧，および運用コマンド一覧を次の表に示します。

表 12-3 コンフィグレーションコマンド一覧

コマンド名	説明
power enable	disable 状態のボードを active 状態にします。また，ボードの電力を OFF にします。
system nif-hdc restart	系切替時の HDC (Hardware Dependent Code) アップデートの方法を設定します。
system nif-hdc software-bundle	ソフトウェアにバンドルされている HDC (Hardware Dependent Code) または NIF の HDC のどちらを適用するか設定します。

表 12-4 運用コマンド一覧

コマンド名	説明
show nif	NIF の運用状態を表示します。
clear counters nif	NIF の統計情報カウンタをクリアします。
inactivate nif	active 状態の NIF を inactive 状態にします。また，NIF の電力を OFF にします。
activate nif	inactive 状態の NIF を active 状態にします。

12.2.2 ボードの disable 設定

未使用のボードに disable 設定をします。また，ボードの電力を OFF にします。

[設定のポイント]

未使用の NIF を disable に設定します。また，ボードの電力を OFF にします。

[コマンドによる設定]

1. (config)# no power enable nif 1

コンフィグレーションモードで，NIF 番号 1 のボードを disable に設定します。

12.2.3 HDC アップデート設定

NIF には，ボード上の読み書き可能な領域に NIF の制御に関するソフトウェア (HDC : Hardware Dependent Code) があります。HDC はソフトウェアにバンドルされていて，ソフトウェアアップデートによって，HDC のアップデートができます。

(1) 系切替時の HDC アップデート設定

BCU，CSU または MSU 二重化構成では，運用系のソフトウェアアップデート時に待機系への系切替をします。この時に，新運用系システムで NIF の HDC のアップデートがある場合，自動で NIF を再起動し，HDC のアップデートを行います。

無停止ソフトウェアアップデートを行う場合は，手動アップデートに設定すると，通信を中断しないでソ

ソフトウェアのアップデートを実施できます。HDC アップデートを行う場合は、該当する NIF に対して `inactivate` コマンド、`activate` コマンドを実行し、再起動してください。

[設定のポイント]

系切替前に設定を確認してください。

[コマンドによる設定]

1. `(config)# no system nif-hdc restart`

コンフィグレーションモードで、系切替時の HDC アップデート設定を手動アップデートにします。

(2) ソフトウェアにバンドルされている HDC アップデート設定

系切替時、および NIF の `activate` 時に、NIF の HDC とソフトウェアにバンドルされている HDC が異なる場合、NIF の HDC をソフトウェアにバンドルされている HDC にアップデートします。

NIF の HDC がソフトウェアにバンドルされている HDC より新しい場合は、ソフトウェアにバンドルされている HDC にアップデートしないを設定することで、そのまま運用できます。

[設定のポイント]

系切替前および NIF の再起動前に設定を確認してください。

[コマンドによる設定]

1. `(config)# no system nif-hdc software-bundle`

コンフィグレーションモードで、新しい NIF の HDC で運用する設定にします。

12.2.4 NIF の状態確認

(1) NIF の動作状態の確認

運用コマンド `show nif` で NIF の動作状態を確認できます。次の図に例を示します。

図 12-2 NIF の動作状態確認

```
>show nif 1
Date 2006/03/23 12:00:00 UTC
NIF1: disable - retry:0
Average:0Mbps/96Gbps Peak:0Mbps at 00:00:00
```

(2) NIF の HDC アップデート要否の確認

運用コマンド `show nif` を実行すると、NIF の HDC アップデート要否を確認できます。該当する NIF の HDC アップデートのために再起動が必要な場合、再起動要否状態の表示が `restart required` となっていることを確認します。次の図に例を示します。

図 12-3 NIF の HDC アップデート要否の確認

```
>show nif 1
Date 2008/04/10 12:00:00 UTC
NIF1: active(restart required) 48-port 10BASE-T/100BASE-TX/1000BASE-T retry:0
      Average:103Mbps/24Gbps Peak:150Mbps at 08:10:30
Port1: active up 1000BASE-T full(auto) 0012.e240.0a04
      Bandwidth:1000000kbps Average out:20Mbps Average in:10Mbps
      description: test lab area network
Port2: active up 1000BASE-T full(auto) 0012.e240.0a05
      Bandwidth:1000000kbps Average out:0Mbps Average in:0Mbps
      description: computer management floor network
Port3: active up 1000BASE-T full(auto) 0012.e240.0a06
      Bandwidth:1000000kbps Average out:2Mbps Average in:1Mbps
```

(省略)

```
>
```

13 省電力機能

この章では、本装置の省電力機能について説明します。

13.1 省電力機能の解説

13.2 省電力機能のコンフィグレーション

13.3 省電力機能のオペレーション

13.1 省電力機能の解説

13.1.1 省電力機能の概要

ネットワークの使用量の増加に備え、収容ポートの帯域を増やしているケースでは、増やしたポート帯域分の電力も消費しています。本装置では、省電力機能によって、不要に消費される電力を抑えられます。

(1) サポートする省電力機能

装置モデルごとの省電力機能サポート一覧を次の表に示します。本装置では、これらの省電力機能を次のように動作させられます。

- 常時動作させる
- スケジューリングによって時間帯を限定して動作させる
- トラフィック量の変化に応じて動作させる

表 13-1 装置モデルごとの省電力機能サポート一覧

省電力機能	AX6708S	AX6604S AX6608S	AX6304S AX6308S
BSU/PSP の電力制御 ¹			×
BSU/PSP・NIF の電力制御 ²			
NIF およびポートの電力供給 OFF			
待機系 BSU/PSP の電力供給 OFF ¹			×
待機系 NIF の電力供給 OFF ³			×
NIF ポートの LED 消灯			
省電力機能のスケジューリング			×
トラフィック量による省電力機能			×

(凡例) : サポート × : 未サポート

注 1

BSU/CSU が 2 枚以上必要です。

注 2

装置の再起動が必要なため、起動が完了するまで本装置を経由する通信が停止します。

注 3

NIF が 2 枚以上必要です。

(2) 目的に応じた省電力機能の選択

省電力機能は、目的に応じて、一つまたは複数の組み合わせで使用します。また、重視する項目によって、選択する省電力機能が決まります。重視する項目を次の三つに分けます。

- 可用性重視
- 通信性能重視
- 消費電力低減重視

重視項目ごとの省電力機能の組み合わせを次の表に示します。

表 13-2 重視項目ごとの省電力機能の組み合わせ【AX6700S】【AX6600S】

重視項目	概要	BSU/ PSP の電力 制御	BSU/ PSP・ NIF の 電力制 御	NIF お よび ポート の電力 供給 OFF	待機系 BSU/ PSP の 電力供 給 OFF	待機系 NIF の 電力供 給 OFF	NIF ポート の LED 消灯
可用性	<ul style="list-style-type: none"> 電力制御のコンフィグレーションを変更する場合でも通信を継続できます。 障害発生時に通信をすぐに回復させます。 		×		×	×	
通信性能	<ul style="list-style-type: none"> 運用系の BSU/PSP の通信性能を維持しながら、使用しない待機系を省電力にすることで消費電力を抑えます。 	×	×	×		×	
消費電力低減	<ul style="list-style-type: none"> 指定した時間帯に応じて、使用していない待機系、NIF、およびポートの電力を OFF にし、大幅に消費電力を抑えます。 電力制御のコンフィグレーションを変更する場合でも通信を継続できます。 		×				
	<ul style="list-style-type: none"> トラフィック量に応じて、使用していない待機系の電力を OFF にし、大幅に消費電力を抑えます。 電力制御のコンフィグレーションを変更する場合でも通信を継続できます。 		×	×		×	
	<ul style="list-style-type: none"> 使用していない待機系、NIF、およびポートの電力を OFF にし、大幅に消費電力を抑えます。 機能の実行には装置の再起動を伴いますが、最大の省電力効果があります。 	×					

(凡例) : 設定可 × : 設定不可

13.1.2 省電力機能【AX6700S】

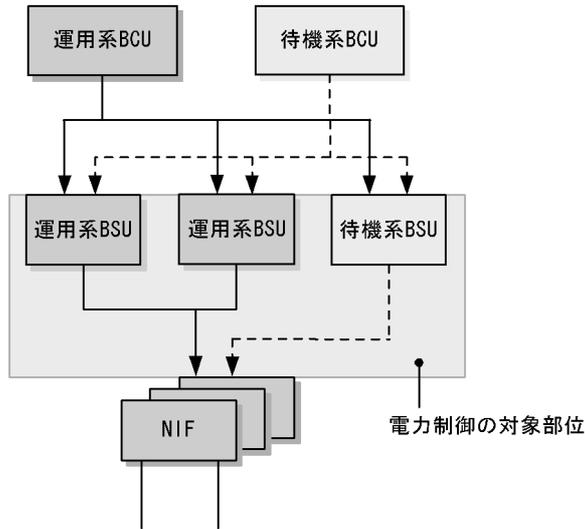
(1) BSU の電力制御

BSU の電力を制御することで、パケット転送で消費する電力を削減できます。この機能は装置単位に設定します。

BSU の電力制御を変更するときは該当 BSU の再起動を伴いますが、通信を継続させるため、運用系 BSU を残しながら待機系 BSU を再起動します。待機系 BSU の変更が完了すると、運用系 BSU と待機系 BSU を切り替え、順番に BSU の電力制御を変更します。これらはすべて自動で動作します。

なお、待機系 BSU の電力制御はホットスタンバイ状態の場合に行います。

図 13-1 BSU の電力制御



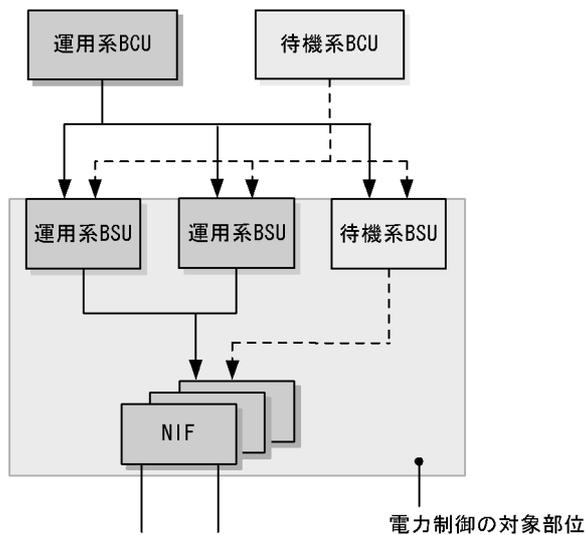
(凡例) —▶ : 運用系通信インターフェース
 - - -▶ : 待機系通信インターフェース

(2) BSU および NIF の電力制御

BSU と NIF の電力を制御することで、パケット転送で消費する電力を削減できます。この機能は装置単位に設定します。電力制御を変更すると、装置を自動で再起動します。再起動が完了するまで本装置を経由する通信が停止します。

なお、待機系 BSU の電力制御はホットスタンバイ状態の場合に行います。

図 13-2 BSU と NIF の電力制御



(凡例) —▶ : 運用系通信インターフェース
 - - -▶ : 待機系通信インターフェース

(3) NIF およびポートの電力供給 OFF

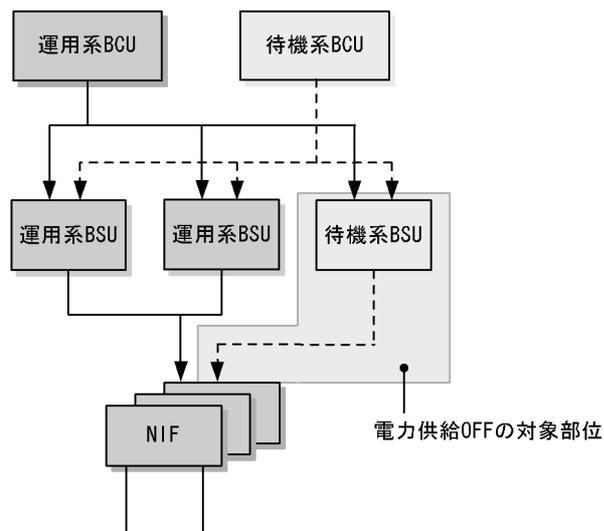
使用していない NIF やポートの電力供給を OFF にすると、消費電力を削減できます。

(4) 待機系 BSU の電力供給 OFF

待機系 BSU の電力供給を OFF にすると、消費電力を削減できます。

- コールドスタンバイ
待機系 BSU の電力供給を部分的に OFF にすることで、待機系 BSU の消費電力を抑えられます。運用系 BSU に障害が発生すると、自動的に待機系 BSU を起動して、系切替をします。系切替には待機系 BSU の起動を伴うため、時間が必要です。
- コールドスタンバイ 2
待機系 BSU の電力供給を完全に OFF にすることで、待機系 BSU の消費電力をほぼ 0 (ゼロ) に抑えられます。運用系 BSU に障害が発生すると、自動的に待機系 BSU を起動して、系切替をします。系切替には待機系 BSU の起動を伴うため、時間が必要です。

図 13-3 待機系 BSU の電力供給 OFF



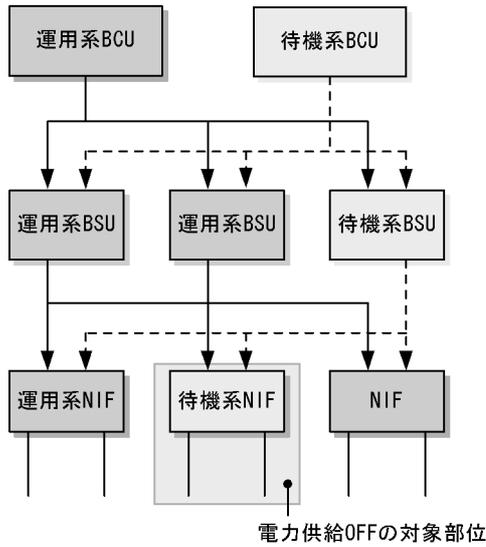
(凡例) —▶ : 運用系通信インターフェース
 ---▶ : 待機系通信インターフェース

(5) 待機系 NIF の電力供給 OFF

待機系 NIF の電力供給を OFF にすると、消費電力を削減できます。

- コールドスタンバイ
待機系 NIF の電力供給を完全に OFF にすることで、待機系 NIF の消費電力をほぼ 0 (ゼロ) に抑えられます。運用系の NIF およびポートに障害が発生すると、自動的に待機系 NIF を起動して、系切替をします。

図 13-4 待機系 NIF の電力供給 OFF



(凡例) —▶ : 運用系通信インターフェース
 - - -▶ : 待機系通信インターフェース

(6) NIF ポートの LED 消灯

NIF ポートの LED をすべて消灯すると、消費電力を削減できます。消灯の対象は次に示す LED です。LED については、マニュアル「ハードウェア取扱説明書」を参照してください。

- LINK/TR LED
- SEL LED

NIF ポートの LED 消灯を設定していても、システム操作パネルの操作キーを操作すると NIF ポートの LED が点灯して、ポートの動作状態を確認できます。なお、点灯した LED は、キー操作のあと 60 秒後に消灯します。

13.1.3 省電力機能【AX6600S】

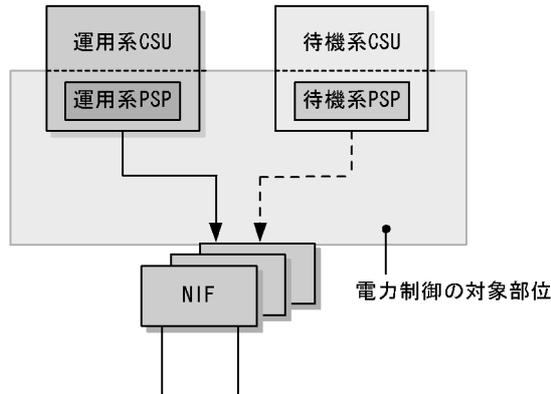
(1) PSP の電力制御

PSP の電力を制御することで、パケット転送で消費する電力を削減できます。この機能は装置単位に設定します。

PSP の電力制御を変更するときは該当 PSP の再起動を伴いますが、通信を継続させるため、運用系 PSP を残しながら待機系 PSP を再起動します。待機系 PSP の変更が完了すると、運用系 PSP と待機系 PSP を切り替え、PSP の電力制御を変更します。これらはすべて自動で動作します。

なお、待機系 PSP の電力制御はホットスタンバイ状態の場合に行います。

図 13-5 PSP の電力制御



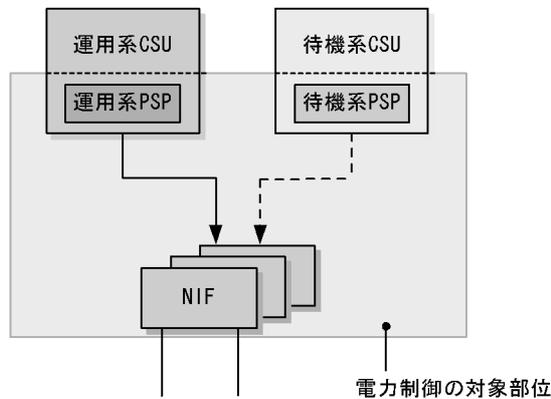
(凡例) —▶ : 運用系通信インターフェース
 ---▶ : 待機系通信インターフェース

(2) PSP および NIF の電力制御

PSP と NIF の電力を制御することで、パケット転送で消費する電力を削減できます。この機能は装置単
 位に設定します。電力制御を変更すると、装置を自動で再起動します。再起動が完了するまで本装置を経
 由する通信が停止します。

なお、待機系 PSP の電力制御はホットスタンバイ状態の場合に行います。

図 13-6 PSP と NIF の電力制御



(凡例) —▶ : 運用系通信インターフェース
 ---▶ : 待機系通信インターフェース

(3) NIF およびポートの電力供給 OFF

使用していない NIF やポートの電力供給を OFF にすると、消費電力を削減できます。

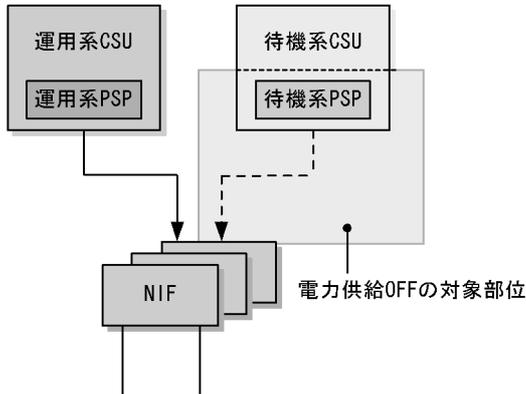
(4) 待機系 PSP の電力供給 OFF

待機系 PSP の電力供給を OFF にすると、消費電力を削減できます。

- コールドスタンバイ 2

待機系 PSP の電力供給を完全に OFF にすることで、待機系 PSP の消費電力をほぼ 0 (ゼロ) に抑えられます。運用系 PSP に障害が発生すると、自動的に待機系 PSP を起動して、系切替をします。系切替には待機系 PSP の起動を伴うため、時間が必要です。

図 13-7 待機系 PSP の電力供給 OFF



(凡例) —▶ : 運用系通信インターフェース
 - - -▶ : 待機系通信インターフェース

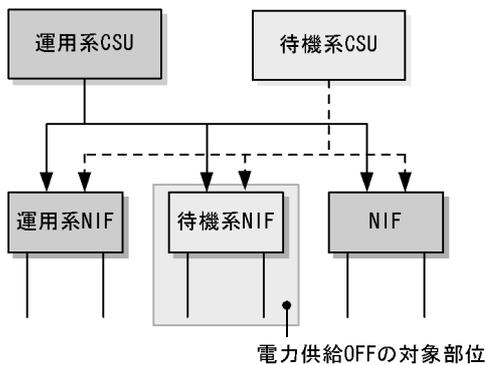
(5) 待機系 NIF の電力供給 OFF

待機系 NIF の電力供給を OFF にすると、消費電力を削減できます。

• コールドスタンバイ

待機系 NIF の電力供給を完全に OFF にすることで、待機系 NIF の消費電力をほぼ 0 (ゼロ) に抑えられます。運用系の NIF およびポートに障害が発生すると、自動的に待機系 NIF を起動して、系切替をします。

図 13-8 待機系 NIF の電力供給 OFF



(凡例) —▶ : 運用系通信インターフェース
 - - -▶ : 待機系通信インターフェース

(6) NIF ポートの LED 消灯

NIF ポートの LED をすべて消灯すると、消費電力を削減できます。消灯の対象は次に示す LED です。LED については、マニュアル「ハードウェア取扱説明書」を参照してください。

- LINK/TR LED
- SEL LED

NIF ポートの LED 消灯を設定していても、システム操作パネルの操作キーを操作すると NIF ポートの LED が点灯して、ポートの動作状態を確認できます。なお、点灯した LED は、キー操作のあと 60 秒後に消灯します。

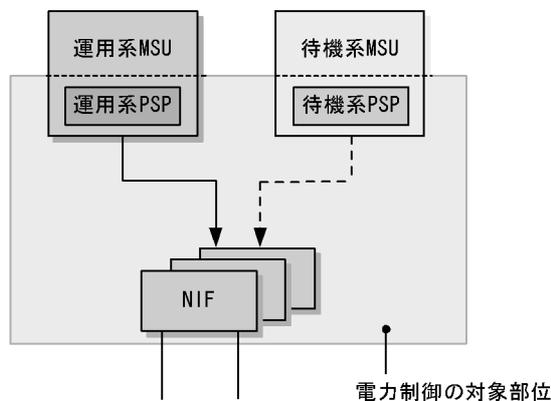
13.1.4 省電力機能【AX6300S】

(1) PSP および NIF の電力制御

PSP と NIF の電力を制御することで、パケット転送で消費する電力を削減できます。この機能は装置単位に設定します。この設定を有効にするためには、コンフィグレーションを保存し、装置を再起動してください。また、装置を再起動する前に、次に示す項目を実施しないでください。

- NIF の再起動
- ソフトウェアアップデート
- 待機系 MSU の再起動および追加起動

図 13-9 PSP と NIF の電力制御



(凡例) —▶ : 運用系通信インターフェース
 ---▶ : 待機系通信インターフェース

なお、初期導入時は無効になっています。

(2) NIF およびポートの電力供給 OFF

使用していない NIF やポートの電力供給を OFF にすると、消費電力を削減できます。

(3) NIF ポートの LED 消灯

NIF ポートの LED をすべて消灯すると、消費電力を削減できます。消灯の対象は次に示す LED です。LED については、マニュアル「ハードウェア取扱説明書」を参照してください。

- LINK/TR LED
- SEL LED

NIF ポートの LED 消灯を設定していても、システム操作パネルの操作キーを操作すると NIF ポートの LED が点灯して、ポートの動作状態を確認できます。なお、点灯した LED は、キー操作のあと 60 秒後に消灯します。

13.1.5 省電力機能のスケジューリング【AX6700S】【AX6600S】

時間帯を指定して省電力機能を実行する場合はスケジューリングをします。スケジューリングでは、実行する省電力機能の組み合わせと実施したい時間帯を指定できます。これらの指定によって、開始時刻になると、自動的に省電力機能が実行されます。また、すでに実行中の省電力機能のある時間帯だけ無効にするスケジューリングもできます。なお、省電力のスケジュールを設定している時間帯をスケジュール時間帯、スケジュールを設定していない時間帯を通常時間帯と呼びます。

(1) スケジュールに指定できる省電力機能

スケジュールは、実行する省電力機能と実施する時間帯で設定します。スケジュールに指定できる省電力機能を次に示します。スケジューリングの際には、これらの機能の中から目的に合わせて一つまたは複数選択し、同時に実行する機能の組み合わせを決めます。

なお、スケジュールで設定できる機能の組み合わせは、装置単位で 1 組だけです。

- BSU/PSP の電力制御
- BSU/PSP，および NIF の電力制御 ¹
- NIF またはポートの電力供給 OFF，またはどちらも電源供給 OFF
- 待機系 BSU/PSP の電力供給 OFF ²
- 待機系 NIF の電力供給 OFF
- NIF ポートの LED 消灯

注 1 装置の再起動を行うため、起動が完了するまで本装置を経由する通信が停止します。

注 2 コールドスタンバイ ² だけ指定できます。

(2) スケジュールの時刻指定方法

省電力で運用する時間帯をスケジュール時間帯として、開始と終了の時刻で指定します。時間帯の指定方法を次に示します。

- 日時に時間帯を指定して省電力にする
- 曜日と時刻で時間帯を指定して省電力にする
- 毎日の時間帯を指定して省電力にする
- 時間帯を指定して省電力スケジュールを無効にする

スケジューリングの際には、これらの指定方法を組み合わせることで設定できるため、さまざまな時間帯で省電力機能を有効にしたり、無効にしたりできます。なお、開始時刻から終了時刻、および終了時刻から開始時刻は、30 分以上の間隔が必要です。

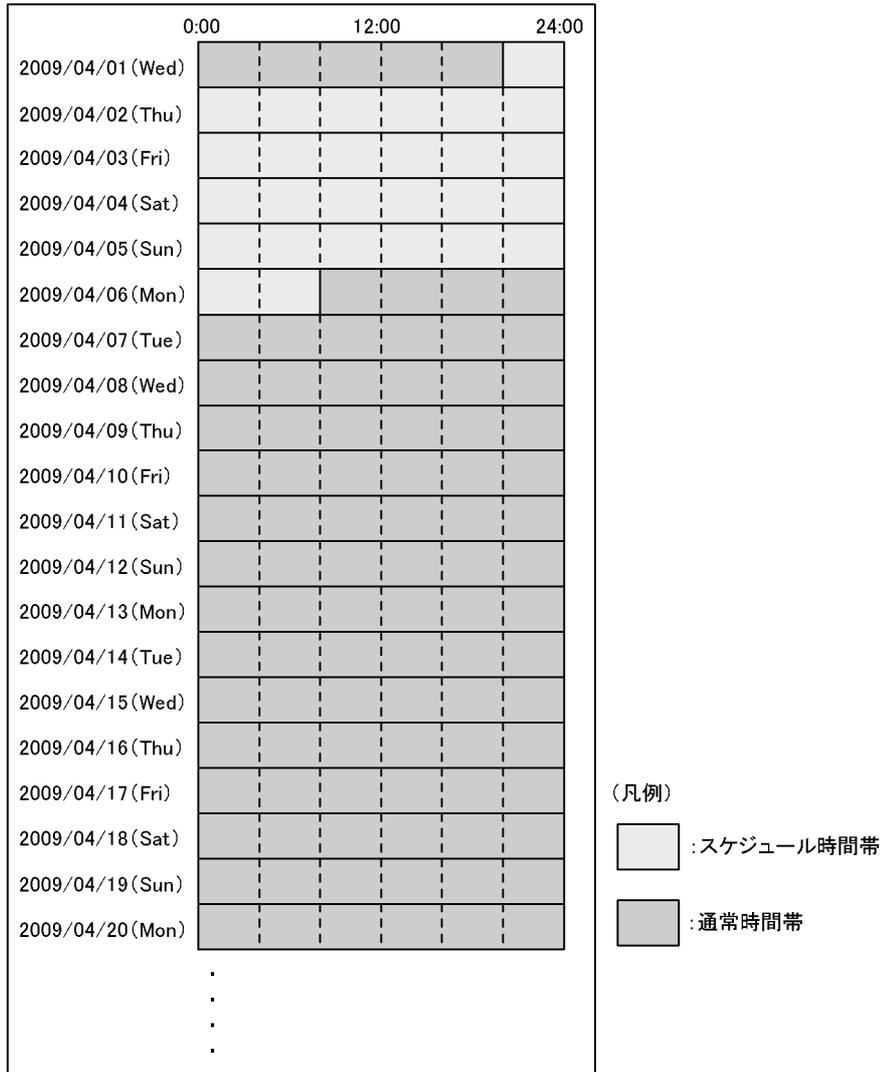
(a) 日時で時間帯を指定して省電力にする

省電力に設定したい，開始と終了の日付および時刻を指定します。

例：

2009年4月2日から5日までは業務システムの稼働が低減します。稼働低減に合わせて，2009年4月1日20時から2009年4月6日8時までを省電力にするスケジュールを指定します。動作スケジュールを次の図に示します。

図 13-10 省電力スケジュール（特定の日付）



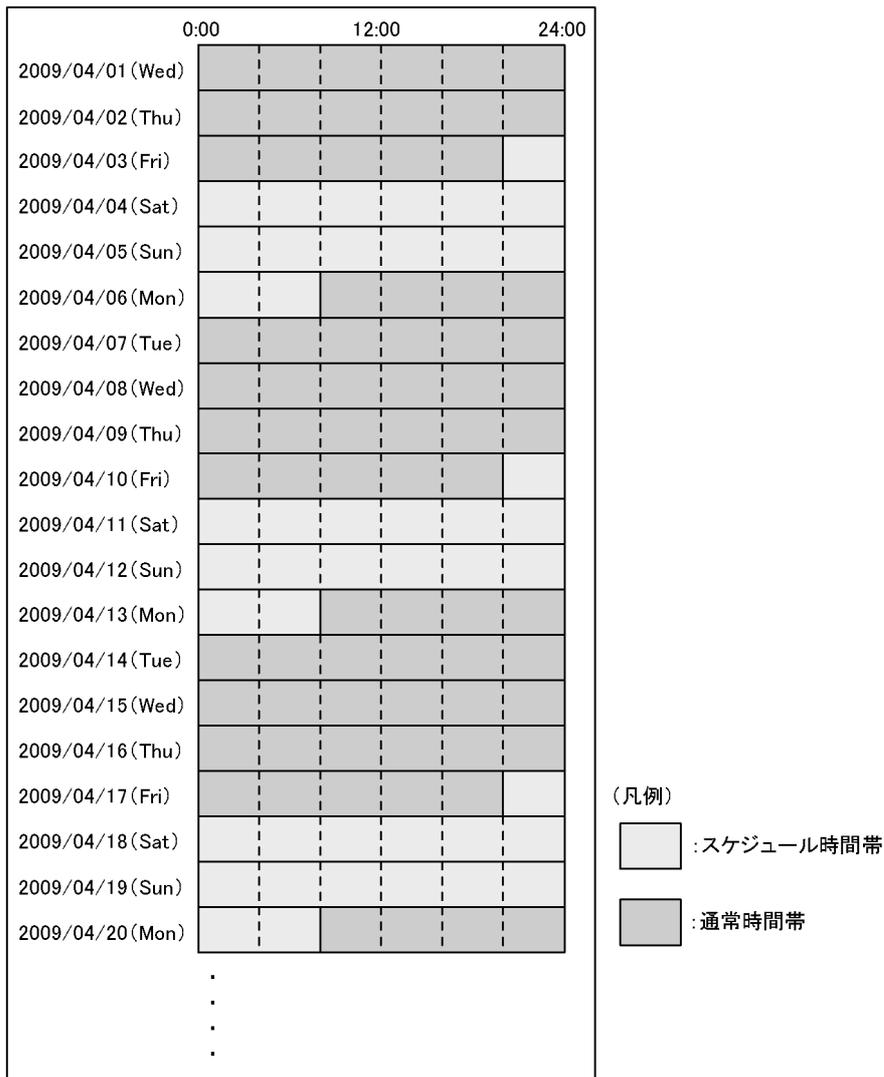
(b) 曜日と時刻で時間帯を指定して省電力にする

省電力に設定したい、開始と終了の曜日および時刻を指定します。

例：

毎週土曜日と日曜日は休日となっていて、その間は業務システムの稼働が低減します。稼働低減に合わせて、毎週金曜日 20 時から毎週月曜日 8 時までを省電力にするスケジュールを指定します。動作スケジュールを次の図に示します。

図 13-11 省電力スケジュール (特定の曜日)



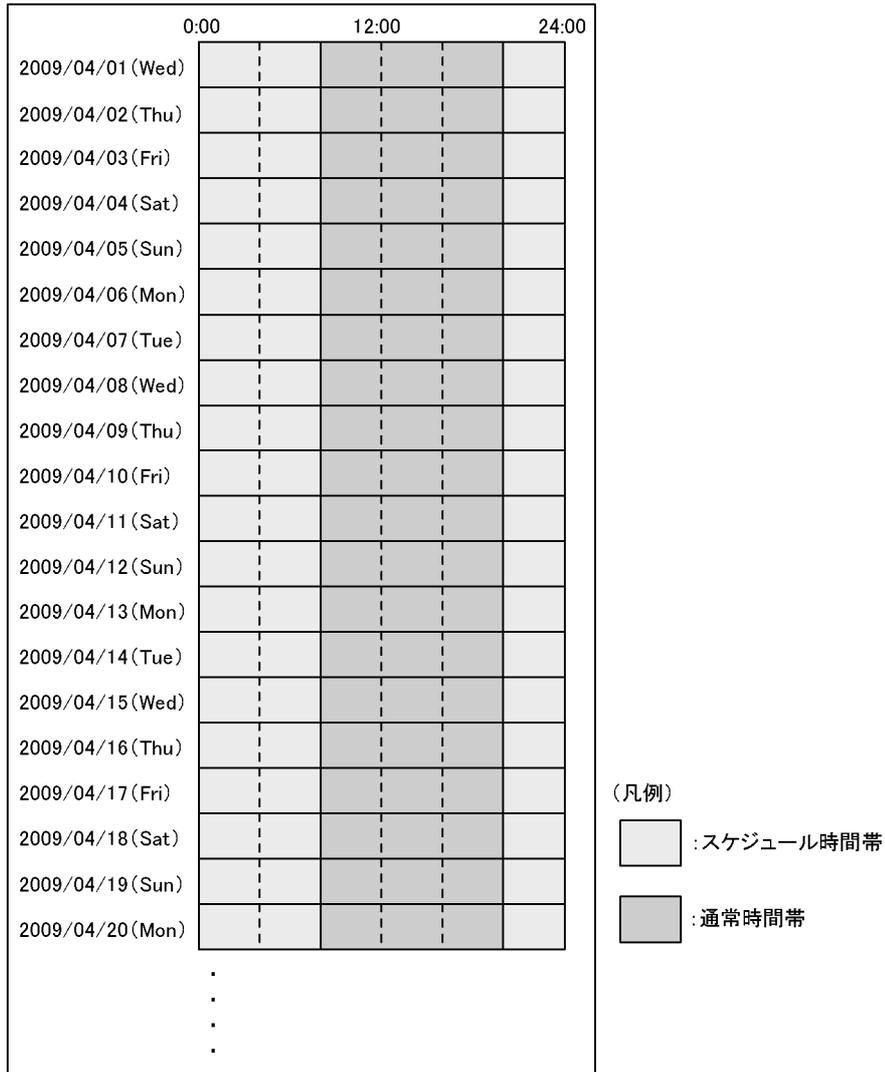
(c) 毎日の時間帯を指定して省電力にする

省電力に設定したい，開始と終了の時刻を指定します。

例：

通常業務は毎日 8 時 30 分から 17 時までとなっているため，業務システムを 8 時から 20 時まで通常の電力で運用します。毎日 20 時から翌日の 8 時までを省電力にするスケジュールを指定します。動作スケジュールを次の図に示します。

図 13-12 省電力スケジュール（毎日）



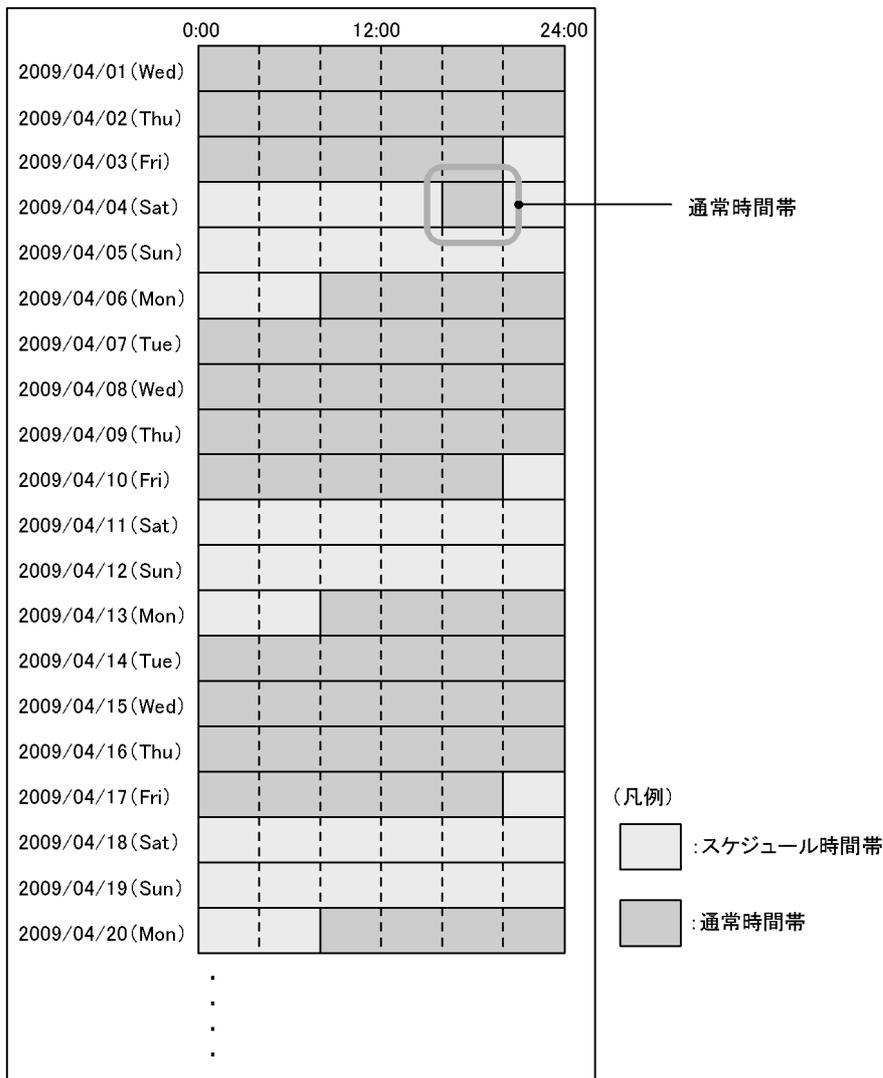
(d) 時間帯を指定して省電力スケジュールを無効にする

すでに省電力機能がスケジュールされている時間帯の、スケジュールの実行を無効にできます。実行を無効にしたい開始と終了の時刻を指定します。特定の日付、特定の曜日、および毎日の特定時間で無効にする時間帯を指定できます。

例：

毎週土曜日と日曜日は休日のため、毎週金曜日 20 時から毎週月曜日 8 時までを省電力にするスケジュールが指定してあります。ただし、業務システムのパッチ処理を行うために 2009 年 4 月 4 日 16 時から 20 時までを通常の電力で運用します。動作スケジュールを次の図に示します。

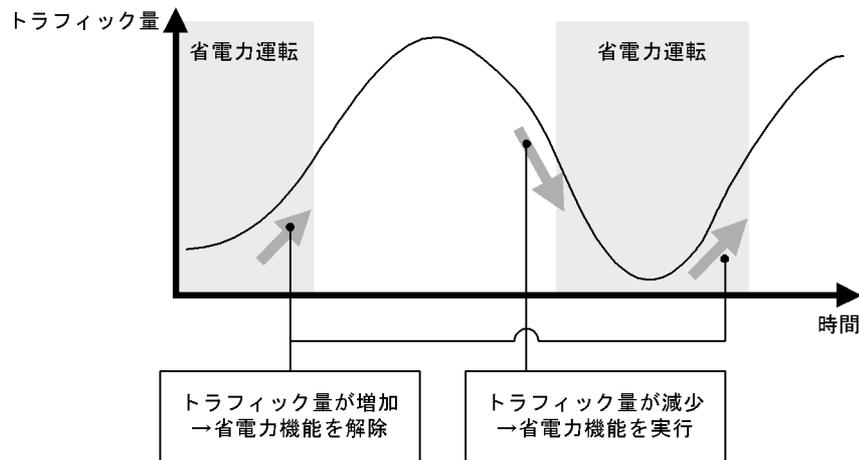
図 13-13 省電力スケジュール（無効設定）



13.1.6 トラフィック量による省電力機能【AX6700S】【AX6600S】

トラフィック量による省電力機能は、本装置を中継するトラフィック量に応じて省電力機能を自動で実行したり解除したりする機能です。本機能では、実行する省電力機能とトラフィック量の監視時間を指定できます。監視時間にトラフィック量の減少が継続した場合は、省電力機能を自動で実行します。トラフィック量の増加が継続した場合は、省電力機能を自動で解除します。

図 13-14 トラフィック量による省電力機能の概念図



(1) 指定できる省電力機能

トラフィック量による省電力機能で指定できる省電力機能を次に示します。これらの機能の中から目的に合わせて一つまたは複数選択し、同時に実行する機能の組み合わせを決めます。

- BSU/PSP の電力制御
- 待機系 BSU/PSP の電力供給 OFF
- NIF ポートの LED 消灯

注 コールドスタンバイ 2 だけ指定できます。

(2) トラフィック量監視時間の指定

トラフィック量の監視時間として、省電力機能が動作するまでの時間と解除するまでの時間をそれぞれ指定できます。指定がない場合、省電力機能が動作するまでの時間は 60 分、解除するまでの時間は 1 分となります。

13.1.7 省電力機能に関する注意事項

(1) BSU/PSP の電力制御機能に関する注意事項【AX6700S】【AX6600S】

- BSU/PSP の電力制御を変更する場合には、BSU/PSP を冗長構成にしてください。
BSU/PSP を順番に再起動して電力制御を変更するため、すべての BSU/PSP を運用系として使用している場合、一時的にパケット転送性能が低下します。1 枚以上を待機系として使用している場合、変更中もパケット転送性能を維持します。また、稼働している BSU/PSP が 1 枚の状態では電力制御機能を使用すると、装置を再起動します。
- BSU/PSP の電力制御の変更中は、次に示す項目に注意してください。

表 13-3 BSU/PSP の電力制御設定に関する注意事項

項目	注意事項
機能の設定変更	BSU/PSP の電力制御の変更中は、次に示す機能の設定を追加・変更・削除しないでください。 <ul style="list-style-type: none"> • 省電力機能 • 省電力スケジュール • 帯域監視機能 • ストームコントロール

項目	注意事項
運用コマンドの入力	BSU/PSP の電力制御の変更中は、次に示す運用コマンドは入力できません。 <ul style="list-style-type: none"> • redundancy force-switchover
系切替【AX6700S】	BSU の電力制御の変更中、ACH スイッチを押した場合または BCU 障害による系切替が発生した場合、ストームコントロール機能の受信帯域の閾値が一時的に 2 倍または 1/2 倍になります。

(2) スケジューリングを使用した省電力機能に関する注意事項【AX6700S】【AX6600S】

- スケジューリングを使用した省電力機能は、次に示すコンフィグレーションがどれも設定されていない場合に設定できます。
 - adaptive-power-control enable
 - redundancy bsu-load-balancing smac
 - redundancy bsu-mode fixed
 - redundancy standby-bsu cold
- 通常時間帯とスケジュール時間帯で同じ省電力機能を使用する場合は、通常時間帯とスケジュール時間帯の両方にその設定をしてください。

例

通常時間帯で NIF の電力供給を OFF にするために、コンフィグレーションコマンド `no power enable` を設定します。スケジュール時間帯でも NIF の電力供給を OFF にする場合は、コンフィグレーションコマンド `schedule-power-control shutdown` を設定してください。

- スケジューリングを使用した省電力機能で、BSU/PSP の電力制御を変更する場合、BSU/PSP を冗長構成にしてください。稼働している BSU/PSP 数が 1 の場合、スケジュール開始時刻および終了時刻になっても、BSU/PSP の電力制御を変更できません。
- スケジュールに指定した省電力機能に BSU/PSP の電力制御機能が含まれる場合、すべての省電力機能の設定が反映されるまでに、最大 30 分の時間が掛かります。スケジュール時間帯を指定するときは、反映に掛かる時間を考慮して開始時刻および完了時刻を指定してください。なお、コンフィグレーションの反映中は通信が継続されます。

(3) トラフィック量による省電力機能に関する注意事項【AX6700S】【AX6600S】

- 本機能は、次に示すコンフィグレーションがどれも設定されていない場合に設定できます。
 - power-control mode1
 - redundancy bsu-load-balancing smac
 - redundancy bsu-mode fixed
 - redundancy standby-bsu cold
 - schedule-power-control time-range
- トラフィック量による省電力機能で BSU/PSP の電力制御を変更する場合、BSU/PSP を冗長構成にしてください。稼働している BSU/PSP 数が 1 の場合、トラフィック量による省電力機能が実行または解除されても、BSU/PSP の電力制御を変更できません。
- 省電力機能を頻繁に実行させたくない場合は、省電力機能が動作するまでの時間を長く設定してください。
- トラフィック量の変化に即時に対応するためには、省電力機能を解除するまでの時間を設定しないでください。

13.2 省電力機能のコンフィグレーション

13.2.1 コンフィグレーションコマンド一覧

省電力機能のコンフィグレーションコマンド一覧を次の表に示します。

表 13-4 コンフィグレーションコマンド一覧【AX6700S】

コマンド名			説明
通常時間帯への 設定コマンド	スケジュール時間帯 への設定コマンド	トラフィック量による 省電力機能への 設定コマンド	
power enable ¹	schedule-power-control shutdown	-	NIF への電力供給を OFF に します。
power-control	schedule-power-control mode	adaptive-power-control mode	電力制御を設定します。
redundancy max-bsu ²	schedule-power-control max-bsu	adaptive-power-control max-bsu	運用系として稼働する BSU 数を設定します。
redundancy standby-bsu ²	schedule-power-control standby-bsu	adaptive-power-control standby-bsu	待機系の BSU モードを設定 します。
redundancy nif-group max-standby-nif ³	schedule-power-control redundancy nif-group max-standby-nif	-	待機系として稼働する NIF 数を設定します。
redundancy nif-group nif priority ³	-	-	NIF 冗長グループを指定し て、グループに所属する NIF およびグループ内での 該当 NIF の優先度を設定し ます。
shutdown ⁴	schedule-power-control shutdown	-	ポートへの電力供給を OFF に設定します。
system port-led	schedule-power-control port-led	adaptive-power-control port-led	NIF ポートの LED 動作を 設定します。
-	schedule-power-control time-range	-	省電力スケジュールの時間 帯を指定します。
-	-	adaptive-power-control decrease-traffic-debounce	トラフィック量による省電 力機能によって、省電力機 能が動作するまでの監視時 間を設定します。
-	-	adaptive-power-control increase-traffic-debounce	トラフィック量による省電 力機能によって動作した省 電力機能を解除するまでの 監視時間を設定します。
-	-	adaptive-power-control enable	トラフィック量による省電 力機能を有効にします。

(凡例) - : 該当なし

注 1

「コンフィグレーションコマンドレファレンス Vol.1 10. BSU/NIF の管理」を参照してください。

注 2

「コンフィグレーションコマンドレファレンス Vol.2 15. BSU の冗長化【AX6700S】」を参照してください。

注 3

13. 省電力機能

「コンフィグレーションコマンドレファレンス Vol.2 17. NIF 冗長制御【AX6700S】【AX6600S】」を参照してください。

注 4

「コンフィグレーションコマンドレファレンス Vol.1 12. イーサネット」を参照してください。

表 13-5 コンフィグレーションコマンド一覧【AX6600S】

コマンド名			説明
通常時間帯への 設定コマンド	スケジュール時間帯 への設定コマンド	トラフィック量による 省電力機能への 設定コマンド	
power enable ¹	schedule-power-control shutdown	-	NIF への電力供給を OFF に します。
power-control	schedule-power-control mode	adaptive-power-control mode	電力制御を設定します。
redundancy max-ppsp ²	schedule-power-control max-ppsp	adaptive-power-control max-ppsp	運用系として稼働する PSP 数を設定します。
redundancy standby-ppsp ²	schedule-power-control standby-ppsp	adaptive-power-control standby-ppsp	待機系の PSP モードを設定 します。
redundancy nif-group max-standby-nif ³	schedule-power-control redundancy nif-group max-standby-nif	-	待機系として稼働する NIF 数を設定します。
redundancy nif-group nif priority ³	-	-	NIF 冗長グループを指定し て、グループに所属する NIF およびグループ内での 該当 NIF の優先度を設定し ます。
shutdown ⁴	schedule-power-control shutdown	-	ポートへの電力供給を OFF に設定します。
system port-led	schedule-power-control port-led	adaptive-power-control port-led	NIF ポートの LED 動作を 設定します。
-	schedule-power-control time-range	-	省電力スケジュールの時間 帯を指定します。
-	-	adaptive-power-control decrease-traffic-debounce	トラフィック量による省電 力機能によって、省電力機 能が動作するまでの監視時 間を設定します。
-	-	adaptive-power-control increase-traffic-debounce	トラフィック量による省電 力機能によって動作した省 電力機能を解除するまでの 監視時間を設定します。
-	-	adaptive-power-control enable	トラフィック量による省電 力機能を有効にします。

(凡例) - : 該当なし

注 1

「コンフィグレーションコマンドレファレンス Vol.1 10. BSU/NIF の管理」を参照してください。

注 2

「コンフィグレーションコマンドレファレンス Vol.2 16. PSP の冗長化【AX6600S】」を参照してください。

注 3

「コンフィグレーションコマンドレファレンス Vol.2 17. NIF 冗長制御【AX6700S】【AX6600S】」を参照してくだ
さい。

注 4

「コンフィグレーションコマンドレファレンス Vol.1 12. イーサネット」を参照してください。

表 13-6 コンフィグレーションコマンド一覧【AX6300S】

コマンド名	説明
通常時間帯への設定コマンド	
power enable ¹	NIF への電力供給を OFF にします。
power-control	電力制御を設定します。
shutdown ²	ポートへの電力供給を OFF に設定します。
system port-led	NIF ポートの LED 動作を設定します。

注 1

「コンフィグレーションコマンドレファレンス Vol.1 10. BSU/NIF の管理」を参照してください。

注 2

「コンフィグレーションコマンドレファレンス Vol.1 12. イーサネット」を参照してください。

13.2.2 コンフィグレーションコマンド設定例【AX6700S】

コンフィグレーションコマンドの設定例を次に示します。

(1) 可用性を重視した設定

[設定のポイント]

待機系 BSU をホットスタンバイ状態にして、障害発生時にすぐに通信を回復させます。BSU の電力制御で低電力、NIF ポートの LED 消灯、未使用 NIF の電力供給 OFF を設定して、消費電力を抑えます。

コンフィグレーションの設定前の運用状態と、設定後の運用状態を次の表に示します。

表 13-7 可用性重視のコンフィグレーション設定例

項目	設定前の運用状態	設定後の運用状態
運用系 BSU 数	2	2
待機系 BSU 数	1	1
電力制御	通常電力	BSU 低電力
NIF およびポートの電力供給	ON	OFF
待機系 BSU の電力供給	ON	ON
待機系 NIF の電力供給	ON	ON
NIF ポートの LED	点灯	消灯

[コマンドによる設定]

- (config)# system port-led disable
NIF ポートの LED を消灯に設定します。
- (config)# no power enable nif 1
未使用 NIF の電力供給を OFF にします。

3. (config)# power-control mode mode2

BSU and NIF might be restarted automatically when the mode is changed.

Do you wish to change mode (y/n):

BSU の電力制御で低電力を設定して、消費電力を抑えます。

(2) 通信性能を重視した設定

[設定のポイント]

待機系 BSU の電力供給 OFF, NIF ポートの LED 消灯を設定して、消費電力を低減します。BSU の電力制御をしないで、通信性能を維持します。

コンフィギュレーションの設定前の運用状態と、設定後の運用状態を次の表に示します。

表 13-8 通信性能重視のコンフィギュレーション設定例

項目	設定前の運用状態	設定後の運用状態
運用系 BSU 数	2	2
待機系 BSU 数	1	1
電力制御	通常電力	通常電力
NIF およびポートの電力供給	ON	ON
待機系 BSU の電力供給	ON	OFF
待機系 NIF の電力供給	ON	ON
NIF ポートの LED	点灯	消灯

[コマンドによる設定]

1. (config)# system port-led disable

NIF ポートの LED を消灯に設定します。

2. (config)# redundancy standby-bsu cold2

待機系 BSU をコールドスタンバイ 2 に指定して、電力供給を OFF にします。

(3) 消費電力低減を重視したスケジュールの設定

[設定のポイント]

BSU の電力制御で低電力を設定して、消費電力を抑えます。さらに、待機系 BSU の電力供給 OFF, 待機系 NIF の電力供給 OFF, NIF ポートの LED 消灯, 未使用 NIF の電力供給 OFF を設定して、消費電力を低減します。

コンフィギュレーションの設定前の運用状態と、設定後の運用状態を次の表に示します。

表 13-9 消費電力低減重視のコンフィギュレーション設定例

項目	設定前の運用状態	設定後の運用状態
運用系 BSU 数	2	1
待機系 BSU 数	1	2
電力制御	通常電力	BSU 低電力
NIF およびポートの電力供給	ON	OFF
待機系 BSU の電力供給	ON	OFF

項目	設定前の運用状態	設定後の運用状態
待機系 NIF の電力供給	ON	OFF
NIF ポートの LED	点灯	消灯

[コマンドによる設定]

- ```
(config)# schedule-power-control port-led disable
(config)# schedule-power-control shutdown nif 3
(config)# schedule-power-control redundancy nif-group 1 max-standby-nif 1
(config)# redundancy nif-group 1 nif 1 priority 1
(config)# redundancy nif-group 1 nif 2 priority 2
(config)# schedule-power-control mode mode2
(config)# schedule-power-control max-bsu 1
(config)# schedule-power-control standby-bsu cold2
```

スケジュール時間帯に設定する省電力機能を指定します。ここでは NIF ポートの LED 消灯、未使用 NIF の電力供給 OFF、待機系 NIF コールドスタンバイ、BSU の電力制御で低電力、運用系 BSU 数 1 枚、待機系 BSU コールドスタンバイ 2 を指定します。
- ```
(config)# schedule-power-control time-range 1 weekly start-time fri 2000
end-time mon 0800 action enable
```

毎週金曜日 20 時から毎週月曜日 8 時まで動作するスケジュールを指定します。
- ```
(config)# schedule-power-control time-range 2 date start-time 090404 1600
end-time 090404 2000 action disable
```

2009 年 4 月 4 日 16 時から 20 時までの時間帯は省電力スケジュールの実行を無効にする指定をします。

## (4) 消費電力低減を重視したトラフィック量による省電力機能の設定

## [ 設定のポイント ]

BSU の電力制御で低電力を設定して、消費電力を抑えます。さらに、待機系 BSU の電力供給 OFF、NIF ポートの LED 消灯を設定して、消費電力を低減します。

コンフィギュレーションの設定前の運用状態と、設定後の運用状態を次の表に示します。

表 13-10 消費電力低減重視のコンフィギュレーション設定例 (トラフィック量による省電力機能)

| 項目              | 設定前の運用状態 | 設定後の運用状態 |
|-----------------|----------|----------|
| 運用系 BSU 数       | 2        | 1        |
| 待機系 BSU 数       | 1        | 2        |
| 電力制御            | 通常電力     | BSU 低電力  |
| NIF およびポートの電力供給 | ON       | ON       |
| 待機系 BSU の電力供給   | ON       | OFF      |
| 待機系 NIF の電力供給   | ON       | ON       |
| NIF ポートの LED    | 点灯       | 消灯       |

## [ コマンドによる設定 ]

1. `(config)# adaptive-power-control enable`  
トラフィック量による省電力機能を有効にします。

### 13.2.3 コンフィグレーションコマンド設定例【AX6600S】

コンフィグレーションコマンドの設定例を次に示します。

#### (1) 可用性を重視した設定

##### [ 設定のポイント ]

待機系 PSP をホットスタンバイ状態にして、障害発生時にすぐに通信を回復させます。PSP の電力制御で低電力、NIF ポートの LED 消灯、未使用 NIF の電力供給 OFF を設定して、消費電力を抑えます。

コンフィグレーションの設定前の運用状態と、設定後の運用状態を次の表に示します。

表 13-11 可用性重視のコンフィグレーション設定例

| 項目              | 設定前の運用状態 | 設定後の運用状態 |
|-----------------|----------|----------|
| 運用系 PSP 数       | 1        | 1        |
| 待機系 PSP 数       | 1        | 1        |
| 電力制御            | 通常電力     | PSP 低電力  |
| NIF およびポートの電力供給 | ON       | OFF      |
| 待機系 PSP の電力供給   | ON       | ON       |
| 待機系 NIF の電力供給   | ON       | ON       |
| NIF ポートの LED    | 点灯       | 消灯       |

##### [ コマンドによる設定 ]

1. `(config)# system port-led disable`  
NIF ポートの LED を消灯に設定します。
2. `(config)# no power enable nif 1`  
未使用 NIF の電力供給を OFF にします。
3. `(config)# power-control mode mode2`  
PSP and NIF might be restarted automatically when the mode is changed.  
Do you wish to change mode (y/n):  
PSP の電力制御で低電力を設定して、消費電力を抑えます。

#### (2) 通信性能を重視した設定

##### [ 設定のポイント ]

待機系 PSP の電力供給 OFF、NIF ポートの LED 消灯を設定して、消費電力を低減します。PSP の電力制御をしないで、通信性能を維持します。

コンフィグレーションの設定前の運用状態と、設定後の運用状態を次の表に示します。

表 13-12 通信性能重視のコンフィグレーション設定例

| 項目              | 設定前の運用状態 | 設定後の運用状態 |
|-----------------|----------|----------|
| 運用系 PSP 数       | 1        | 1        |
| 待機系 PSP 数       | 1        | 1        |
| 電力制御            | 通常電力     | 通常電力     |
| NIF およびポートの電力供給 | ON       | ON       |
| 待機系 PSP の電力供給   | ON       | OFF      |
| 待機系 NIF の電力供給   | ON       | ON       |
| NIF ポートの LED    | 点灯       | 消灯       |

## [ コマンドによる設定 ]

1. `(config)# system port-led disable`  
NIF ポートの LED を消灯に設定します。
2. `(config)# redundancy standby-bsp cold2`  
待機系 PSP をコールドスタンバイ 2 に指定して、電力供給を OFF にします。

## (3) 消費電力低減を重視したスケジュールの設定

## [ 設定のポイント ]

PSP の電力制御で低電力を設定して、消費電力を抑えます。さらに、待機系 PSP の電力供給 OFF、NIF ポートの LED 消灯、未使用 NIF の電力供給 OFF、待機系 NIF の電力供給 OFF を設定して、消費電力を低減します。

コンフィグレーションの設定前の運用状態と、設定後の運用状態を次の表に示します。

表 13-13 消費電力低減重視のコンフィグレーション設定例

| 項目              | 設定前の運用状態 | 設定後の運用状態 |
|-----------------|----------|----------|
| 運用系 PSP 数       | 1        | 1        |
| 待機系 PSP 数       | 1        | 1        |
| 電力制御            | 通常電力     | PSP 低電力  |
| NIF およびポートの電力供給 | ON       | OFF      |
| 待機系 PSP の電力供給   | ON       | OFF      |
| 待機系 NIF の電力供給   | ON       | OFF      |
| NIF ポートの LED    | 点灯       | 消灯       |

## [ コマンドによる設定 ]

1. `(config)# schedule-power-control port-led disable`  
`(config)# schedule-power-control shutdown nif 3`  
`(config)# schedule-power-control redundancy nif-group 1 max-standby-nif 1`  
`(config)# redundancy nif-group 1 nif 1 priority 1`  
`(config)# redundancy nif-group 1 nif 2 priority 2`  
`(config)# schedule-power-control mode mode2`  
`(config)# schedule-power-control max-bsp 1`

```
(config)# schedule-power-control standby-psp cold2
```

スケジュール時間帯に設定する省電力機能を指定します。ここでは NIF ポートの LED 消灯，未使用 NIF の電力供給 OFF，待機系 NIF コールドスタンバイ，PSP の電力制御を低電力，運用系 PSP 数一つ，待機系 PSP コールドスタンバイ 2 を指定します。

```
2. (config)# schedule-power-control time-range 1 weekly start-time fri 2000
end-time mon 0800 action enable
```

毎週金曜日 20 時から毎週月曜日 8 時まで動作するスケジュールを指定します。

```
3. (config)# schedule-power-control time-range 2 date start-time 090404 1600
end-time 090404 2000 action disable
```

2009 年 4 月 4 日 16 時から 20 時までの時間帯は省電力スケジュールの実行を無効にする指定をします。

#### (4) 消費電力低減を重視したトラフィック量による省電力機能の設定

##### [ 設定のポイント ]

PSP の電力制御で低電力を設定して，消費電力を抑えます。さらに，待機系 PSP の電力供給 OFF，NIF ポートの LED 消灯を設定して，消費電力を低減します。

コンフィグレーションの設定前の運用状態と，設定後の運用状態を次の表に示します。

表 13-14 消費電力低減重視のコンフィグレーション設定例（トラフィック量による省電力機能）

| 項目              | 設定前の運用状態 | 設定後の運用状態 |
|-----------------|----------|----------|
| 運用系 PSP 数       | 1        | 1        |
| 待機系 PSP 数       | 1        | 1        |
| 電力制御            | 通常電力     | PSP 低電力  |
| NIF およびポートの電力供給 | ON       | ON       |
| 待機系 PSP の電力供給   | ON       | OFF      |
| 待機系 NIF の電力供給   | ON       | ON       |
| NIF ポートの LED    | 点灯       | 消灯       |

##### [ コマンドによる設定 ]

```
1. (config)# adaptive-power-control enable
```

トラフィック量による省電力機能を有効にします。

### 13.2.4 コンフィグレーションコマンド設定例【AX6300S】

コンフィグレーションコマンドの設定例を次に示します。

##### [ 設定のポイント ]

電力制御を装置単位に有効にします。また，NIF ポートの LED を消灯します。

コンフィグレーションの設定前の運用状態と，設定後の運用状態を次の表に示します。

表 13-15 消費電力低減重視のコンフィグレーション設定例

| 項目              | 設定前の運用状態 | 設定後の運用状態    |
|-----------------|----------|-------------|
| 運用系 PSP 数       | 1        | 1           |
| 待機系 PSP 数       | 1        | 1           |
| 電力制御            | 通常電力     | PSP・NIF 低電力 |
| NIF およびポートの電力供給 | ON       | ON          |
| 待機系 PSP の電力供給   | ON       | ON          |
| 待機系 NIF の電力供給   | ON       | ON          |
| NIF ポートの LED    | 点灯       | 消灯          |

## [ コマンドによる設定 ]

1. `(config)# system port-led disable`  
NIF ポートの LED を消灯に設定します。
2. `(config)# power-control`  
電力制御を装置単位に有効にします。
3. `(config)# save`  
`(config)# exit`  
保存して、コンフィグレーションモードから装置管理者モードに移行します。
4. `# reload`  
本装置を再起動します。再起動によって電力制御のコンフィグレーションが有効になります。





図 13-19 省電力機能使用時の電力情報の確認

```
>show power
Date 2010/04/13 13:00:00 UTC
Elapsed time 2Days 04:25
H/W Wattage Accumulated Wattage Power-Status Status
Chassis 56.00 W 2.91 kWh - active
BCU1 42.00 W 2.18 kWh - active
BCU2 42.00 W 2.18 kWh - standby
BSU1 268.00 W 16.49 kWh saving active
BSU2 268.00 W 16.49 kWh saving active
BSU3 0.00 W 16.32 kWh - standby cold2
NIF1 118.00 W 6.14 kWh normal active
NIF2 118.00 W 6.14 kWh normal active
NIF3 109.00 W 5.67 kWh normal active
NIF4 108.00 W 5.62 kWh normal active
NIF5 0.00 W 7.34 kWh - inactive
NIF6 0.00 W 7.34 kWh - inactive
NIF7 0.00 W 5.56 kWh - inactive
NIF8 0.00 W 5.51 kWh - inactive
Total 1129.00 W 105.89 kWh
```

## (2) トラフィック情報の確認

運用コマンド show engine-traffic statistics で、転送エンジンを経由するトラフィックの情報を確認できます。次の図に例を示します。

図 13-20 トラフィック情報の確認【AX6700S】

```
> show engine-traffic statistics average-bps
Date 2010/03/01 12:00:00 UTC
 BSU/Forwarding Engine
 1/1 1/2 2/1 2/2 3/1 3/2 total
Average bps
Mar 01 11:00
 Inbound 17.5G 18.5G 20.0G 17.5G 0.0G 0.0G 73.5G
 Outbound 17.5G 18.5G 20.0G 17.5G 0.0G 0.0G 73.5G
 :
 :
Mar 01 11:59
 Inbound 17.0G 18.0G 21.0G 17.0G 0.0G 0.0G 73.0G
 Outbound 17.0G 18.0G 21.0G 17.0G 0.0G 0.0G 73.0G
```

図 13-21 トラフィック情報の確認【AX6600S】

```
> show engine-traffic statistics average-bps
Date 2010/03/01 12:00:00 UTC
 PSP/Forwarding Engine
 1/1 2/1 total
Average bps
Mar 01 11:00
 Inbound 17.5G 18.5G 36.0G
 Outbound 17.5G 18.5G 36.0G
 :
 :
Mar 01 11:59
 Inbound 17.0G 18.0G 35.0G
 Outbound 17.0G 18.0G 35.0G
```

図 13-22 トラフィック情報の確認【AX6300S】

```
> show engine-traffic statistics average-bps
Date 2010/03/01 12:00:00 UTC
 PSP/Forwarding Engine
 1/1 2/1 total
Average bps
Mar 01 11:00
 Inbound 17.5G 0.0G 17.5G
 Outbound 17.5G 0.0G 17.5G
 :
 :
Mar 01 11:59
 Inbound 17.0G 0.0G 17.0G
 Outbound 17.0G 0.0G 17.0G
```



# 14 ソフトウェアの管理

この章では、ソフトウェアのアップデートについて説明します。実際のアップデート手順については、「ソフトウェアアップデートガイド」を参照してください。

---

14.1 運用コマンド一覧

---

14.2 ソフトウェアのアップデート

---

14.3 無停止ソフトウェアアップデート

---

14.4 オプションライセンスの設定

---

## 14.1 運用コマンド一覧

---

ソフトウェア管理に関する運用コマンド一覧を次の表に示します。

表 14-1 運用コマンド一覧

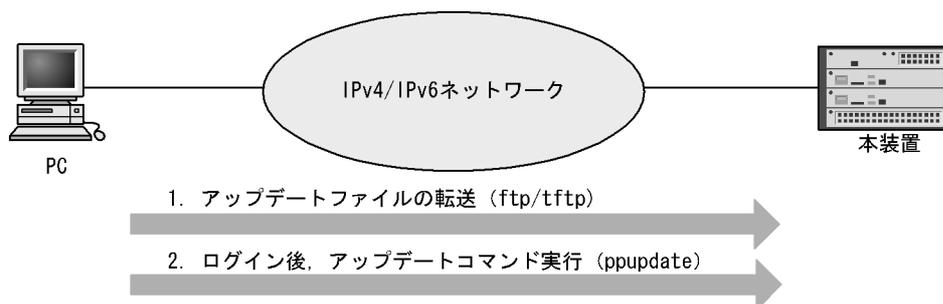
| コマンド名         | 説明                                       |
|---------------|------------------------------------------|
| ppupdate      | ftp, tftp などダウンロードした新しいソフトウェアにアップデートします。 |
| set license   | 購入したオプションライセンスを設定します。                    |
| show license  | 認証しているオプションライセンスを表示します。                  |
| erase license | 指定したオプションライセンスを削除します。                    |

## 14.2 ソフトウェアのアップデート

ソフトウェアのアップデートとは、旧バージョンのソフトウェアから新バージョンのソフトウェアにバージョンアップすることを指します。ソフトウェアのアップデートは、PCなどのリモート運用端末からアップデートファイルの本装置に転送し、運用コマンド `ppupdate` を実行することで実現します。アップデート時、装置管理のコンフィグレーションおよびユーザ情報（ログインアカウント、パスワードなど）はそのまま引き継がれます。詳細については、「ソフトウェアアップデートガイド」を参照してください。

ソフトウェアのアップデートの概要を次の図に示します。

図 14-1 ソフトウェアのアップデートの概要



## 14.3 無停止ソフトウェアアップデート

### 14.3.1 概要

無停止ソフトウェアアップデートは、通信を中断しないで BCU, BSU, CSU または MSU の二重化構成で系切替をしながら、運用系および待機系それぞれのソフトウェアをアップデートする機能です。系切替の間にルーティングテーブルなどを保持し続け、アップデート作業中の通信を維持します。

ソフトウェアのバージョンアップ・バージョンダウン共に通信無停止でアップデートができます。

### 14.3.2 無停止ソフトウェアアップデートの適用条件

無停止ソフトウェアアップデートを行うための条件を次の表に示します。

表 14-2 無停止ソフトウェアアップデートの適用条件

| 項目          | 適用条件                                                                                                                                                                                                                                                                                    |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 装置構成        | <ul style="list-style-type: none"> <li>AX6700S の場合<br/>BCU の二重化構成であること<br/>BSU を 2 枚以上実装していること</li> <li>AX6600S の場合<br/>CSU の二重化構成であること</li> <li>AX6300S の場合<br/>MSU の二重化構成であること</li> </ul> <p>バージョンダウンの場合、アップデート後のソフトウェアバージョンで未サポートのハードウェア（例えば、BCU, BSU, CSU, MSU, NIF）を使用していないこと。</p> |
| サポート機能      | <p>通信無停止の系切替をサポートしている機能を使用していること。詳しくは、マニュアル「コンフィグレーションガイド Vol.2 17.1.5 系切替時の通信無停止対応機能一覧」を参照してください。</p> <p>バージョンダウンの場合、アップデート後のソフトウェアで未サポートの機能を使用していないこと。</p>                                                                                                                            |
| ソフトウェアバージョン | <ul style="list-style-type: none"> <li>AX6700S および AX6300S の場合<br/>Ver.10.3.C 以降であること。アップデート前、アップデート後ともに Ver.10.3.C 以降である必要があります。</li> <li>AX6600S の場合<br/>Ver.11.1 以降であること。アップデート前、アップデート後ともに Ver.11.1 以降である必要があります。</li> </ul> <p>アップデート作業前に、運用系、待機系ともに同じバージョンのソフトウェアで動作していること。</p>   |
| コンフィグレーション  | <p>ランニング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が一致している状態であること。</p> <p>運用系システムと待機系システムのスタートアップコンフィグレーションが一致している状態であること。</p>                                                                                                                                                                         |
| ライセンスキー     | <p>運用系システムと待機系システムのライセンスキーが一致している状態であること。</p> <p>なお、ライセンスキーはキー入力だけでは反映されません。装置再起動後にライセンスが適用されます。ライセンスの適用状態は show license コマンドの「Available:」を確認してください。</p>                                                                                                                                |

### 14.3.3 無停止ソフトウェアアップデートの手順

無停止ソフトウェアアップデートの詳細な手順は、「ソフトウェアアップデートガイド」を参照してください

い。

### 14.3.4 無停止ソフトウェアアップデートに関する注意事項

#### (1) AX6700S に関する注意事項

AX6700S では、BSU の制御に関するソフトウェア (HDC : Hardware Dependent Code) を更新することがあります。更新時には、ソフトウェアアップデートによって BSU を再起動するため、次のことに注意してください。

- AX6700S で無停止ソフトウェアアップデートを実施するためには BSU を 2 枚以上実装し、すべての BSU を運用系またはホットスタンバイの待機系としておく必要があります。
- アップデートによって BSU を 1 枚ずつ再起動します。すべての BSU を運用系として使用中の場合、一時的にパケット転送性能が低下します。1 枚以上をホットスタンバイの待機系として使用中の場合はアップデート中もパケット転送性能を維持します。

#### (2) AX6600S に関する注意事項

AX6600S では、ソフトウェアアップデートによって CSU を再起動するため、再起動する CSU の PSP を使用したパケット転送が停止します。そのため、次のように運用してください。

- AX6600S で無停止ソフトウェアアップデートを実施するためには CSU を 2 枚実装し、一方の PSP を運用系、もう一方の PSP をホットスタンバイの待機系としてください。

#### (3) NIF に関する注意事項

本装置では、NIF の制御に関するソフトウェア (HDC : Hardware Dependent Code) を更新することがあります。更新時には、ソフトウェアアップデートによって NIF を再起動するため、次のことに注意してください。

- 無停止ソフトウェアアップデートを実施する場合、ソフトウェアアップデート時に NIF の HDC アップデートを手動アップデートにしておく必要があります。
- NIF の HDC アップデートを手動アップデートに設定している状態で、アップデート後に「HDC on NIF update required, but not updated by configuration.」のログメッセージが出力された場合は、NIF 上の HDC とソフトウェアにバンドルされている HDC が不一致となっています。この場合、アップデート後にサポートされた機能を使用できません。NIF を再起動し、NIF 上の HDC とソフトウェアにバンドルされている HDC を一致させてください。

## 14.4 オプションライセンスの設定

---

オプションライセンスとは、装置に含まれる付加機能を使用するために必要なライセンスです。付加機能ごとにオプションライセンスを提供します。オプションライセンスが設定されていない場合、付加機能を使用できません。オプションライセンスの設定および削除については、「オプションライセンス設定ガイド」を参照してください。

# 15 イーサネット

この章では、本装置のイーサネットについて説明します。

---

15.1 イーサネット共通の解説

---

15.2 イーサネット共通のコンフィグレーション

---

15.3 イーサネット共通のオペレーション

---

15.4 10BASE-T/100BASE-TX/1000BASE-T の解説

---

15.5 10BASE-T/100BASE-TX/1000BASE-T のコンフィグレーション

---

15.6 1000BASE-X の解説

---

15.7 1000BASE-X のコンフィグレーション

---

15.8 10GBASE-R の解説

---

15.9 10GBASE-R のコンフィグレーション

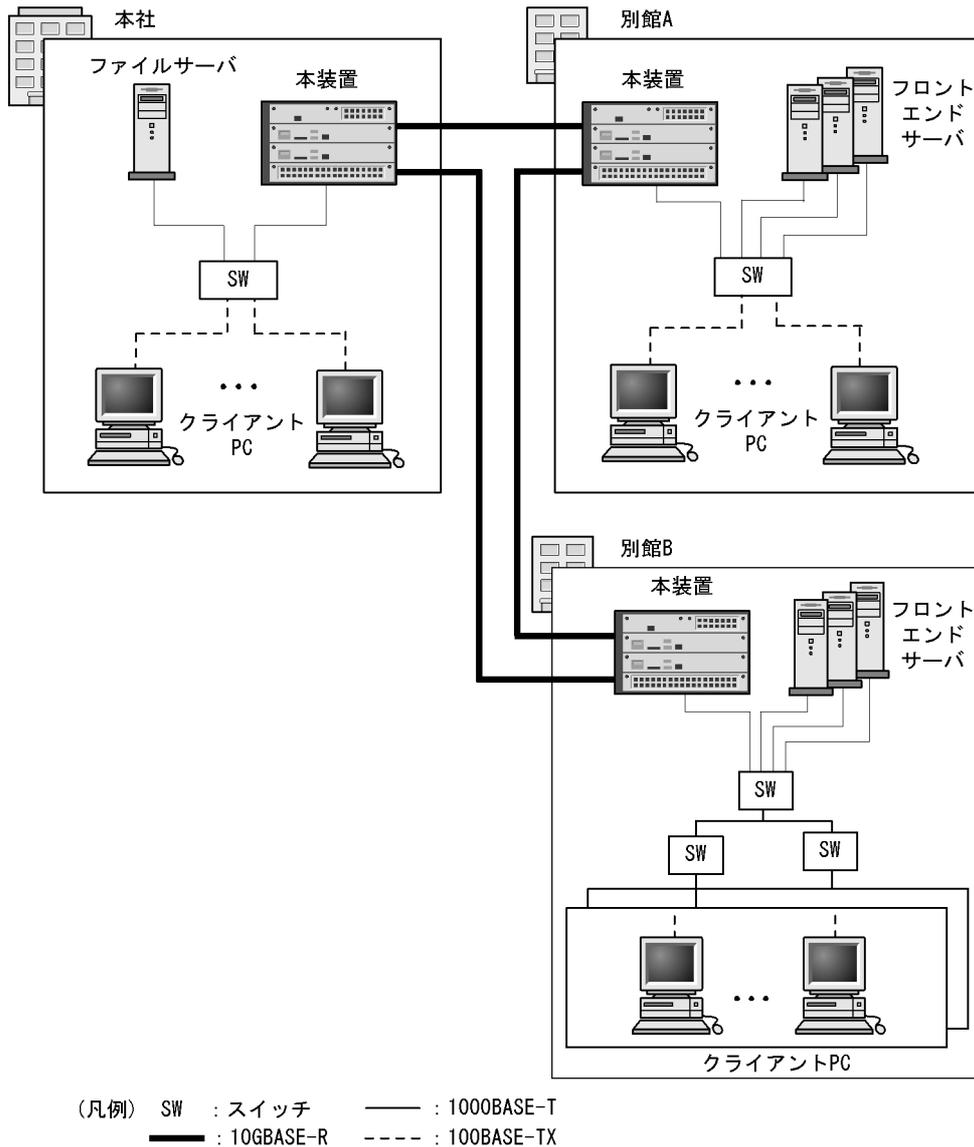
---

## 15.1 イーサネット共通の解説

### 15.1.1 ネットワーク構成例

本装置を使用した代表的なイーサネットの構成例を次の図に示します。各ビル間，サーバ間を10GBASE-R で接続することによって，10BASE-T/100BASE-TX/1000BASE-T および 1000BASE-X よりもサーバ間のパフォーマンスが向上します。

図 15-1 イーサネットの構成例



### 15.1.2 物理インターフェース

イーサネットには次の 3 種類があります。

- IEEE802.3 に準拠した 10BASE-T / 100BASE-TX / 1000BASE-T のツイストペアケーブル (UTP) を使用したインターフェース

- IEEE802.3 に準拠した 1000BASE-X の光ファイバを使用したインタフェース
- IEEE802.3ae に準拠した 10GBASE-R の光ファイバを使用したインタフェース

### 15.1.3 MAC および LLC 副層制御

フレームフォーマットを次の図に示します。

図 15-2 フレームフォーマット

| Preamble<br>およびSFD (8) | MACヘッダ                       |        |                 | DATAおよびPAD (46~9582 <sup>※</sup> ) | FCS              |            |            |
|------------------------|------------------------------|--------|-----------------|------------------------------------|------------------|------------|------------|
|                        | DA (6)                       | SA (6) | TYPE/LENGTH (2) |                                    |                  |            |            |
| Ethernet V2形式<br>フレーム時 | TYPE=<br>0x05DD~             |        |                 | DATA                               | (PAD)            |            |            |
| 802.3形式<br>フレーム時       | LENGTH=<br>0x0000~<br>0x05DC |        | LLCヘッダ          |                                    | SNAPヘッダ          | DATA (PAD) |            |
|                        |                              |        | DSAP<br>(1)     | SSAP<br>(1)                        | CONTROL<br>(1~2) | OUI<br>(3) | PID<br>(2) |
| その他                    | TYPE=上記以外                    |        |                 | DATA                               |                  |            |            |

( )内の数字はフィールド長を示す。(単位: オクテット)

注※ DATAおよびPADの最大長はEthernetV2形式フレーム時だけ9582。  
802.3形式フレームおよびその他の形式のフレームは1500。

#### (1) MAC 副層フレームフォーマット

##### (a) Preamble および SFD

64 ビット長の 2 進数で「1010...1011(最初の 62 ビットは 10 繰り返し、最後の 2 ビットは 11)」のデータです。送信時にフレームの先頭に付加します。この 64 ビットパターンのないフレームは受信できません。

##### (b) DA および SA

48 ビット形式をサポートします。16 ビット形式およびローカルアドレスはサポートしていません。

##### (c) TYPE / LENGTH

TYPE / LENGTH フィールドの扱いを次の表に示します。

表 15-1 TYPE / LENGTH フィールドの扱い

| TYPE / LENGTH 値 | 本装置での扱い                  |
|-----------------|--------------------------|
| 0x0000 ~ 0x05DC | IEEE802.3 CSMA/CD のフレーム長 |
| 0x05DD ~        | Ethernet V2.0 のフレームタイプ   |

##### (d) FCS

32 ビットの CRC 演算を使用します。

(2) LLC 副層フレームフォーマット

IEEE802.2 の LLC タイプ 1 をサポートしています。Ethernet V2 では LLC 副層はありません。

(a) DSAP

LLC 情報部の宛先のサービスアクセス点を示します。

(b) SSAP

LLC 情報部を発信した特定のサービスアクセス点を示します。

(c) CONTROL

情報転送形式，監視形式，非番号制御形式の三つの形式を示します。

(d) OUI

SNAP 情報部を発信した組織コードフィールドを示します。

(e) PID

SNAP 情報部を発信したイーサネット・タイプ・フィールドを示します。

(3) LLC の扱い

IEEE802.2 の LLC タイプ 1 をサポートしています。また，次に示す条件に合致したフレームだけを中継の対象にします。次に示す条件以外のフレームは，廃棄します。

(a) CONTROL フィールド

CONTROL フィールドの値と送受信サポート内容を「表 15-2 CONTROL フィールドの値と送受信サポート内容」に示します。また，「表 15-2 CONTROL フィールドの値と送受信サポート内容」に示す TEST フレームおよび XID フレームについては「表 15-3 XID および TEST レスポンス」に示す形で応答を返します。

表 15-2 CONTROL フィールドの値と送受信サポート内容

| 種別   | コード<br>(16 進数) | コマンド   | レスポンス  | 備考                                                                                               |
|------|----------------|--------|--------|--------------------------------------------------------------------------------------------------|
| TEST | F3 または E3      | 受信サポート | 送信サポート | IEEE802.2 の仕様に従って，TEST レスポンスを返送します。                                                              |
| XID  | BF または AF      | 受信サポート | 送信サポート | IEEE802.2 の仕様に従って，XID レスポンスを返送します。ただし，XID レスポンスの情報部は 129.1.0(IEEE802.2 の規定による ClassI を示す値) とします。 |

表 15-3 XID および TEST レスポンス

| MAC ヘッダの DA        | フレーム種別       | DSAP                                           | 応答   |
|--------------------|--------------|------------------------------------------------|------|
| ブロードキャストまたはマルチキャスト | XID および TEST | AA(SNAP)<br>42(BPDU)<br>00(null)<br>FF(global) | 返す   |
|                    |              | 上記以外                                           | 返さない |

| MAC ヘッダの DA       | フレーム種別       | DSAP                                           | 応答   |
|-------------------|--------------|------------------------------------------------|------|
| 個別アドレスで<br>自局アドレス | XID および TEST | AA(SNAP)<br>42(BPDU)<br>00(null)<br>FF(global) | 返す   |
|                   |              | 上記以外                                           | 返さない |
| 個別アドレスで<br>他局アドレス | XID および TEST | すべてのアドレス                                       | 返さない |

#### (4) 受信フレームの廃棄条件

次に示すどれかの条件によって受信したフレームを廃棄します。

- フレーム長がオクテットの整数倍でない
- 受信フレーム長 (DA ~ FCS) が 64 オクテット未満、または 1523 オクテット以上  
ただし、ジャンボフレーム選択時は、指定したフレームサイズを超えた場合
- FCS エラー
- 接続インタフェースが半二重の場合は、受信中に衝突が発生したフレーム

#### (5) パッドの扱い

送信フレーム長が 64 オクテット未満の場合、MAC 副層で FCS の直前にパッドを付加します。パッドの値は不定です。

### 15.1.4 本装置の MAC アドレス

#### (1) 装置 MAC アドレス

本装置は、装置を識別するための MAC アドレスを一つ持ちます。この MAC アドレスのことを装置 MAC アドレスと呼びます。装置 MAC アドレスは、レイヤ 3 インタフェースの MAC アドレスやスパニングツリーなどのプロトコルの装置識別子として使用します。

#### (2) 装置 MAC アドレスを使用する機能

装置 MAC アドレスを使用する機能を次の表に示します。

表 15-4 装置 MAC アドレスを使用する機能

| 機能                | 用途                      |
|-------------------|-------------------------|
| VLAN              | レイヤ 3 インタフェースの MAC アドレス |
| リンクアグリゲーションの LACP | 装置識別子                   |
| スパニングツリー          | 装置識別子                   |
| Ring Protocol     | 装置識別子                   |
| GSRP              | 装置識別子                   |
| IEEE802.3ah/UDLD  | 装置識別子                   |
| L2 ループ検知          | 装置識別子                   |
| CFM               | 装置識別子                   |
| LLDP              | 装置識別子                   |
| OADP              | 装置識別子                   |

## 15.2 イーサネット共通のコンフィグレーション

### 15.2.1 コンフィグレーションコマンド一覧

イーサネット共通のコンフィグレーションコマンド一覧を次の表に示します。

表 15-5 コンフィグレーションコマンド一覧

| コマンド名                                | 説明                                                           |
|--------------------------------------|--------------------------------------------------------------|
| bandwidth                            | 帯域幅を設定します。                                                   |
| description                          | 補足説明を設定します。                                                  |
| duplex                               | duplex を設定します。                                               |
| flowcontrol                          | フローコントロールを設定します。                                             |
| frame-error-notice                   | フレーム受信エラーおよびフレーム送信エラー発生時のエラーの通知条件を設定します。                     |
| interface gigabitethernet            | 10BASE-T/100BASE-TX/1000BASE-T/1000BASE-X のコンフィグレーションを指定します。 |
| interface tengigabitethernet         | 10GBASE-R のコンフィグレーションを指定します。                                 |
| link debounce                        | リンクダウン検出時間を設定します。                                            |
| link up-debounce                     | リンクアップ検出時間を設定します。                                            |
| mdix auto                            | 自動 MDIX 機能を設定します。                                            |
| media-type <b>【AX6700S】【AX6600S】</b> | 選択型ポートで使用するポートを設定します。                                        |
| mtu                                  | イーサネットの MTU を設定します。                                          |
| shutdown                             | イーサネットをシャットダウンします。                                           |
| speed                                | 速度を設定します。                                                    |
| system mtu                           | イーサネットの MTU の装置としての値を設定します。                                  |

### 15.2.2 複数インタフェースの一括設定

#### [ 設定のポイント ]

イーサネットのコンフィグレーションでは、複数のインタフェースに同じ情報を設定することがあります。このような場合、複数のインタフェースを range 指定することで、情報を一括して設定できます。

#### [ コマンドによる設定 ]

1. (config)# interface range gigabitethernet 1/1-10, gigabitethernet 1/15-20, tengigabitethernet 3/1  
1G ビットイーサネットインタフェース 1/1 から 1/10, 1/15 から 1/20, および 10G ビットイーサネットインタフェース 3/1 への設定を指定します。
2. (config-if-range)# \* \* \* \* \*  
複数のインタフェースに同じコンフィグレーションを一括して設定します。

## 15.2.3 イーサネットのシャットダウン

### [ 設定のポイント ]

イーサネットのコンフィグレーションでは、複数のコマンドでコンフィグレーションを設定することがあります。そのとき、コンフィグレーションの設定が完了していない状態でイーサネットがリンクアップ状態になると期待した通信ができません。したがって、最初にイーサネットをシャットダウンしてから、コンフィグレーションの設定が完了したあとにイーサネットのシャットダウンを解除することを推奨します。なお、使用しないイーサネットはシャットダウンしておいてください。また、本設定によってポートの電力を OFF にします。

### [ コマンドによる設定 ]

1. `(config)# interface gigabitethernet 1/10`  
イーサネットインタフェース 1/10 の設定を指定します。
2. `(config-if)# shutdown`  
イーサネットインタフェースをシャットダウンします。
3. `(config-if)# * * * * *`  
イーサネットインタフェースに対するコンフィグレーションを設定します。
4. `(config-if)# no shutdown`  
イーサネットインタフェースのシャットダウンを解除します。

### [ 関連事項 ]

運用コマンド `inactivate` でイーサネットの運用を停止することもできます。ただし、`inactivate` コマンドで `inactive` 状態とした場合は、装置を再起動するとイーサネットが `active` 状態になります。イーサネットをシャットダウンした場合は、装置を再起動してもイーサネットは `disable` 状態のままとなり、`active` 状態にするためにはコンフィグレーションで `no shutdown` を設定してシャットダウンを解除する必要があります。

## 15.2.4 ジャンボフレームの設定

イーサネットインタフェースの MTU は規格上 1500 オクテットです。本装置は、ジャンボフレームを使用して MTU を拡張し、一度に転送するデータ量を大きくすることでスループットを向上できます。

ジャンボフレームを使用するポートでは MTU を設定します。本装置は、設定された MTU に VLAN Tag が一つ付いているフレームを送受信できるようになります。

ポートの MTU の設定値は、ネットワークおよび相手装置と合わせて決定します。VLAN トンネリングなどで、VLAN Tag が二つ付く場合は、そのフレームを送受信できるように、MTU の値に 4 を加えた値を設定します。

### (1) ポート単位の MTU の設定

#### [ 設定のポイント ]

ポート 1/10 のポートの MTU を 8192 オクテットに設定します。この設定によって、8210 オクテットまでのジャンボフレームを送受信できるようになります。

#### [ コマンドによる設定 ]

1. `(config)# interface gigabitethernet 1/10`  
`(config-if)# shutdown`  
`(config-if)# mtu 8192`  
 ポートの MTU を 8192 オクテットに設定します。

2. `(config-if)# no shutdown`

[ 注意事項 ]

- コンフィグレーションでポートの MTU を設定していても、10BASE-T または 100BASE-TX 半二重で接続する場合（オートネゴシエーションの結果が 10BASE-T または 100BASE-TX 半二重になった場合も含みます）は、ポートの MTU は 1500 オクテットになります。
- サポートするジャンボフレーム長に制限がある NIF を次の表に示します。これらの NIF でジャンボフレームを使用する場合は、ポートの MTU を「MTU 長の上限」に示す値以下で設定してください。また、装置内で該当ポートと同じ VLAN に収容されるすべてのポートの MTU も同様に設定してください。

表 15-6 ジャンボフレーム長の上限（FCS を含まない）と MTU 長の上限

| NIF 略称   | ジャンボフレーム長の上限（FCS を含まない） | MTU 長の上限 |
|----------|-------------------------|----------|
| NK1GS-8M | 2000                    | 1982     |
| NH1G-16S | 4092                    | 4074     |
| NH1G-48T | 4092                    | 4074     |
| NH1GS-6M | 2000                    | 1982     |

## (2) 全ポート共通の MTU の設定

[ 設定のポイント ]

本装置の全イーサネットインタフェースでポートの MTU を 4096 オクテットに設定します。この設定によって、4114 オクテットまでのジャンボフレームを送受信できるようになります。

[ コマンドによる設定 ]

1. `(config)# system mtu 4096`  
 装置の全ポートで、ポートの MTU を 4096 オクテットに設定します。

[ 注意事項 ]

- コンフィグレーションでポートの MTU を設定していても、10BASE-T または 100BASE-TX 半二重で接続する場合（オートネゴシエーションの結果が 10BASE-T または 100BASE-TX 半二重になった場合も含みます）は、ポートの MTU は 1500 オクテットになります。
- サポートするジャンボフレーム長に制限がある NIF を「表 15-6 ジャンボフレーム長の上限（FCS を含まない）と MTU 長の上限」に示します。これらの NIF でジャンボフレームを使用する場合は、ポートの MTU を「MTU 長の上限」に示す値以下で設定してください。また、装置内で該当ポートと同じ VLAN に収容されるすべてのポートの MTU も同様に設定してください。

## 15.2.5 リンクダウン検出タイマの設定

リンク障害を検出してからリンクダウンするまでのリンクダウン検出時間が短い場合、相手装置によってはリンクが不安定になることがあります。このような場合、リンクダウン検出タイマを設定することで、

リンクが不安定になることを防ぐことができます。

[ 設定のポイント ]

リンクダウン検出時間は、リンクが不安定とまらない範囲でできるだけ短い値にします。リンクダウン検出時間を設定しなくてもリンクが不安定とまらない場合は、リンクダウン検出時間を設定しないでください。

[ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/10  
イーサネットインタフェース 1/10 の設定を指定します。
2. (config-if)# link debounce time 5000  
リンクダウン検出タイマを 5000 ミリ秒に設定します。

[ 注意事項 ]

リンクダウン検出時間を設定すると、リンクが不安定になることを防ぐことができますが、障害が発生した場合にリンクダウンするまでの時間が長くなります。リンク障害を検出してからリンクダウンするまでの時間を短くしたい場合は、リンクダウン検出タイマを設定しないでください。

## 15.2.6 リンクアップ検出タイマの設定

リンク障害回復を検出してからリンクアップするまでのリンクアップ検出時間が短い場合、相手装置によってはネットワーク状態が不安定になることがあります。このような場合、リンクアップ検出タイマを設定することで、ネットワーク状態が不安定になることを防ぐことができます。

[ 設定のポイント ]

リンクアップ検出時間は、ネットワーク状態が不安定とまらない範囲でできるだけ短い値にします。リンクアップ検出時間を設定しなくてもネットワーク状態が不安定とまらない場合は、リンクアップ検出時間を設定しないでください。

[ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/10  
イーサネットインタフェース 1/10 の設定を指定します。
2. (config-if)# link up-debounce time 5000  
リンクアップ検出タイマを 5000 ミリ秒に設定します。

[ 注意事項 ]

リンクアップ検出タイマを長く設定すると、リンク障害回復から通信できるまでの時間が長くなります。リンク障害回復から通信できるまでの時間を短くしたい場合は、リンクアップ検出タイマを設定しないでください。

## 15.2.7 フレーム送受信エラー通知の設定

軽度のエラーが発生してフレームの受信または送信に失敗した場合、本装置はフレームが廃棄された原因を統計情報として採取します。30 秒間に発生したエラーの回数とエラーの発生する割合が閾値を超えた場合は、エラーの発生をログおよびプライベートトラップで通知します。

本装置では、閾値とエラーが発生した場合の通知について設定ができます。設定がない場合、30 秒間に

15 回エラーが発生したときに最初の 1 回だけログを表示します。

#### (1) エラーフレーム数を閾値にしての通知

[ 設定のポイント ]

エラーの通知条件のうち、エラーの発生回数（エラーフレーム数）の閾値を本装置に設定する場合は、`frame-error-notice` コマンドで `error-frames` を設定します。

[ コマンドによる設定 ]

1. `(config)# frame-error-notice error-frames 50`  
エラーの発生回数（エラーフレーム数）の閾値を 50 回に設定します。

#### (2) エラーレートを閾値にしての通知

[ 設定のポイント ]

エラーの通知条件のうち、エラーの発生割合（エラーレート）の閾値を本装置に設定する場合は、`frame-error-notice` コマンドで `error-rate` を設定します。

[ コマンドによる設定 ]

1. `(config)# frame-error-notice error-rate 20`  
エラーの発生割合の閾値を 20% に設定します。

#### (3) 通知時のログ表示設定

[ 設定のポイント ]

エラーの通知条件のうち、エラーが発生したときのログの表示を設定する場合は、`frame-error-notice` コマンドで `onetime-display`、または `everytime-display` を設定します。ログを表示しないようにする場合は、`off` を設定します。この設定は、プライベートトラップには関係しません。

[ コマンドによる設定 ]

1. `(config)# frame-error-notice everytime-display`  
エラーが発生するたびにログを表示します。

#### (4) 条件の組み合わせ設定

[ 設定のポイント ]

エラーの通知条件を複数組み合わせる場合は、`frame-error-notice` コマンドで、複数の条件を同時に設定します。`frame-error-notice` コマンド入力前に設定していた通知条件は無効となりますので、引き続き同じ通知条件を設定する場合は、`frame-error-notice` コマンドで再度設定し直してください。

[ コマンドによる設定 ]

すでにエラーが発生するたびにログを表示することを設定していて、さらにエラーの発生割合（エラーレート）の閾値を設定する場合の設定例を示します。

1. `(config)# frame-error-notice error-frames 50 everytime-display`  
エラーの発生回数（エラーフレーム数）の閾値を 50 回に設定し、エラーが発生するたびにログを表示します。

## [ 注意事項 ]

プライベートトラップを使用する場合は、snmp-server host コマンドでフレーム受信エラー発生時のトラップとフレーム送信エラー発生時のトラップを送信するように設定してください。

## 15.3 イーサネット共通のオペレーション

### 15.3.1 運用コマンド一覧

イーサネットで使用する運用コマンド一覧を次の表に示します。

表 15-7 運用コマンド一覧

| コマンド名              | 説明                                 |
|--------------------|------------------------------------|
| show interfaces    | イーサネットの情報を表示します。                   |
| clear counters     | イーサネットの統計情報カウンタをクリアします。            |
| show port          | イーサネットの情報を一覧で表示します。                |
| activate           | inactive 状態のイーサネットを active 状態にします。 |
| inactivate         | active 状態のイーサネットを inactive 状態にします。 |
| test interfaces    | 回線テストを実行します。                       |
| no test interfaces | 回線テストを停止し、結果を表示します。                |

### 15.3.2 イーサネットの動作状態を確認する

#### (1) 全イーサネットの動作状態を確認する

show port コマンドを実行すると、本装置に実装している全イーサネットの状態を確認できます。使用するイーサネットの Status の表示が up になっていることを確認します。

show port コマンドの実行結果を次の図に示します。

図 15-3 「本装置に実装している全イーサネットの状態」の表示例

```
> show port
Date 2006/03/21 15:16:19 UTC
Port Counts: 24
Port Name Status Speed Duplex FCtl FrLen ChGr/Status
1/ 1 geth1/1 up 1000BASE-SX full(auto) off 1518 -/-
1/ 2 geth1/2 down - - - - -/-
1/ 3 geth1/3 up 100BASE-TX full(auto) off 1518 -/-
1/ 4 geth1/4 up 1000BASE-SX full(auto) off 1518 -/-
:
:
```

## 15.4 10BASE-T/100BASE-TX/1000BASE-T の解説

---

10BASE-T / 100BASE-TX / 1000BASE-T のツイストペアケーブル (UTP) を使用したインタフェースについて説明します。

### 15.4.1 機能一覧

#### (1) 接続インタフェース

##### (a) 10BASE-T / 100BASE-TX / 1000BASE-T 自動認識 (オートネゴシエーション)

10BASE-T / 100BASE-TX / 1000BASE-T では自動認識機能 (オートネゴシエーション) と固定接続機能をサポートしています。

- 自動認識...10BASE-T, 100BASE-TX, 1000BASE-T (全二重)
- 固定接続...10BASE-T, 100BASE-TX

コンフィグレーションでは次のモードを指定できます。接続するネットワークに合わせて設定してください。本装置のデフォルト値は、オートネゴシエーションとなります。

- オートネゴシエーション
- 100BASE-TX 全二重固定
- 100BASE-TX 半二重固定
- 10BASE-T 全二重固定
- 10BASE-T 半二重固定

##### (b) 10BASE-T / 100BASE-TX / 1000BASE-T 接続仕様

本装置のコンフィグレーションでの指定値と相手装置の伝送速度および、全二重および半二重モードの接続仕様を次の表に示します。

10BASE-T および 100BASE-TX は、相手装置によってオートネゴシエーションでは接続できない場合がありますので、できるだけ相手装置のインタフェースに合わせた固定設定にしてください。

1000BASE-T は、全二重のオートネゴシエーションだけの接続となります。

表 15-8 伝送速度および、全二重および半二重モードごとの接続仕様

| 接続装置                    |                                                             | 本装置の設定                       |                 |                                |                   |                                |
|-------------------------|-------------------------------------------------------------|------------------------------|-----------------|--------------------------------|-------------------|--------------------------------|
| 設定                      | インタフェース                                                     | 固定                           |                 |                                |                   | オート<br>ネゴシエーシ<br>ョン            |
|                         |                                                             | 10BASE-T<br>半二重 <sup>1</sup> | 10BASE-T<br>全二重 | 100BASE-TX<br>半二重 <sup>1</sup> | 100BASE-TX<br>全二重 |                                |
| 固定                      | 10BASE-T<br>半二重                                             | 10BASE-T<br>半二重              | ×               | ×                              | ×                 | 10BASE-T<br>半二重 <sup>2</sup>   |
|                         | 10BASE-T<br>全二重                                             | ×                            | 10BASE-T<br>全二重 | ×                              | ×                 | ×                              |
|                         | 100BASE-TX<br>半二重                                           | ×                            | ×               | 100BASE-TX<br>半二重              | ×                 | 100BASE-TX<br>半二重 <sup>2</sup> |
|                         | 100BASE-TX<br>全二重                                           | ×                            | ×               | ×                              | 100BASE-TX<br>全二重 | ×                              |
|                         | 1000BASE-T<br>半二重                                           | ×                            | ×               | ×                              | ×                 | ×                              |
|                         | 1000BASE-T<br>全二重                                           | ×                            | ×               | ×                              | ×                 | ×                              |
| オート<br>ネゴシ<br>エー<br>ション | 10BASE-T<br>半二重                                             | 10BASE-T<br>半二重              | ×               | ×                              | ×                 | 10BASE-T<br>半二重 <sup>2</sup>   |
|                         | 10BASE-T<br>全二重                                             | ×                            | ×               | ×                              | ×                 | 10BASE-T<br>全二重                |
|                         | 10BASE-T<br>全二重および<br>半二重                                   | 10BASE-T<br>半二重              | ×               | ×                              | ×                 | 10BASE-T<br>全二重                |
|                         | 100BASE-TX<br>半二重                                           | ×                            | ×               | 100BASE-TX<br>半二重              | ×                 | 100BASE-TX<br>半二重 <sup>2</sup> |
|                         | 100BASE-TX<br>全二重                                           | ×                            | ×               | ×                              | ×                 | 100BASE-TX<br>全二重              |
|                         | 100BASE-TX<br>全二重および<br>半二重                                 | ×                            | ×               | 100BASE-TX<br>半二重              | ×                 | 100BASE-TX<br>全二重              |
|                         | 10BASE-T/<br>100BASE-TX<br>全二重および<br>半二重                    | 10BASE-T<br>半二重              | ×               | 100BASE-TX<br>半二重              | ×                 | 100BASE-TX<br>全二重              |
|                         | 1000BASE-T<br>半二重                                           | ×                            | ×               | ×                              | ×                 | ×                              |
|                         | 1000BASE-T<br>全二重                                           | ×                            | ×               | ×                              | ×                 | 1000BASE-T<br>全二重              |
|                         | 1000BASE-T<br>全二重および<br>半二重                                 | ×                            | ×               | ×                              | ×                 | 1000BASE-T<br>全二重              |
|                         | 10BASE-T/<br>100BASE-TX<br>/<br>1000BASE-T<br>全二重および<br>半二重 | 10BASE-T<br>半二重              | ×               | 100BASE-TX<br>半二重              | ×                 | 1000BASE-T<br>全二重              |

(凡例) × : 接続できない

注 1

NK1GS-8M, NH1GS-6M の 10BASE-T および 100BASE-TX の場合、設定できません。

注 2

NK1GS-8M, NH1GS-6M の 10BASE-T および 100BASE-TX の場合、接続できません。

## (2) オートネゴシエーション

オートネゴシエーションは、伝送速度および、全二重および半二重モード認識およびフローコントロールについて、対向装置間でやりとりを行い、接続動作を決定する機能です。

本装置での接続仕様を、「表 15-8 伝送速度および、全二重および半二重モードごとの接続仕様」に示します。また、本装置では、ネゴシエーションで解決できなかった場合、リンク接続されるまで接続動作を繰り返します。

## (3) フローコントロール

フローコントロールは、装置内の受信バッファ枯渇でフレームを廃棄しないように、相手装置にフレームの送信をポーズパケットによって、一時的に停止指示する機能です。自装置がポーズパケット受信時は、送信規制を行います。この機能は全二重だけサポートします。

本装置では、受信バッファの使用状況を監視し、相手装置の送信規制を行う場合、ポーズパケットを送信します。本装置がポーズパケット受信時は、送信規制を行います。フローコントロールのコンフィグレーションは、送信と受信でそれぞれ設定でき、有効または無効および、ネゴシエーション結果により決定したモードを選択できます。本装置と相手装置の設定を送信と受信が一致するように合わせてください。例えば、本装置のポーズパケット送信を on に設定した場合、相手装置のポーズパケット受信は有効に設定してください。本装置と相手装置の設定内容と実行動作モードを「表 15-9 フローコントロールの送信動作」、「表 15-10 フローコントロールの受信動作」および「表 15-11 オートネゴシエーション時のフローコントロール動作」に示します。

表 15-9 フローコントロールの送信動作

| 本装置のポーズパケット送信 | 相手装置のポーズパケット受信 | フローコントロール動作    |
|---------------|----------------|----------------|
| on            | 有効             | 相手装置が送信規制を行う   |
| off           | 無効             | 相手装置が送信規制を行わない |
| desired       | desired        | 相手装置が送信規制を行う   |

(凡例)

on：有効。

off：無効。desired と組み合わせた設定の場合、ネゴシエーション結果によって動作します。フローコントロール動作は「表 15-11 オートネゴシエーション時のフローコントロール動作」を参照してください。

desired：有効。オートネゴシエーション選択時は、ネゴシエーション結果によって動作します。フローコントロール動作は「表 15-11 オートネゴシエーション時のフローコントロール動作」を参照してください。

表 15-10 フローコントロールの受信動作

| 本装置のポーズパケット受信 | 相手装置のポーズパケット送信 | フローコントロール動作   |
|---------------|----------------|---------------|
| on            | 有効             | 本装置が送信規制を行う   |
| off           | 無効             | 本装置が送信規制を行わない |
| desired       | desired        | 本装置が送信規制を行う   |

(凡例)

on：有効。

off：無効。desired と組み合わせた設定の場合、ネゴシエーション結果によって動作します。フローコントロール動作は「表 15-11 オートネゴシエーション時のフローコントロール動作」を参照してください。

desired：有効。オートネゴシエーション選択時は、ネゴシエーション結果によって動作します。フローコントロール動作は「表 15-11 オートネゴシエーション時のフローコントロール動作」を参照してください。

表 15-11 オートネゴシエーション時のフローコントロール動作

| 本装置       |           | 相手装置      |           | 本装置のオートネゴシエーション結果 |           | フローコントロール動作 |           |      |      |
|-----------|-----------|-----------|-----------|-------------------|-----------|-------------|-----------|------|------|
| ポーズパケット送信 | ポーズパケット受信 | ポーズパケット送信 | ポーズパケット受信 | ポーズパケット送信         | ポーズパケット受信 | 本装置の送信規制    | 相手装置の送信規制 |      |      |
| on        | desired   | 有効        | 有効        | on                | on        | 行う          | 行う        |      |      |
|           |           |           | 無効        | on                | off       | 行わない        | 行わない      |      |      |
|           |           |           | desired   | on                | on        | 行う          | 行う        |      |      |
|           |           | 無効        | 有効        | on                | on        | 行わない        | 行う        |      |      |
|           |           |           | 無効        | on                | off       | 行わない        | 行わない      |      |      |
|           |           |           | desired   | on                | on        | 行う          | 行う        |      |      |
|           |           | desired   | 有効        | on                | on        | 行う          | 行う        |      |      |
|           |           |           | 無効        | on                | off       | 行わない        | 行わない      |      |      |
|           |           |           | desired   | on                | on        | 行う          | 行う        |      |      |
|           |           | off       |           | 有効                | 有効        | on          | on        | 行う   | 行う   |
|           |           |           |           |                   | 無効        | off         | on        | 行う   | 行わない |
|           |           |           |           |                   | desired   | on          | on        | 行う   | 行う   |
| 無効        | 有効        |           |           | on                | on        | 行わない        | 行う        |      |      |
|           | 無効        |           |           | off               | off       | 行わない        | 行わない      |      |      |
|           | desired   |           |           | on                | on        | 行う          | 行う        |      |      |
| desired   | 有効        |           |           | on                | on        | 行う          | 行う        |      |      |
|           | 無効        |           |           | off               | on        | 行う          | 行わない      |      |      |
|           | desired   |           |           | on                | on        | 行う          | 行う        |      |      |
| desired   | on        |           |           | 有効                | 有効        | on          | on        | 行う   | 行う   |
|           |           |           |           |                   | 無効        | off         | on        | 行う   | 行わない |
|           |           |           |           |                   | desired   | on          | on        | 行う   | 行う   |
|           |           | 無効        | 有効        | on                | on        | 行わない        | 行う        |      |      |
|           |           |           | 無効        | off               | on        | 行わない        | 行わない      |      |      |
|           |           |           | desired   | on                | on        | 行う          | 行う        |      |      |
|           |           | desired   | 有効        | on                | on        | 行う          | 行う        |      |      |
|           |           |           | 無効        | off               | on        | 行わない        | 行わない      |      |      |
|           |           |           | desired   | on                | on        | 行う          | 行う        |      |      |
|           |           | off       |           | 有効                | 有効        | off         | off       | 行わない | 行わない |
|           |           |           |           |                   | 無効        | off         | off       | 行わない | 行わない |
|           |           |           |           |                   | desired   | off         | off       | 行わない | 行わない |
| 無効        | 有効        |           |           | on                | off       | 行わない        | 行う        |      |      |
|           | 無効        |           |           | off               | off       | 行わない        | 行わない      |      |      |
|           | desired   |           |           | on                | off       | 行わない        | 行う        |      |      |

| 本装置       |           | 相手装置      |           | 本装置のオートネゴシエーション結果 |           | フローコントロール動作 |           |
|-----------|-----------|-----------|-----------|-------------------|-----------|-------------|-----------|
| ポーズパケット送信 | ポーズパケット受信 | ポーズパケット送信 | ポーズパケット受信 | ポーズパケット送信         | ポーズパケット受信 | 本装置の送信規制    | 相手装置の送信規制 |
|           |           | desired   | 有効        | off               | off       | 行わない        | 行わない      |
|           |           |           | 無効        | off               | off       | 行わない        | 行わない      |
|           |           |           | desired   | off               | off       | 行わない        | 行わない      |
|           | desired   | 有効        | 有効        | on                | on        | 行う          | 行う        |
|           |           |           | 無効        | off               | off       | 行わない        | 行わない      |
|           |           |           | desired   | on                | on        | 行う          | 行う        |
|           |           | 無効        | 有効        | on                | on        | 行わない        | 行う        |
|           |           |           | 無効        | off               | off       | 行わない        | 行わない      |
|           |           |           | desired   | on                | on        | 行う          | 行う        |
|           |           | desired   | 有効        | on                | on        | 行う          | 行う        |
|           |           |           | 無効        | off               | off       | 行わない        | 行わない      |
|           |           |           | desired   | on                | on        | 行う          | 行う        |

#### (4) 自動 MDIX 機能

自動 MDIX 機能は、MDI と MDI-X を自動的に切り替える機能です。これによって、クロスケーブルまたはストレートケーブルどちらでも通信できるようになります。オートネゴシエーション時だけサポートします。半二重および全二重固定時は MDI-X となります。MDI / MDI-X のピンマッピングを次の表に示します。

表 15-12 MDI / MDI-X のピンマッピング

| RJ45<br>Pin No. | MDI        |            |          | MDI-X      |            |          |
|-----------------|------------|------------|----------|------------|------------|----------|
|                 | 1000BASE-T | 100BASE-TX | 10BASE-T | 1000BASE-T | 100BASE-TX | 10BASE-T |
| 1               | BI_DA +    | TD +       | TD +     | BI_DB +    | RD +       | RD +     |
| 2               | BI_DA -    | TD -       | TD -     | BI_DB -    | RD -       | RD -     |
| 3               | BI_DB +    | RD +       | RD +     | BI_DA +    | TD +       | TD +     |
| 4               | BI_DC +    | Unused     | Unused   | BI_DD +    | Unused     | Unused   |
| 5               | BI_DC -    | Unused     | Unused   | BI_DD -    | Unused     | Unused   |
| 6               | BI_DB -    | RD -       | RD -     | BI_DA -    | TD -       | TD -     |
| 7               | BI_DD +    | Unused     | Unused   | BI_DC +    | Unused     | Unused   |
| 8               | BI_DD -    | Unused     | Unused   | BI_DC -    | Unused     | Unused   |

注 1

10BASE-T と 100BASE-TX では、送信 (TD) と受信 (RD) 信号は別々の信号線を使用しています。

注 2

1000BASE-T では、8 ピンすべてを送信と受信が同時双方向 (bi-direction) 通信するため、信号名表記が異なります。(BI\_Dx: 双方向データ信号)

### (5) ジャンボフレーム

ジャンボフレームは、MAC ヘッダの DA ~ データが 1518 オクテットを超えるフレームを中継するための機能です。コンフィグレーションコマンド `ip mtu` の MTU 長を合わせて変更することで、IP パケットをフラグメント化するサイズを大きくすることもできます。

本装置では、Ethernet V2 形式フレームだけをサポートします。802.3 形式フレームはサポートしていません。フレームについては「15.1.3 MAC および LLC 副層制御」のフレームフォーマットを参照してください。Tagged フレームについては「19.1.5 VLAN Tag」の Tagged フレームのフォーマットを参照してください。また、物理インタフェースは、100BASE-TX（全二重）、1000BASE-T（全二重）だけサポートします。ジャンボフレームのサポート機能を次の表に示します。

表 15-13 ジャンボフレームサポート機能

| 項目               | フレーム形式                  |           | 内容                                                              |
|------------------|-------------------------|-----------|-----------------------------------------------------------------|
|                  | EthernetV2 <sup>1</sup> | IEEE802.3 |                                                                 |
| フレーム長<br>(オクテット) | 1519 ~ 9596             | ×         | MAC ヘッダの DA ~ データの長さ。FCS は含みません。                                |
| 受信機能             |                         | ×         | IEEE802.3 フレームは、LENGTH フィールド値が 0x05DD (1501 オクテット) 以上の場合に廃棄します。 |
| 送信機能             |                         | ×         | IEEE802.3 フレームは送信しません。                                          |

(凡例) ○ : サポート × : 未サポート

注 <sup>1</sup> 「15.1.3 MAC および LLC 副層制御」のフレームフォーマットを参照してください。

### (6) 10BASE-T / 100BASE-TX / 1000BASE-T 接続時の注意事項

- 伝送速度、および全二重および半二重モードが相手装置と不一致の場合、接続できないので注意してください。  
不一致の状態では通信を行うと、以降の通信が停止することがあります。この場合、当該ポートに対して `inactivate` コマンド、`activate` コマンドを実行してください。
- 使用するケーブルについては、マニュアル「ハードウェア取扱説明書」を参照してください。
- 全二重インタフェースはコリジョン検出とループバック機能を行わないことによって実現しています。このため、10BASE-T または 100BASE-TX を全二重インタフェース設定で使用する場合は、相手接続ポートは必ず全二重インタフェースに設定して接続してください。
- 1000BASE-T を使用する場合は全二重のオートネゴシエーションだけとなります。

## 15.4.2 10BASE-T/100BASE-TX/1000BASE-T・1000BASE-X 選択型 ポート【AX6700S】【AX6600S】

本装置は、NIF 種別によって 10BASE-T/100BASE-TX/1000BASE-T または 1000BASE-X (SFP) のポートを選択できる 1Gbit/s のワイヤレートを保証したポートを搭載しています。10BASE-T/100BASE-TX/1000BASE-T ポートと 1000BASE-X (SFP) のどちらのポートを使うかは、`media-type` コマンドで設定します。

本装置の出荷時のデフォルトコンフィグレーションでは、1000BASE-X (SFP) ポートを使う設定になっています。10BASE-T/100BASE-TX/1000BASE-T ポートを使う場合は、`media-type` コマンドで `rj45` を設定します。

### 15.4.3 10BASE-T/100BASE-TX/1000BASE-T 用 SFP

本装置では、専用の SFP を使用することで、1000BASE-X (SFP) ポートで 10BASE-T/100BASE-TX/1000BASE-T の接続ができます。

通信機能については、10BASE-T/100BASE-TX/1000BASE-T ポートと、SFP による接続で違いはありません。

なお、10BASE-T/100BASE-TX/1000BASE-T 用 SFP をサポートする NIF は次のとおりです。

- NK1G-24S
- NH1G-24S

## 15.5 10BASE-T/100BASE-TX/1000BASE-T のコンフィグレーション

---

### 15.5.1 イーサネットの設定

#### (1) 速度と duplex の設定

本装置と相手装置の伝送速度と duplex を設定できます。デフォルトではオートネゴシエーションで、相手装置と伝送速度と duplex を決定します。

##### (a) オートネゴシエーションに対応していない相手装置と接続する場合

###### [ 設定のポイント ]

10BASE-T および 100BASE-TX では、相手装置によってはオートネゴシエーションで接続できない場合があります。その場合は、相手装置に合わせて回線速度と duplex を指定し、固定設定で接続します。

###### [ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/10  
(config-if)# shutdown  
(config-if)# speed 10  
(config-if)# duplex half  
相手装置と 10BASE-T 半二重で接続する設定をします。

2. (config-if)# no shutdown

##### (b) オートネゴシエーションでも特定の速度を使用したい場合

###### [ 設定のポイント ]

本装置は、オートネゴシエーションで接続する場合でも、回線速度を設定できます。オートネゴシエーションに加えて回線速度を設定した場合、相手装置とオートネゴシエーションで接続しても、設定された回線速度にならないときはリンクがアップしません。そのため、意図しない回線速度で接続されることを防止できます。

###### [ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/10  
(config-if)# shutdown  
(config-if)# speed auto 1000  
相手装置とオートネゴシエーションで接続しても、1000BASE-T だけで接続するようにします。

2. (config-if)# no shutdown

###### [ 注意事項 ]

回線速度と duplex は正しい組み合わせで設定してください。オートネゴシエーションの場合は、回線速度と duplex の両方ともにオートネゴシエーションを設定する必要があります。固定設定の場合は、回線速度と duplex の両方を固定設定にする必要があります。正しい組み合わせが設定されていない場合は、オートネゴシエーションで相手装置と接続します。

## 15.5.2 フローコントロールの設定

本装置内の受信バッファが枯渇して受信フレームを廃棄することがないようにするためには、ポーズパケットを送信して相手装置に送信規制を要求します。相手装置はポーズパケットを受信して送信規制できる必要があります。

相手装置からのポーズパケットを受信したとき、本装置が送信規制するかどうかは設定に従います。本装置では、オートネゴシエーション時に相手装置とポーズパケットを送受信するかどうかを折衝できます。

[ 設定のポイント ]

フローコントロールの設定内容は、相手装置と矛盾しないように決定してください。

[ コマンドによる設定 ]

```
1. (config)# interface gigabitethernet 1/10
 (config-if)# shutdown
 (config-if)# flowcontrol send off
 (config-if)# flowcontrol receive off
 相手装置とのポーズパケット送受信を停止します。
```

```
2. (config-if)# no shutdown
```

## 15.5.3 自動 MDIX の設定

本装置の 10BASE-T/100BASE-TX/1000BASE-T ポートは、自動 MDIX 機能をサポートしています。そのため、オートネゴシエーション時に、ケーブルのストレートまたはクロスに合わせて自動的に MDI 設定が切り替わり通信できます。また、本装置は MDI の固定機能を持っており、MDI 固定時は MDI-X (HUB 仕様) となります。

[ 設定のポイント ]

自動 MDIX を MDI-X に固定する場合に、固定したいインタフェースに設定します。

[ コマンドによる設定 ]

```
1. (config)# interface gigabitethernet 1/24
 イーサネットインタフェース 1/24 の設定を指定します。
```

```
2. (config-if)# no mdix auto
 (config-if)# exit
 自動 MDIX 機能を無効にし、MDI-X 固定にします。
```

## 15.5.4 選択型ポートでの 10BASE-T/100BASE-TX/1000BASE-T の設定 【AX6700S】【AX6600S】

10BASE-T/100BASE-TX/1000BASE-T・1000BASE-X 選択型ポートで 10BASE-T/100BASE-TX/1000BASE-T ポートを使う場合は、そのポートに対して media-type コマンドで rj45 を設定します。

[ 設定のポイント ]

1000BASE-X ポートを使う場合は設定不要です。10BASE-T/100BASE-TX/1000BASE-T ポートを使

う場合に設定が必要です。

[ コマンドによる設定 ]

1. (config)# interface range gigabitethernet 1/1-2  
(config-if-range)# shutdown  
(config-if-range)# media-type rj45  
10BASE-T/100BASE-TX/1000BASE-T ポートを使うように設定します。
2. (config-range)# no shutdown

## 15.6 1000BASE-X の解説

---

### 15.6.1 機能一覧

1000BASE-X の光ファイバを使用したインタフェースについて説明します。

#### (1) 接続インタフェース

##### (a) 1000BASE-X

1000BASE-SX, 1000BASE-SX2, 1000BASE-LX, 1000BASE-LH, 1000BASE-LHB および 1000BASE-BX をサポートしています。回線速度は 1000Mbit/s 全二重固定です。

1000BASE-SX :

短距離間を接続するために使用します。  
(マルチモード, 最大 550m)

1000BASE-SX2 :

マルチモード光ファイバを使用して 2km の伝送距離を実現します。  
(マルチモード, 最大 2km)

1000BASE-LX :

中距離間を接続するために使用します。  
(シングルモード, 最大 5km / マルチモード, 最大 550m)

1000BASE-LH, 1000BASE-LHB :

長距離間を接続するために使用します。  
1000BASE-LH : (シングルモード, 最大 70km)  
1000BASE-LHB : (シングルモード, 最大 100km)

1000BASE-BX :

送受信で異なる波長の光を使用するため, アップ側とダウン側で 1 対となるトランシーバを使用します。  
本装置では, IEEE802.3ah で規定されている 1000BASE-BX10-D/1000BASE-BX10-U と, 独自規格の 1000BASE-BX40-D/1000BASE-BX40-U をサポートします。

1000BASE-BX10-D/1000BASE-BX10-U :

中距離間を接続するために使用します。  
(シングルモード, 最大 10km)

1000BASE-BX40-D/1000BASE-BX40-U :

長距離間を接続するために使用します。  
(シングルモード, 最大 40km)

コンフィグレーションでは次のモードを指定できます。接続するネットワークに合わせて設定してください。本装置のデフォルト値は, オートネゴシエーションになります。

- オートネゴシエーション
- 1000BASE-X 全二重固定

##### (b) 1000BASE-X 接続仕様

本装置のコンフィグレーションでの指定値と相手装置の伝送速度および, 全二重および半二重モードの接

続仕様を次の表に示します。なお、1000BASE-X の物理仕様については、マニュアル「ハードウェア取扱説明書」を参照してください。

表 15-14 伝送速度および、全二重および半二重モードごとの接続仕様

| 接続装置側設定     |                 | 本装置の設定          |                 |
|-------------|-----------------|-----------------|-----------------|
| 設定          | インタフェース         | 固定              | オートネゴシエーション     |
|             |                 | 1000BASE<br>全二重 | 1000BASE<br>全二重 |
| 固定          | 1000BASE<br>半二重 | ×               | ×               |
|             | 1000BASE<br>全二重 | 1000BASE<br>全二重 | ×               |
| オートネゴシエーション | 1000BASE<br>半二重 | ×               | ×               |
|             | 1000BASE<br>全二重 | ×               | 1000BASE<br>全二重 |

(凡例) × : 接続できない

## (2) オートネゴシエーション

オートネゴシエーションは、全二重モード選択およびフローコントロールについて、対向装置間でやり取りを行い、接続動作を決定する機能です。

本装置での接続仕様を、「表 15-14 伝送速度および、全二重および半二重モードごとの接続仕様」に示します。また、本装置では、ネゴシエーションで解決できなかった場合、リンク接続されるまで接続動作を繰り返します。

## (3) フローコントロール

フローコントロールは、装置内の受信バッファ枯渇でフレームを廃棄しないように、相手装置にフレームの送信をポーズパケットによって、一時的に停止指示する機能です。自装置がポーズパケット受信時は、送信規制を行います。この機能は全二重だけサポートします。

本装置では、受信バッファの使用状況を監視し、相手装置の送信規制を行う場合、ポーズパケットを送信します。本装置がポーズパケット受信時は、送信規制を行います。フローコントロールのコンフィグレーションは、送信と受信でそれぞれ設定でき、有効または無効、およびネゴシエーション結果によって決定したモードを選択できます。本装置と相手装置の設定を送信と受信が一致するように合わせてください。例えば、本装置のポーズパケット送信を on に設定した場合、相手装置のポーズパケット受信は有効に設定してください。本装置と相手装置の設定内容と実行動作モードを「表 15-15 フローコントロールの送信動作」、「表 15-16 フローコントロールの受信動作」および「表 15-17 オートネゴシエーション時のフローコントロール動作」に示します。

表 15-15 フローコントロールの送信動作

| 本装置のポーズパケット送信 | 相手装置のポーズパケット受信 | フローコントロール動作    |
|---------------|----------------|----------------|
| on            | 有効             | 相手装置が送信規制を行う   |
| off           | 無効             | 相手装置が送信規制を行わない |
| desired       | desired        | 相手装置が送信規制を行う   |

(凡例)

on：有効。

off：無効。desired と組み合わせた設定の場合、ネゴシエーション結果によって動作します。フローコントロール動作は「表 15-17 オートネゴシエーション時のフローコントロール動作」を参照してください。

desired：有効。オートネゴシエーション選択時は、ネゴシエーション結果によって動作します。フローコントロール動作は「表 15-17 オートネゴシエーション時のフローコントロール動作」を参照してください。

表 15-16 フローコントロールの受信動作

| 本装置のポーズ<br>パケット受信 | 相手装置の<br>ポーズパケット送信 | フローコントロール動作   |
|-------------------|--------------------|---------------|
| on                | 有効                 | 本装置が送信規制を行う   |
| off               | 無効                 | 本装置が送信規制を行わない |
| desired           | desired            | 本装置が送信規制を行う   |

(凡例)

on：有効。

off：無効。desired と組み合わせた設定の場合、ネゴシエーション結果によって動作します。フローコントロール動作は「表 15-17 オートネゴシエーション時のフローコントロール動作」を参照してください。

desired：有効。オートネゴシエーション選択時は、ネゴシエーション結果によって動作します。フローコントロール動作は「表 15-17 オートネゴシエーション時のフローコントロール動作」を参照してください。

表 15-17 オートネゴシエーション時のフローコントロール動作

| 本装置               |                   | 相手装置              |                   | 本装置のオートネゴシエーション結果 |                   | フローコントロール動作  |               |    |      |
|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|--------------|---------------|----|------|
| ポーズパ<br>ケット送<br>信 | ポーズパ<br>ケット受<br>信 | ポーズパ<br>ケット送<br>信 | ポーズパ<br>ケット受<br>信 | ポーズパ<br>ケット送<br>信 | ポーズパ<br>ケット受<br>信 | 本装置の送<br>信規制 | 相手装置の<br>送信規制 |    |      |
| on                | desired           | 有効                | 有効                | on                | on                | 行う           | 行う            |    |      |
|                   |                   |                   | 無効                | on                | off               | 行わない         | 行わない          |    |      |
|                   |                   |                   | desired           | on                | on                | 行う           | 行う            |    |      |
|                   |                   | 無効                | 有効                | on                | on                | 行わない         | 行う            |    |      |
|                   |                   |                   | 無効                | on                | off               | 行わない         | 行わない          |    |      |
|                   |                   |                   | desired           | on                | on                | 行う           | 行う            |    |      |
|                   |                   | desired           | 有効                | on                | on                | 行う           | 行う            |    |      |
|                   |                   |                   | 無効                | on                | off               | 行わない         | 行わない          |    |      |
|                   |                   |                   | desired           | on                | on                | 行う           | 行う            |    |      |
|                   |                   | off               | desired           | 有効                | 有効                | on           | on            | 行う | 行う   |
|                   |                   |                   |                   |                   | 無効                | off          | on            | 行う | 行わない |
|                   |                   |                   |                   |                   | desired           | on           | on            | 行う | 行う   |
| 無効                | 有効                |                   |                   | on                | on                | 行わない         | 行う            |    |      |
|                   | 無効                |                   |                   | off               | off               | 行わない         | 行わない          |    |      |
|                   | desired           |                   |                   | on                | on                | 行う           | 行う            |    |      |
| desired           | 有効                |                   |                   | on                | on                | 行う           | 行う            |    |      |
|                   | 無効                |                   |                   | off               | on                | 行う           | 行わない          |    |      |
|                   | desired           |                   |                   | on                | on                | 行う           | 行う            |    |      |
| desired           | on                |                   |                   | 有効                | 有効                | on           | on            | 行う | 行う   |

| 本装置       |           | 相手装置      |           | 本装置のオートネゴシエーション結果 |           | フローコントロール動作 |           |      |
|-----------|-----------|-----------|-----------|-------------------|-----------|-------------|-----------|------|
| ポーズパケット送信 | ポーズパケット受信 | ポーズパケット送信 | ポーズパケット受信 | ポーズパケット送信         | ポーズパケット受信 | 本装置の送信規制    | 相手装置の送信規制 |      |
|           |           |           | 無効        | off               | on        | 行う          | 行わない      |      |
|           |           |           | desired   | on                | on        | 行う          | 行う        |      |
|           |           | 無効        | 有効        | on                | on        | 行わない        | 行う        |      |
|           |           |           | 無効        | off               | on        | 行わない        | 行わない      |      |
|           |           | desired   | desired   | on                | on        | 行う          | 行う        |      |
|           |           |           | 有効        | on                | on        | 行う          | 行う        |      |
|           |           | desired   | 無効        | off               | on        | 行わない        | 行わない      |      |
|           |           |           | desired   | on                | on        | 行う          | 行う        |      |
|           |           | off       | 有効        | 有効                | off       | off         | 行わない      | 行わない |
|           |           |           |           | 無効                | off       | off         | 行わない      | 行わない |
|           |           |           |           | desired           | off       | off         | 行わない      | 行わない |
|           |           |           | 無効        | 有効                | on        | off         | 行わない      | 行う   |
|           |           |           |           | 無効                | off       | off         | 行わない      | 行わない |
|           |           |           |           | desired           | on        | off         | 行わない      | 行う   |
|           | desired   |           | 有効        | off               | off       | 行わない        | 行わない      |      |
|           |           |           | 無効        | off               | off       | 行わない        | 行わない      |      |
|           |           |           | desired   | off               | off       | 行わない        | 行わない      |      |
|           | desired   |           | 有効        | 有効                | on        | on          | 行う        | 行う   |
|           |           |           |           | 無効                | off       | off         | 行わない      | 行わない |
|           |           |           |           | desired           | on        | on          | 行う        | 行う   |
|           |           | 無効        | 有効        | on                | on        | 行わない        | 行う        |      |
|           |           |           | 無効        | off               | off       | 行わない        | 行わない      |      |
|           |           |           | desired   | on                | on        | 行う          | 行う        |      |
|           |           | desired   | 有効        | on                | on        | 行う          | 行う        |      |
|           |           |           | 無効        | off               | off       | 行わない        | 行わない      |      |
|           |           |           | desired   | on                | on        | 行う          | 行う        |      |

#### (4) ジャンボフレーム

ジャンボフレームは、MAC ヘッダの DA ~ データが 1518 オクテットを超えるフレームを中継するための機能です。コンフィグレーションコマンド `ip mtu` の MTU 長を合わせて変更することで、IP パケットをフラグメント化するサイズを大きくすることも可能となります。

本装置では、Ethernet V2 形式フレームだけをサポートします。802.3 形式フレームはサポートしていません。フレームについては「15.1.3 MAC および LLC 副層制御」のフレームフォーマットを参照してください。Tagged フレームについては「19.1.5 VLAN Tag」の Tagged フレームのフォーマットを参照してください。ジャンボフレームのサポート機能を次の表に示します。

表 15-18 ジャンボフレームサポート機能

| 項目               | フレーム形式      |           | 内容                                                              |
|------------------|-------------|-----------|-----------------------------------------------------------------|
|                  | EthernetV2  | IEEE802.3 |                                                                 |
| フレーム長<br>(オクテット) | 1519 ~ 9596 | ×         | MAC ヘッダの DA ~ データの長さ。FCS は含みません。                                |
| 受信機能             |             | ×         | IEEE802.3 フレームは、LENGTH フィールド値が 0x05DD (1501 オクテット) 以上の場合に廃棄します。 |
| 送信機能             |             | ×         | IEEE802.3 フレームは送信しません。                                          |

(凡例) ○ : サポート × : 未サポート

注 「15.1.3 MAC および LLC 副層制御」のフレームフォーマットを参照してください。

#### (5) 1000BASE-X 接続時の注意事項

- 全二重のオートネゴシエーションおよび固定接続だけサポートします。
- 相手装置 (スイッチングハブなど) をオートネゴシエーションまたは全二重固定に設定してください。
- マニュアル「ハードウェア取扱説明書」に示すトランシーバ以外を使用した場合の動作は保証できません。

## 15.7 1000BASE-X のコンフィグレーション

---

### 15.7.1 ポートの設定

#### (1) 速度と duplex の設定

本装置と相手装置の伝送速度と duplex を設定できます。デフォルトではオートネゴシエーションで、相手装置と伝送速度と duplex を決定します。

##### [ 設定のポイント ]

通常は相手装置とオートネゴシエーションで接続します。本装置のデフォルトはオートネゴシエーションなので、速度と duplex を設定する必要はありません。オートネゴシエーションを使用しない場合は、速度を 1000Mbit/s に、duplex を全二重に設定します。

##### [ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/1

(config-if)# shutdown

(config-if)# speed 1000

(config-if)# duplex full

相手装置と 1000Mbit/s 全二重で接続する設定をします。

2. (config-if)# no shutdown

##### [ 注意事項 ]

回線速度を 1000Mbit/s に設定する場合は、必ず duplex も full (全二重) に設定してください。speed と duplex の両方が正しく設定されている場合以外は、オートネゴシエーションでの接続になります。

### 15.7.2 フローコントロールの設定

本装置内の受信バッファが枯渇して受信フレームを廃棄することがないようにするためには、ポーズパケットを送信して相手装置に送信規制を要求します。相手装置はポーズパケットを受信して送信規制する必要があります。

相手装置からのポーズパケットを受信したとき、本装置が送信規制するかどうかは設定に従います。本装置では、オートネゴシエーション時に相手装置とポーズパケットを送受信するかどうかを折衝できます。

##### [ 設定のポイント ]

フローコントロールの設定内容は、相手装置と矛盾しないように決定してください。

##### [ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/1

(config-if)# shutdown

(config-if)# flowcontrol send off

(config-if)# flowcontrol receive off

相手装置とのポーズパケット送受信を停止します。

2. (config-if)# no shutdown

## 15.8 10GBASE-R の解説

### 15.8.1 機能一覧

10GBASE-R の光ファイバを使用したインタフェースについて説明します。

#### (1) 接続インタフェース

##### (a) 10GBASE-R

10GBASE-SR, 10GBASE-LR, 10GBASE-ER, および 10GBASE-ZR をサポートしています。回線速度は 10Gbit/s 全二重固定です。

10GBASE-SR :

短距離間を接続するために使用します。(マルチモード, 伝送距離: 最大 300m )

注

伝送距離は使用するケーブルによって異なります。ケーブルごとの伝送距離は、マニュアル「ハードウェア取扱説明書」を参照してください。

10GBASE-LR :

中距離間を接続するために使用します。(シングルモード, 伝送距離: 最大 10km)

10GBASE-ER :

長距離間を接続するために使用します。(シングルモード, 伝送距離: 最大 40km)

10GBASE-ZR :

長距離間を接続するために使用します。(シングルモード, 伝送距離: 最大 80km)

##### (b) 10GBASE-R 接続仕様

本装置の物理仕様については、マニュアル「ハードウェア取扱説明書」を参照してください。

#### (2) フローコントロール

フローコントロールは、装置内の受信バッファ枯渇でフレームを廃棄しないように、相手装置にフレームの送信をポーズパケットによって、一時的に停止指示する機能です。自装置がポーズパケット受信時は、送信規制を行います。

本装置では、受信バッファの使用状況を監視し、相手装置の送信規制を行う場合、ポーズパケットを送信します。本装置がポーズパケット受信時は、送信規制を行います。フローコントロールのコンフィグレーションは、送信と受信とでそれぞれ設定でき、有効または無効モードを選択できます。本装置と相手装置の設定を送信と受信が一致するように合わせてください。例えば、本装置のポーズパケット送信を on に設定した場合、相手装置のポーズパケット受信は有効に設定してください。本装置と相手装置の設定内容と実行動作を「表 15-19 フローコントロールの送信動作」および「表 15-20 フローコントロールの受信動作」に示します。

表 15-19 フローコントロールの送信動作

| 本装置のポーズパケット送信 | 相手装置のポーズパケット受信 | フローコントロール動作    |
|---------------|----------------|----------------|
| on            | 有効             | 相手装置が送信規制を行う   |
| off           | 無効             | 相手装置が送信規制を行わない |

| 本装置のポーズ<br>パケット送信 | 相手装置の<br>ポーズパケット受信 | フローコントロール<br>動作 |
|-------------------|--------------------|-----------------|
| desired           | desired            | 相手装置が送信規制を行う    |

(凡例) on : 有効 off : 無効 desired : 有効

表 15-20 フローコントロールの受信動作

| 本装置のポーズ<br>パケット受信 | 相手装置の<br>ポーズパケット送信 | フローコントロール<br>動作 |
|-------------------|--------------------|-----------------|
| on                | 有効                 | 本装置が送信規制を行う     |
| off               | 無効                 | 本装置が送信規制を行わない   |
| desired           | desired            | 本装置が送信規制を行う     |

(凡例) on : 有効 off : 無効 desired : 有効

### (3) ジャンボフレーム

ジャンボフレームは、MAC ヘッダの DA ~ データが 1518 オクテットを超えるフレームを中継するための機能です。コンフィグレーションコマンド ip mtu の MTU 長を合わせて変更することで、IP パケットをフラグメント化するサイズを大きくすることもできます。

本装置では、Ethernet V2 形式フレームだけをサポートします。802.3 形式フレームはサポートしていません。フレームについては「15.1.3 MAC および LLC 副層制御」のフレームフォーマットを参照してください。Tagged フレームについては「19.1.5 VLAN Tag」の Tagged フレームのフォーマットを参照してください。ジャンボフレームのサポート機能を次の表に示します。

表 15-21 ジャンボフレームサポート機能

| 項目               | フレーム形式                  |                        | 内容                                                              |
|------------------|-------------------------|------------------------|-----------------------------------------------------------------|
|                  | EthernetV2 <sup>1</sup> | IEEE802.3 <sup>1</sup> |                                                                 |
| フレーム長<br>(オクテット) | 1519 ~ 9596             | ×                      | MAC ヘッダの DA ~ データの長さ。FCS は含みません。                                |
| 受信機能             |                         | ×                      | IEEE802.3 フレームは、LENGTH フィールド値が 0x05DD (1501 オクテット) 以上の場合に廃棄します。 |
| 送信機能             |                         | ×                      | IEEE802.3 フレームは送信しません。                                          |

(凡例) : サポート × : 未サポート

注 1 「15.1.3 MAC および LLC 副層制御」のフレームフォーマットを参照してください。

### (4) 10GBASE-R 接続時の注意事項

- 10GBASE-R の半二重およびオートネゴシエーションは IEEE802.3ae 規格にないので、全二重固定接続だけになります。
- マニュアル「ハードウェア取扱説明書」に示すトランシーバ以外を使用した場合の動作は保証できません。
- 10GBASE-ZR は IEEE802.3ae 規格にない独自仕様ですので、他ベンダーの装置と接続した場合の動作は保証できません。

## 15.9 10GBASE-R のコンフィグレーション

---

### 15.9.1 フローコントロールの設定

本装置内の受信バッファが枯渇して受信フレームを廃棄することがないようにするためには、ポーズパケットを送信して相手装置に送信規制を要求します。また、相手装置でポーズパケットを受信して送信規制できる必要があります。

相手装置からのポーズパケットを受信したとき、本装置が送信規制するかどうかは設定に従います。

[ 設定のポイント ]

フローコントロールの設定内容は、相手装置と矛盾しないように決定してください。

[ コマンドによる設定 ]

1. `(config)# interface tengigabitethernet 1/1`  
`(config-if)# shutdown`  
イーサネットインタフェースをシャットダウンします。
2. `(config-if)# flowcontrol send off`  
`(config-if)# flowcontrol receive off`  
相手装置とのポーズパケット送受信を停止します。
3. `(config-if)# no shutdown`  
イーサネットインタフェースのシャットダウンを解除します。



# 16 リンクアグリゲーション

この章では、リンクアグリゲーションの解説と操作方法について説明します。

- 
- 16.1 リンクアグリゲーション基本機能の解説
  - 16.2 リンクアグリゲーション基本機能のコンフィグレーション
  - 16.3 リンクアグリゲーション拡張機能の解説
  - 16.4 リンクアグリゲーション拡張機能のコンフィグレーション
  - 16.5 リンクアグリゲーションのオペレーション
-

## 16.1 リンクアグリゲーション基本機能の解説

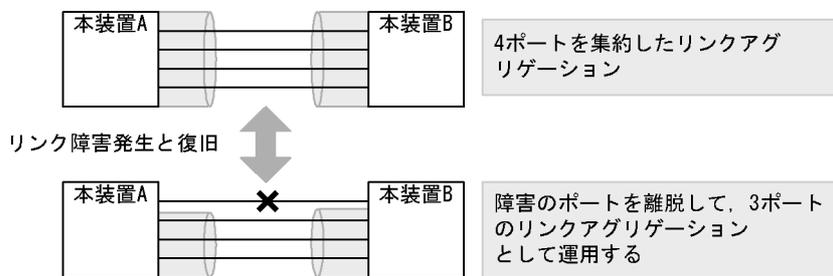
### 16.1.1 概要

リンクアグリゲーションは、隣接装置との間を複数のイーサネットポートで接続し、それらを束ねて一つの仮想リンクとして扱う機能です。この仮想リンクをチャンネルグループと呼びます。リンクアグリゲーションによって接続装置間の帯域の拡大や冗長性を確保できます。

### 16.1.2 リンクアグリゲーションの構成

リンクアグリゲーションの構成例を次の図に示します。この例では四つのポートを集約しています。集約しているポートのうちの1本が障害となった場合には、チャンネルグループから離脱し、残りのポートでチャンネルグループとして通信を継続します。

図 16-1 リンクアグリゲーションの構成例



### 16.1.3 サポート仕様

#### (1) リンクアグリゲーションのモード

本装置のリンクアグリゲーションは、モードとしてLACPおよびスタティックの2種類をサポートします。

- LACP リンクアグリゲーション  
IEEE802.3ad 準拠の LACP を利用したリンクアグリゲーションです。LACP によるネゴシエーションが成功した場合にチャンネルグループとしての運用を開始します。LACP によって、隣接装置との整合性確認やリンクの正常性確認ができます。
- スタティックリンクアグリゲーション  
コンフィグレーションによるスタティックなリンクアグリゲーションです。LACP は動作させません。チャンネルグループとして設定したポートがリンクアップした時点で運用を開始します。

リンクアグリゲーションのサポート仕様を次の表に示します。

表 16-1 リンクアグリゲーションのサポート仕様

| 項目              | サポート仕様                                                                     | 備考                                               |
|-----------------|----------------------------------------------------------------------------|--------------------------------------------------|
| リンクアグリゲーションのモード | <ul style="list-style-type: none"> <li>• LACP</li> <li>• スタティック</li> </ul> | -                                                |
| ポート速度           | デフォルト時：同一速度だけを使用します。<br>異速度混在モード時：異なる速度を同時に使用します。                          | デフォルト時：遅い回線は離脱します。<br>異速度混在モード時：回線速度による離脱はありません。 |

| 項目         | サポート仕様 | 備考 |
|------------|--------|----|
| Duplex モード | 全二重だけ  | -  |

(凡例) - : 該当しない

### 16.1.4 チャネルグループの MAC アドレス

スパニングツリーなどのプロトコルを運用する際に、チャネルグループの MAC アドレスを使用します。本装置は、チャネルグループの MAC アドレスとして、グループごとにユニークな MAC アドレスを使用します。

### 16.1.5 フレーム送信時のポート振り分け

リンクアグリゲーションへフレームを送信するとき、送信するフレームごとにポートを選択しトラフィックを各ポートへ分散させることで複数のポートを効率的に利用します。ポートの振り分けは、フレーム内情報による振り分け方法と VLAN ごとの振り分け方法の 2 種類があり、コンフィグレーションによってチャネルグループごとに指定できます。

#### (1) フレーム内情報によるポート振り分け

リンクアグリゲーションへフレームを送信するとき、フレーム内の情報を基にポートを選択して送信します。フレーム内の情報の参照方法は、レイヤ 2 中継時と IP レイヤ中継時では異なります。それぞれの参照情報を次の表に示します。

表 16-2 レイヤ 2 中継時の参照情報

| 分類                            | 中継 (受信フレーム)                                                                                                                                                     | 自発送信 (送信フレーム)                                                                       |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| TCP/UDP/SCTP のフレーム            | <ul style="list-style-type: none"> <li>宛先 MAC アドレス</li> <li>送信元 MAC アドレス</li> <li>宛先 IP アドレス</li> <li>送信元 IP アドレス</li> <li>宛先ポート番号</li> <li>送信元ポート番号</li> </ul> | -                                                                                   |
| IP のフレーム<br>(TCP/UDP/SCTP 以外) | <ul style="list-style-type: none"> <li>宛先 MAC アドレス</li> <li>送信元 MAC アドレス</li> <li>宛先 IP アドレス</li> <li>送信元 IP アドレス</li> </ul>                                    | -                                                                                   |
| その他のフレーム                      | <ul style="list-style-type: none"> <li>宛先 MAC アドレス</li> <li>送信元 MAC アドレス</li> </ul>                                                                             | <ul style="list-style-type: none"> <li>宛先 MAC アドレス</li> <li>送信元 MAC アドレス</li> </ul> |

(凡例) - : 該当しない

表 16-3 IP レイヤ中継時の参照情報

| 分類                            | 中継 (受信フレーム)                                                                                                          | 自発送信 (送信フレーム)                                                                                                        |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| TCP/UDP/SCTP のフレーム            | <ul style="list-style-type: none"> <li>宛先 IP アドレス</li> <li>送信元 IP アドレス</li> <li>宛先ポート番号</li> <li>送信元ポート番号</li> </ul> | <ul style="list-style-type: none"> <li>宛先 IP アドレス</li> <li>送信元 IP アドレス</li> <li>宛先ポート番号</li> <li>送信元ポート番号</li> </ul> |
| IP のフレーム<br>(TCP/UDP/SCTP 以外) | <ul style="list-style-type: none"> <li>宛先 IP アドレス</li> <li>送信元 IP アドレス</li> </ul>                                    | <ul style="list-style-type: none"> <li>宛先 IP アドレス</li> <li>送信元 IP アドレス</li> </ul>                                    |
| その他のフレーム                      | -                                                                                                                    | -                                                                                                                    |

(凡例) - : 該当しない

(2) VLAN ごとのポート振り分け

リンクアグリゲーションへフレームを送信するとき、フレームを送信したい VLAN ごとに宛先ポートを選択して送信します。振り分けに使用する情報は、VLAN ごとに割り当てられている本装置の内部的な識別子を使用します。Tag 変換を使用していて異なる VLAN Tag が付与されたフレームであっても、同じ VLAN は同じポートに振り分けられます。振り分けモードでの動作を次の表に示します。

表 16-4 VLAN ごとのポート振り分け動作

| 動作分類     | 情報元                    |
|----------|------------------------|
| レイヤ 2 中継 | フレームを送信する VLAN ごとに振り分け |
| IP レイヤ中継 | フレームを送信する VLAN ごとに振り分け |
| 自発送信     | 送信する VLAN ごとに振り分け      |

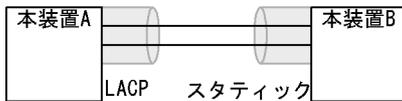
16.1.6 リンクアグリゲーション使用時の注意事項

(1) リンクアグリゲーションが不可能な構成

リンクアグリゲーション構成時には、装置間での設定が一致している必要があります。リンクアグリゲーションが不可能な構成例を次に示します。

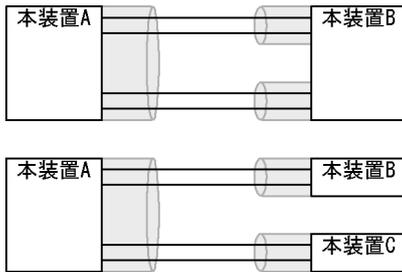
図 16-2 リンクアグリゲーションが不可能な構成例

●装置間でモードが異なる場合



この構成を実施したときの動作  
 ・ LACP のネゴシエーションが成立しないで通信断状態になる。

●装置間でチャネルグループがポイントーマルチポイントになっている場合



この構成を実施したときの動作  
 ・ 本装置Aから送信したフレームが本装置Bを経由して戻るなど、ループ構成となって正常に動作しない。

(2) リンクアグリゲーションの設定手順

リンクアグリゲーション構成時には、装置間での設定が一致している必要があります。一致していない状態で通信を開始しようとするるとループ構成となるおそれがあります。設定はリンクダウン状態で行い、「(1) リンクアグリゲーションが不可能な構成」のような構成になっていないことを確認したあとで、ポートをリンクアップさせることをお勧めします。

### (3) CPU 過負荷時

LACP リンクアグリゲーションモード使用時に CPU が過負荷な状態になった場合、本装置が送受信する LACPDU の廃棄または処理遅延が発生して、タイムアウトのメッセージ出力、一時的な通信断になることがあります。過負荷状態が頻発する場合は、LACPDU の送信間隔を長くするか、スタティックリンクアグリゲーションを使用してください。

## 16.2 リンクアグリゲーション基本機能のコンフィグレーション

### 16.2.1 コンフィグレーションコマンド一覧

リンクアグリゲーション基本機能のコンフィグレーションコマンド一覧を次の表に示します。

表 16-5 コンフィグレーションコマンド一覧

| コマンド名                              | 説明                                                                            |
|------------------------------------|-------------------------------------------------------------------------------|
| channel-group lacp system-priority | チャンネルグループごとに LACP システム優先度を設定します。                                              |
| channel-group load-balance         | 振り分け方法を指定します。                                                                 |
| channel-group mode                 | ポートをチャンネルグループに登録します。                                                          |
| channel-group periodic-timer       | LACPDU の送信間隔を設定します。                                                           |
| description                        | チャンネルグループの補足説明を設定します。                                                         |
| interface port-channel             | ポートチャンネルインタフェースを設定します。<br>チャンネルグループのパラメータもポートチャンネルインタフェースコンフィグレーションモードで設定します。 |
| lacp port-priority                 | LACP のポート優先度を設定します。                                                           |
| lacp system-priority               | LACP システム優先度のデフォルト値を設定します。                                                    |
| shutdown                           | チャンネルグループに登録したポートを shutdown にして通信を停止します。                                      |

### 16.2.2 スタティックリンクアグリゲーションの設定

#### [ 設定のポイント ]

スタティックリンクアグリゲーションは、イーサネットインタフェースコンフィグレーションモードで channel-group mode コマンドを使用してチャンネルグループ番号と「on」のモードを設定します。スタティックリンクアグリゲーションは channel-group mode コマンドを設定することによって動作を開始します。

#### [ コマンドによる設定 ]

1. (config)# interface range gigabitethernet 1/1-2  
ポート 1/1, 1/2 のイーサネットインタフェースモードに移行します。
2. (config-if-range)# channel-group 10 mode on  
ポート 1/1, 1/2 を、スタティックモードのチャンネルグループ 10 に登録します。

### 16.2.3 LACP リンクアグリゲーションの設定

#### (1) チャンネルグループの設定

#### [ 設定のポイント ]

LACP リンクアグリゲーションは、イーサネットインタフェースコンフィグレーションモードで channel-group mode コマンドを使用してチャンネルグループ番号と「active」または「passive」のモードを設定します。

## [ コマンドによる設定 ]

1. (config)# interface range gigabitethernet 1/1-2  
ポート 1/1, 1/2 のイーサネットインタフェースモードに移行します。
2. (config-if-range)# channel-group 10 mode active  
ポート 1/1, 1/2 を LACP モードのチャネルグループ 10 に登録します。LACP は active モードとして対向装置に関係なく LACPDU の送信を開始します。passive を指定した場合は、対向装置からの LACPDU を受信したときだけ LACPDU の送信を開始します。

## (2) システム優先度の設定

LACP のシステム優先度を設定します。本装置では、システム優先度は拡張機能の離脱ポート制限機能で使われます。通常、本パラメータを変更する必要はありません。

## [ 設定のポイント ]

LACP システム優先度は値が小さいほど高い優先度となります。

## [ コマンドによる設定 ]

1. (config)# lacp system-priority 100  
本装置の LACP システム優先度を 100 に設定します。
2. (config)# interface port-channel 10  
(config-if)# channel-group lacp system-priority 50  
チャネルグループ 10 の LACP システム優先度を 50 に設定します。本設定を行わない場合は装置のシステム優先度である 100 を使用します。

## (3) ポート優先度の設定

LACP のポート優先度を設定します。本装置では、ポート優先度は拡張機能のスタンバイリンク機能で使われます。通常、本パラメータを変更する必要はありません。

## [ 設定のポイント ]

LACP ポート優先度は値が小さいほど高い優先度となります。

## [ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/1  
(config-if)# lacp port-priority 100  
ポート 1/1 の LACP ポート優先度を 100 に設定します。

## (4) LACPDU 送信間隔の設定

## [ 設定のポイント ]

対向装置が本装置に向けて送信する LACPDU の間隔を設定します。本装置は本パラメータで設定した間隔で LACPDU を受信します。

LACPDU の送信間隔は long (30 秒), short (1 秒) のどちらかを選択します。デフォルトは long (30 秒) で動作します。送信間隔を short (1 秒) に変更した場合、リンクの障害によるタイムアウトを検知しやすくなり、障害時に通信が途絶える時間を短く抑えることができます。

## [ コマンドによる設定 ]

1. (config)# interface port-channel 10  
 (config-if)# channel-group periodic-timer short  
 チャンネルグループ 10 の LACPDU 送信間隔を short (1 秒) に設定します。

## [ 注意事項 ]

LACPDU 送信間隔を short (1 秒) に設定すると、障害を検知しやすくなる一方で、LACPDU トラフィックが増加することによってリンクアグリゲーションプログラムの負荷が増加します。本パラメータを short (1 秒) にすることでタイムアウトのメッセージや一時的な通信断が頻発する場合は、デフォルトの long (30 秒) に戻すかスタティックモードを使用してください。

## (5) 振り分け方法の設定

## [ 設定のポイント ]

チャンネルグループに振り分け方法を指定します。

## [ コマンドによる設定 ]

1. (config)# interface port-channel 10  
 (config-if)# channel-group load-balance mac-ip-port  
 チャンネルグループ 10 の振り分け方法を受信フレーム内情報によって振り分けるように設定します。

## 16.2.4 ポートチャンネルインタフェースの設定

ポートチャンネルインタフェースでは、チャンネルグループ上で動作する機能を設定します。

ポートチャンネルインタフェースは、コンフィグレーションコマンドで設定するか、イーサネットインタフェースコンフィグレーションモードで channel-group mode コマンドを設定することによって自動的に生成されます。

## (1) ポートチャンネルインタフェースとイーサネットインタフェースの関係

ポートチャンネルインタフェースは、チャンネルグループ上で動作する機能を設定します。それらはイーサネットインタフェースコンフィグレーションモードでも設定することができます。このような機能を設定するコマンドはポートチャンネルインタフェースとイーサネットインタフェースで関連性があり、設定する際に次のように動作します。

- ポートチャンネルインタフェースとイーサネットインタフェースで関連コマンドの設定が一致している必要があります。
- ポートチャンネルインタフェースを未設定の状態にイーサネットインタフェースに channel-group mode コマンドを設定すると、自動的にポートチャンネルインタフェースを生成します。このとき、channel-group mode コマンドを設定するイーサネットインタフェースに関連コマンドが設定されていないはいけません。
- ポートチャンネルインタフェースがすでに設定済みの状態でイーサネットインタフェースに channel-group mode コマンドを設定する場合、関連コマンドが一致している必要があります。
- ポートチャンネルインタフェースで関連コマンドを設定すると、channel-group mode コマンドで登録されているイーサネットインタフェースの設定にも同じ設定が反映されます。

ポートチャンネルインタフェースとイーサネットインタフェースで一致している必要のあるポートチャンネル関連コマンドを次の表に示します。

表 16-6 ポートチャンネルインタフェースの関連コマンド

| 機能            | コマンド                               |
|---------------|------------------------------------|
| VLAN          | switchport mode                    |
|               | switchport access                  |
|               | switchport trunk                   |
|               | switchport protocol                |
|               | switchport mac                     |
|               | switchport vlan mapping            |
|               | switchport vlan mapping enable     |
| スパンニングツリー     | spanning-tree portfast             |
|               | spanning-tree bpdufilter           |
|               | spanning-tree bpduguard            |
|               | spanning-tree guard                |
|               | spanning-tree link-type            |
|               | spanning-tree port-priority        |
|               | spanning-tree cost                 |
|               | spanning-tree vlan port-priority   |
|               | spanning-tree vlan cost            |
|               | spanning-tree single port-priority |
|               | spanning-tree single cost          |
|               | spanning-tree mst port-priority    |
|               | spanning-tree mst cost             |
| IEEE802.1X    | dot1x port-control                 |
|               | dot1x force-authorize-port         |
|               | dot1x multiple-hosts               |
|               | dot1x multiple-authentication      |
|               | dot1x max-supplicant               |
|               | dot1x reauthentication             |
|               | dot1x timeout reauth-period        |
|               | dot1x timeout tx-period            |
|               | dot1x timeout supp-timeout         |
|               | dot1x timeout server-timeout       |
|               | dot1x timeout keep-unauth          |
|               | dot1x timeout quiet-period         |
|               | dot1x max-req                      |
|               | dot1x ignore-eapol-start           |
|               | dot1x supplicant-detection         |
| DHCP snooping | ip dhcp snooping trust             |
|               | ip arp inspection trust            |
|               | ip verify source                   |
| GSRP          | gsrp direct-link                   |
|               | gsrp reset-flush-port              |

| 機能       | コマンド                |
|----------|---------------------|
|          | gsrp no-flush-port  |
|          | gsrp exception-port |
| L2 ループ検知 | loop-detection      |
| OADP     | oadp enable         |

## (2) チャネルグループ上で動作する機能の設定

### [ 設定のポイント ]

ポートチャネルインタフェースでは、VLAN やスパンニングツリーなど、チャネルグループ上で動作する機能を設定します。ここでは、トランクポートを設定する例を示します。

### [ コマンドによる設定 ]

1. (config)# interface range gigabitethernet 1/1-2  
(config-if-range)# channel-group 10 mode on  
(config-if-range)# exit  
ポート 1/1, 1/2 をスタティックモードのチャネルグループ 10 に登録します。また、チャネルグループ 10 のポートチャネルインタフェースが自動生成されます。
2. (config)# interface port-channel 10  
チャネルグループ 10 のポートチャネルインタフェースコンフィギュレーションモードに移行します。
3. (config-if)# switchport mode trunk  
チャネルグループ 10 をトランクポートに設定します。

## (3) ポートチャネルインタフェースの shutdown

### [ 設定のポイント ]

ポートチャネルインタフェースを shutdown に設定すると、チャネルグループに登録されているすべてのポートの通信を停止します。リンクアップしているポートはアップ状態のまま通信停止状態になります。

### [ コマンドによる設定 ]

1. (config)# interface range gigabitethernet 1/1-2  
(config-if-range)# channel-group 10 mode on  
(config-if-range)# exit  
ポート 1/1, 1/2 をスタティックモードのチャネルグループ 10 として登録します。
2. (config)# interface port-channel 10  
(config-if)# shutdown  
ポートチャネルインタフェースコンフィギュレーションモードに移行して shutdown を設定します。ポート 1/1, 1/2 の通信が停止し、チャネルグループ 10 は停止状態になります。

## 16.2.5 チャネルグループの削除

チャネルグループのポートやチャネルグループ全体を削除する場合は、削除する対象のポートをあらかじめ

イーサネットインタフェースコンフィグレーションモードで shutdown に設定しておく必要があります。shutdown に設定することで、削除する際にループが発生することを防ぎます。

## (1) チャネルグループ内のポートの削除

### [ 設定のポイント ]

ポートをチャネルグループから削除します。削除したポートはチャネルグループとは別のポートとして動作するため、削除時のループを回避するために事前に次のどちらかを実施してください。

- イーサネットインタフェースコンフィグレーションモードで shutdown を設定
- 省電力機能のコンフィグレーションコマンド schedule-power-control shutdown で、ポートを disable 状態に設定 **【AX6700S】【AX6600S】**

削除したポートには、削除前に interface port-channel で設定した関連コマンド（表 16-6 ポートチャネルインタフェースの関連コマンド）は残るため、別の用途に使用する際には注意してください。チャネルグループ内のすべてのポートを削除しても、interface port-channel の設定は自動的に削除されません。チャネルグループ全体の削除は、「(2) チャネルグループ全体の削除」を参照してください。

### [ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/1  
(config-if)# shutdown  
ポート 1/1 をチャネルグループから削除するために、事前に shutdown にしてリンクダウンさせます。
2. (config-if)# no channel-group  
ポート 1/1 からチャネルグループの設定を削除します。

## (2) チャネルグループ全体の削除

### [ 設定のポイント ]

チャネルグループ全体を削除します。削除したチャネルグループに登録していたポートはそれぞれ個別のポートとして動作するため、削除時のループを回避するために事前に shutdown に設定します。チャネルグループは interface port-channel を削除することによって、全体が削除されます。この削除によって、登録していた各ポートから channel-group mode コマンドが自動的に削除されます。ただし、各ポートには削除前に interface port-channel で設定した関連コマンド（表 16-6 ポートチャネルインタフェースの関連コマンド）は残るため、別の用途に使用する際には注意してください。

### [ コマンドによる設定 ]

1. (config)# interface range gigabitethernet 1/1-2  
(config-if-range)# shutdown  
(config-if-range)# exit  
チャネルグループ全体を削除するために、削除したいチャネルグループに登録されているポートをすべて shutdown に設定しリンクダウンさせます。
2. (config)# no interface port-channel 10  
チャネルグループ 10 を削除します。ポート 1/1、1/2 に設定されている channel-group mode コマンドも自動的に削除されます。

## 16.3 リンクアグリゲーション拡張機能の解説

### 16.3.1 スタンバイリンク機能

#### (1) 解説

チャンネルグループ内にあらかじめ待機用のポートを用意しておき、運用中のポートで障害が発生したときに待機用のポートに切り替えることによって、グループとして運用するポート数を維持する機能です。この機能を使用すると、障害時に帯域の減少を防ぐことができます。

この機能は、スタティックリンクアグリゲーションだけ使用できます。

#### (2) スタンバイリンクの選択方法

コンフィグレーションでチャンネルグループとして運用する最大ポート数を設定します。グループに属するポート数が指定された最大ポート数を越えた分のポートが待機用ポートになります。

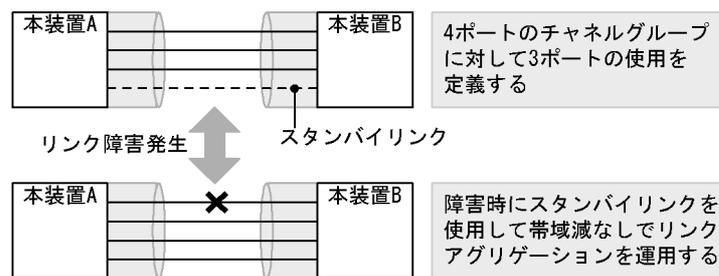
待機用ポートは、コンフィグレーションで設定するポート優先度、NIF 番号、ポート番号から選択されます。待機用ポートは、次の表に示すように選択優先度の高い順に決定します。

表 16-7 待機用ポートの選択方法

| 選択優先度 | パラメータ  | 備考                      |
|-------|--------|-------------------------|
| 高     | ポート優先度 | 優先度の低いポートから待機用ポートとして選択  |
|       | NIF 番号 | NIF 番号の大きい順に待機用ポートとして選択 |
|       | ポート番号  | ポート番号の大きい順に待機用ポートとして選択  |
| 低     |        |                         |

スタンバイリンク機能の例を次の図に示します。この例では、グループに属するポート数を 4、運用する最大ポート数を 3 としています。

図 16-3 スタンバイリンク機能の構成例



#### (3) スタンバイリンクのモード

スタンバイリンク機能には、次に示す二つのモードがあります。

- リンクダウンモード  
スタンバイリンクをリンクダウン状態にします。スタンバイリンク機能をサポートしていない対向装置も待機用ポートにすることができます。
- 非リンクダウンモード  
スタンバイリンクをリンクダウン状態にしないで、送信だけを停止します。リンクアップ状態のため、

待機中のポートでも障害を監視できます。また、待機中のポートは送信だけを停止して、受信は行います。スタンバイリンク機能をサポートしていない対向装置は、リンクダウンが伝わらないためスタンバイリンク上で送信を継続しますが、そのような対向装置とも接続できます。

リンクダウンモードを使用している場合、運用中のポートが一つするとき、そのポートで障害が発生すると、待機用のポートに切り替わる際にチャンネルグループがいったんダウンします。非リンクダウンモードの場合、ダウンせずに待機用ポートを使用します。

運用中のポートが一つの状態とは、次に示すどちらかの状態です。

- コンフィグレーションコマンド `max-active-port` で 1 を設定している状態。
- 異速度混在モードを未設定で、最高速のポートが一つだけ、そのほかのポートが一つ以上ある状態。

### 16.3.2 離脱ポート制限機能

離脱ポート制限機能は、リンクに障害が発生したポートを離脱して残りのポートで運用を継続する機能を抑止します。チャンネルグループのどれかのポートに障害が発生するとグループ全体を障害とみなして、該当チャンネルグループの運用を停止します。グループ内の全ポートが復旧するとグループの運用を再開します。

GSRP などの冗長化機能と合わせて運用することで、チャンネルグループ内に 1 ポートだけ障害が発生した場合でも、グループ単位で経路を切り替えることができます。

この機能は LACP リンクアグリゲーションだけ使用できます。

離脱ポート制限機能の集約動作は、チャンネルグループで接続する装置間で、優先度の高い装置が、自装置および対向装置のチャンネルグループ内の全ポートで集約可能な状態と判断できた場合に集約します。そうすることで、一部のポートだけが集約することがないようにしており、帯域保証しています。

優先度は、コンフィグレーションで設定する LACP システム優先度、チャンネルグループの MAC アドレスによって、次の表に示すように決定します。すなわち LACP システム優先度が同じだった場合は、チャンネルグループの MAC アドレスで判断します。

表 16-8 チャンネルグループ内の全ポートが集約可能か判定する装置の決定方法

| 優先度 | パラメータ               | 備考                      |
|-----|---------------------|-------------------------|
| 高   | LACP システム優先度        | LACP システム優先度の値が小さい装置が優先 |
| 低   | チャンネルグループの MAC アドレス | MAC アドレスの小さい装置が優先       |

### 16.3.3 異速度混在モード

異なる速度のポートを一つのチャンネルグループで同時に使用するモードです。通常は同じ速度のポートでチャンネルグループを構成しますが、異なる速度のポートで構成することで、スタンバイリンクに低速ポートを使用することや、チャンネルグループの構成変更を容易に行えます。本機能の適用例を次に示します。

なお、フレーム送信時のポート振り分けにはポートの速度は反映しません。例えば、異速度混在モードで 1Gbit/s のポートと 10Gbit/s のポートを使用している場合、その速度の差はフレーム振り分けには反映しません。通常の運用時は同じ速度のポートで運用することをお勧めします。

#### (1) スタンバイリンク機能での適用例

高速なポートに対して低速なポートを待機用ポートにすることができます。例えば、10Gbit/s ポートで接

続する際に、最大ポート数を 1 としてスタンバイリンク機能を適用して、待機用ポートに 1Gbit/s のポートを設定します。10Gbit/s のポートに障害が発生した場合にも 1Gbit/s のポートで通信を継続できます。

異速度混在モードでスタンバイリンクを適用する際は、最大ポート数を 1 とすることをお勧めします。最大ポート数を 2 以上とした場合は、通常運用に異なる速度のポートが混在することがあります。また、最大ポート数を 1 として運用する場合は、非リンクダウンモードを使用することをお勧めします。リンクダウンモードで最大ポート数が 1 の場合は、切り替え時にチャンネルグループがいったんダウンします。

## (2) チャンネルグループの構成変更手順での適用例

本機能によって、チャンネルグループで利用するポートの速度を変更（ネットワーク構成の変更）する際に、チャンネルグループをダウンさせないで構成を変更できます。

異速度混在モードを利用したチャンネルグループの速度移行について、移行手順の具体例を次に示します。

1. 従来状態で運用（1Gbit/s の 2 ポートとします）
2. 異速度混在モードを設定
3. チャンネルグループに 10Gbit/s の 2 ポートを追加  
異速度混在モード未設定時は、この手順でリンクアグリゲーションがいったんダウンします。
4. 手順 3 で追加した 10Gbit/s の 2 ポートをリンクアップ
5. 従来の 1Gbit/s の 2 ポートをリンクダウン
6. 従来の 1Gbit/s の 2 ポートをチャンネルグループから削除
7. 10Gbit/s の 2 ポートに移行完了

## 16.4 リンクアグリゲーション拡張機能のコンフィグレーション

### 16.4.1 コンフィグレーションコマンド一覧

リンクアグリゲーション拡張機能のコンフィグレーションコマンド一覧を次の表に示します。

表 16-9 コンフィグレーションコマンド一覧

| コマンド名                              | 説明                                                     |
|------------------------------------|--------------------------------------------------------|
| channel-group lacp system-priority | システム優先度をチャンネルグループごとに設定します。離脱ポート制限機能で集約条件を判定する装置を決定します。 |
| channel-group max-active-port      | スタンバイリンク機能を設定し、最大ポート数を指定します。                           |
| channel-group max-detach-port      | 離脱ポート制限機能を設定します。                                       |
| channel-group multi-speed          | 異速度混在モードを設定します。                                        |
| lacp port-priority                 | ポート優先度を設定します。スタンバイリンクを選択するために使用します。                    |
| lacp system-priority               | システム優先度のデフォルト値を設定します。離脱ポート制限機能で集約条件を判定する装置を決定します。      |

### 16.4.2 スタンバイリンク機能のコンフィグレーション

#### [ 設定のポイント ]

チャンネルグループにスタンバイリンク機能を設定して、同時に最大ポート数を設定します。また、リンクダウンモード、非リンクダウンモードのどちらかを設定します。スタンバイリンク機能は、スタンバイリンクアグリゲーションだけで使用できます。

待機用ポートはポート優先度によって設定し、優先度が低いポートからスタンバイリンクに選択します。ポート優先度は値が小さいほど高い優先度になります。

#### [ コマンドによる設定 ]

1. `(config)# interface port-channel 10`  
チャンネルグループ 10 のポートチャンネルインタフェースコンフィグレーションモードに移行します。
2. `(config-if)# channel-group max-active-port 3`  
チャンネルグループ 10 にスタンバイリンク機能を設定して、最大ポート数を 3 に設定します。チャンネルグループ 10 はリンクダウンモードで動作します。
3. `(config-if)# exit`  
グローバルコンフィグレーションモードに戻ります。
4. `(config)# interface port-channel 20`  
`(config-if)# channel-group max-active-port 1 no-link-down`  
`(config-if)# exit`  
チャンネルグループ 20 のポートチャンネルインタフェースコンフィグレーションモードに移行して、スタンバイリンク機能を設定します。最大ポート数を 1 とし、非リンクダウンモードを設定します。
5. `(config)# interface gigabitethernet 1/1`

```
(config-if)# channel-group 20 mode on
(config-if)# lacp port-priority 300
```

チャンネルグループ 20 にポート 1/1 を登録して、ポート優先度を 300 に設定します。ポート優先度は値が小さいほど優先度が高く、ポート優先度のデフォルト値の 128 よりもスタンバイリンクに選択されやすくなります。

### 16.4.3 離脱ポート制限機能のコンフィグレーション

#### [ 設定のポイント ]

チャンネルグループに離脱ポート制限機能を設定します。本コマンドではチャンネルグループから離脱することを許容する最大ポート数に 0 と 15 のどちらかを指定します。15 を指定した場合は離脱ポート制限機能を設定しない場合と同じです。

離脱ポート制限機能をサポートしている装置と接続する場合、接続先の装置と本設定を合わせてください。離脱ポート制限機能をサポートしていない装置と接続する場合、本装置の LACP システム優先度を高くしてください。LACP システム優先度は値が小さいほど優先度が高くなります。

離脱ポート制限機能は、LACP リンクアグリゲーションだけで使用できます。

#### [ コマンドによる設定 ]

1. (config)# interface port-channel 10  
チャンネルグループ 10 のポートチャンネルインタフェースコンフィグレーションモードに移行します。
2. (config-if)# channel-group max-detach-port 0  
チャンネルグループ 10 に離脱ポート制限機能を設定します。離脱を許容する最大ポート数を 0 とし、障害などによって 1 ポートでも離脱した場合にチャンネルグループ全体を障害とみなします。
3. (config-if)# channel-group lacp system-priority 100  
チャンネルグループ 10 のシステム優先度を 100 に設定します。

### 16.4.4 異速度混在モードのコンフィグレーション

#### [ 設定のポイント ]

チャンネルグループに異速度混在モードを設定します。本機能を設定すると、ポートの速度は離脱条件ではなくなります。

#### [ コマンドによる設定 ]

1. (config)# interface port-channel 10  
チャンネルグループ 10 のポートチャンネルインタフェースコンフィグレーションモードに移行します。
2. (config-if)# channel-group multi-speed  
チャンネルグループ 10 に異速度混在モードを設定します。

## 16.5 リンクアグリゲーションのオペレーション

### 16.5.1 運用コマンド一覧

リンクアグリゲーションの運用コマンド一覧を次の表に示します。

表 16-10 運用コマンド一覧

| コマンド名                               | 説明                                              |
|-------------------------------------|-------------------------------------------------|
| show channel-group                  | リンクアグリゲーションの情報を表示します。                           |
| show channel-group statistics       | リンクアグリゲーションの統計情報を表示します。                         |
| clear channel-group statistics lacp | LACPDU の送受信統計情報をクリアします。                         |
| restart link-aggregation            | リンクアグリゲーションプログラムを再起動します。                        |
| dump protocols link-aggregation     | リンクアグリゲーションの詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。 |

### 16.5.2 リンクアグリゲーションの状態の確認

#### (1) リンクアグリゲーションの接続状態の確認

リンクアグリゲーションの情報を show channel-group コマンドで表示します。CH Status でチャンネルグループの接続状態を確認できます。また、設定が正しいことを各項目で確認してください。

show channel-group コマンドの実行結果を次の図に示します。

図 16-4 show channel-group コマンドの実行結果

```
> show channel-group 1
Date 2006/03/07 13:13:38 UTC
channel-group Counts:1
ChGr:1 Mode:LACP
CH Status :Up Elapsed Time:10:10:39
Multi Speed :Off Load Balance:MAC-IP-PORT
Max Active Port:16
Max Detach Port:15
MAC address: 0012.e2ac.8301 VLAN ID:10
Periodic Timer:Short
Actor information: System Priority:1 MAC: 0012.e212.ff02
KEY:1
Partner information: System Priority:10000 MAC: 0012.e2f0.69be
KEY:10
Port(4) :1/5-8
Up Port(2) :1/5-6
Down Port(2) :1/7-8
>
```

#### (2) 各ポートの運用状態の確認

show channel-group detail コマンドで各ポートの詳細な状態を表示します。ポートの通信状態を Status で確認してください。Status が Down 状態のときは Reason で理由を確認できます。

show channel-group detail コマンドの実行結果を次の図に示します。

図 16-5 show channel-group detail コマンドの実行結果

```

> show channel-group detail
Date 2006/03/07 13:13:38 UTC
channel-group Counts:1
ChGr:1 Mode:LACP
 CH Status :Up Elapsed Time:00:13:51
 Multi Speed :Off Load Balance:MAC-IP-PORT
 Max Active Port:16
 Max Detach Port:15
 MAC address: 0012.e205.0545 VLAN ID:10
 Periodic Timer:Long
 Actor information: System Priority:128 MAC: 0012.e205.0540
 KEY:1
 Partner information: System Priority:128 MAC: 0012.e2c4.2b5b
 KEY:1
 Port Counts:4 Up Port Counts:2
 Port:1/5 Status:Up Reason:-
 Speed :100M Duplex:Full LACP Activity:Active
 Actor Priority:128 Partner Priority:128
 Port:1/6 Status:Up Reason:-
 Speed :100M Duplex:Full LACP Activity:Active
 Actor Priority:128 Partner Priority:128
 Port:1/7 Status:Down Reason:Duplex Half
 Speed :100M Duplex:Half LACP Activity:Active
 Actor Priority:128 Partner Priority:0
 Port:1/8 Status:Down Reason:Port Down
 Speed :- Duplex:- LACP Activity:Active
 Actor Priority:128 Partner Priority:0
>

```

# 17 レイヤ2スイッチ概説

この章では、本装置の機能のうち、OSI階層モデルの第2レイヤでデータを中継するレイヤ2スイッチ機能の概要について説明します。

---

17.1 概要

---

17.2 サポート機能

---

17.3 レイヤ2スイッチ機能と他機能の共存について

---

## 17.1 概要

### 17.1.1 MAC アドレス学習

レイヤ2スイッチはフレームを受信すると送信元 MAC アドレスを MAC アドレステーブルに登録します。MAC アドレステーブルの各エントリには、MAC アドレスとフレームを受信したポートおよびエージングタイマを記録します。フレームを受信するごとに送信元 MAC アドレスに対応するエントリを更新します。

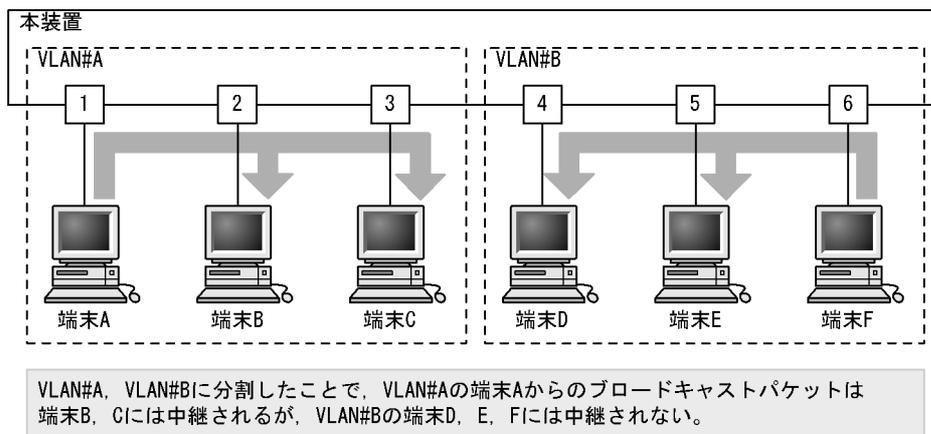
レイヤ2スイッチは、MAC アドレステーブルのエントリに従ってフレームを中継します。フレームの宛先 MAC アドレスに一致するエントリがあると、そのエントリのポートに中継します（エントリのポートが受信したポートである場合は中継しません）。一致するエントリがない場合、受信したポート以外のすべてのポートにフレームを中継します。この中継をフラディングと呼びます。

### 17.1.2 VLAN

VLAN は、スイッチ内を仮想的なグループに分ける機能のことです。スイッチ内を複数の VLAN にグループ分けすることによってブロードキャストドメインを分割します。これによって、ブロードキャストフレームの抑制や、セキュリティの強化を図ることができます。

VLAN の概要を次の図に示します。VLAN#A と VLAN#B の間ではブロードキャストドメインが分割されるため、フレームが届くことはありません。

図 17-1 VLAN の概要



## 17.2 サポート機能

レイヤ2スイッチ機能として、本装置がサポートする機能を次の表に示します。

これらの機能は、組み合わせて利用できる機能とできない機能があります。機能の組み合わせ制限については、次項で説明します。

表 17-1 レイヤ2スイッチサポート機能

| サポート機能                     |                  | 機能概要                                                               |
|----------------------------|------------------|--------------------------------------------------------------------|
| MAC アドレス学習                 |                  | MAC アドレステーブルに登録する MAC アドレスの学習機能                                    |
| VLAN                       | ポート VLAN         | ポート単位にスイッチ内を仮想的なグループに分ける機能                                         |
|                            | プロトコル VLAN       | プロトコル単位にスイッチ内を仮想的なグループに分ける機能                                       |
|                            | MAC VLAN         | 送信元の MAC アドレス単位にスイッチ内を仮想的なグループに分ける機能                               |
|                            | デフォルト VLAN       | コンフィギュレーションが未設定のときにデフォルトで所属する VLAN                                 |
|                            | ネイティブ VLAN       | トランクポート、プロトコルポート、MAC ポートでの Untagged フレームを扱うポート VLAN の呼称            |
|                            | トンネリング           | 複数ユーザの VLAN をほかの VLAN に集約して「トンネル」する機能                              |
|                            | Tag 変換           | VLAN Tag を変換して別の VLAN に中継する機能                                      |
|                            | L2 プロトコルフレーム透過機能 | レイヤ2のプロトコルのフレームを中継する機能<br>スパンニングツリー (BPDU)、IEEE802.1X(EAP) を透過します。 |
|                            | VLAN ごと MAC アドレス | レイヤ3 インタフェースの MAC アドレスを VLAN ごとに異なるアドレスにする機能                       |
| スパンニングツリー                  | PVST+            | VLAN 単位のスイッチ間のループ防止機能                                              |
|                            | シングルスパンニングツリー    | 装置単位のスイッチ間のループ防止機能                                                 |
|                            | マルチプルスパンニングツリー   | MST インスタンス単位のスイッチ間のループ防止機能                                         |
| Ring Protocol              |                  | リングトポロジーでのレイヤ2 ネットワークの冗長化機能                                        |
| IGMP snooping/MLD snooping |                  | レイヤ2 スイッチで VLAN 内のマルチキャストトラフィック制御機能                                |

## 17.3 レイヤ2スイッチ機能と他機能の共存について

レイヤ2スイッチ機能と併用する際、共存不可または制限事項がある機能があります。機能間の共存についての制限事項を次の表に示します。

なお、これらの表では各機能間の共存関係で、制限のある項目だけを示しています。

表 17-2 VLAN での制限事項

| 使用したい機能            |                         | 制限のある機能             | 制限の内容               |
|--------------------|-------------------------|---------------------|---------------------|
| VLAN 種別            | ポート VLAN                | VLAN トンネリング         | 一部制限あり <sup>1</sup> |
|                    |                         | レイヤ2 認証             | 一部制限あり <sup>2</sup> |
|                    |                         | ポートミラーリング (ミラーポート)  | 共存不可                |
|                    | プロトコル VLAN              | デフォルト VLAN          | 共存不可                |
|                    |                         | VLAN トンネリング         |                     |
|                    |                         | PVST+               |                     |
|                    |                         | レイヤ2 認証             | 一部制限あり <sup>2</sup> |
|                    |                         | ポートミラーリング (ミラーポート)  | 共存不可                |
|                    | MAC VLAN                | デフォルト VLAN          | 共存不可                |
|                    |                         | VLAN トンネリング         |                     |
|                    |                         | PVST+               |                     |
|                    |                         | レイヤ2 認証             | 一部制限あり <sup>2</sup> |
|                    |                         | ポートミラーリング (ミラーポート)  | 共存不可                |
|                    | デフォルト VLAN              | プロトコル VLAN          | 共存不可                |
| MAC VLAN           |                         |                     |                     |
| IGMP snooping      |                         |                     |                     |
| MLD snooping       |                         |                     |                     |
| レイヤ2 認証            |                         | 一部制限あり <sup>2</sup> |                     |
| ポートミラーリング (ミラーポート) |                         | 共存不可                |                     |
| VLAN 拡張機能          | Tag 変換                  | PVST+               | 共存不可                |
|                    |                         | IGMP snooping       |                     |
|                    |                         | MLD snooping        |                     |
|                    | VLAN トンネリング             | ポート VLAN            | 一部制限あり <sup>1</sup> |
|                    |                         | プロトコル VLAN          | 共存不可                |
|                    |                         | MAC VLAN            |                     |
|                    |                         | IGMP snooping       |                     |
|                    |                         | MLD snooping        |                     |
|                    |                         | レイヤ2 認証             | 一部制限あり <sup>2</sup> |
|                    |                         | DHCP snooping       | 共存不可                |
|                    | L2 プロトコルフレーム透過機能 (BPDU) | PVST+               | 共存不可                |
|                    |                         | ポリシーベーススイッチング       | 一部制限あり <sup>3</sup> |

| 使用したい機能                | 制限のある機能       | 制限の内容               |
|------------------------|---------------|---------------------|
| L2 プロトコルフレーム透過機能 (EAP) | レイヤ 2 認証      | 一部制限あり <sup>2</sup> |
|                        | ポリシーベーススイッチング | 一部制限あり <sup>3</sup> |

注 1

VLAN トンネリング機能を使用する場合は、トランクポートでネイティブ VLAN を使用しないでください。

注 2

「コンフィグレーションガイド Vol.2 7.2.1 レイヤ 2 認証と他機能との共存」を参照してください。

注 3

「25.1.4 ポリシーベーススイッチングと他機能との共存」を参照してください。

表 17-3 スパニングツリーでの制限事項

| 使用したい機能       | 制限のある機能                 | 制限の内容  |
|---------------|-------------------------|--------|
| PVST+         | プロトコル VLAN              | 共存不可   |
|               | MAC VLAN                |        |
|               | Tag 変換                  |        |
|               | L2 プロトコルフレーム透過機能 (BPDU) |        |
|               | マルチプルスパニングツリー           |        |
|               | GSRP                    |        |
|               | レイヤ 2 認証                | 一部制限あり |
| シングルスパニングツリー  | マルチプルスパニングツリー           | 共存不可   |
|               | GSRP                    |        |
|               | レイヤ 2 認証                | 一部制限あり |
| マルチプルスパニングツリー | シングルスパニングツリー            | 共存不可   |
|               | PVST+                   |        |
|               | ループガード                  |        |
|               | GSRP                    |        |
|               | レイヤ 2 認証                | 一部制限あり |

注

「コンフィグレーションガイド Vol.2 7.2.1 レイヤ 2 認証と他機能との共存」を参照してください。

表 17-4 Ring Protocol での制限事項

| 使用したい機能       | 制限のある機能       | 制限の内容               |
|---------------|---------------|---------------------|
| Ring Protocol | レイヤ 2 認証      | 一部制限あり <sup>1</sup> |
|               | ポリシーベーススイッチング | 一部制限あり <sup>2</sup> |

注 1

「コンフィグレーションガイド Vol.2 7.2.1 レイヤ 2 認証と他機能との共存」を参照してください。

注 2

「25.1.4 ポリシーベーススイッチングと他機能との共存」を参照してください。

表 17-5 IGMP snooping/MLD snooping での制限事項

| 使用したい機能       | 制限のある機能     | 制限の内容 |
|---------------|-------------|-------|
| IGMP snooping | デフォルト VLAN  | 共存不可  |
|               | Tag 変換      |       |
|               | VLAN トンネリング |       |
| MLD snooping  | デフォルト VLAN  | 共存不可  |
|               | Tag 変換      |       |
|               | VLAN トンネリング |       |

# 18 MAC アドレス学習

この章では、MAC アドレス学習機能の解説と操作方法について説明します。

---

18.1 MAC アドレス学習の解説

---

18.2 MAC アドレス学習のコンフィグレーション

---

18.3 MAC アドレス学習のオペレーション

---

## 18.1 MAC アドレス学習の解説

本装置は、フレームを宛先 MAC アドレスによって目的のポートへ中継するレイヤ 2 スイッチングを行います。宛先 MAC アドレスによって特定のポートだけに中継することで、ユニキャストフレームのフラグディングによるむだなトラフィックを抑止します。

MAC アドレス学習では、チャンネルグループを一つのポートとして扱います。

### 18.1.1 送信元 MAC アドレス学習

すべての受信フレームを MAC アドレス学習の対象とし、送信元 MAC アドレスを学習して MAC アドレステーブルに登録します。登録した MAC アドレスはエージングタイムアウトまで保持します。学習は VLAN 単位に行い、MAC アドレステーブルは MAC アドレスと VLAN のペアによって管理します。異なる VLAN であれば同一の MAC アドレスを学習することもできます。

### 18.1.2 MAC アドレス学習の移動検出

学習済みの送信元 MAC アドレスを持つフレームを学習時と異なるポートから受信した場合、その MAC アドレスが移動したものとみなして MAC アドレステーブルのエントリを再登録（移動先ポートに関する上書き）します。

チャンネルグループで学習した MAC アドレスについては、そのチャンネルグループに含まれないポートからフレームを受信した場合に MAC アドレスが移動したものとみなします。

### 18.1.3 学習 MAC アドレスのエージング

学習したエントリは、エージングタイム内に同じ送信元 MAC アドレスからフレームを受信しなかった場合はエントリを削除します。これによって、不要なエントリの蓄積を防止します。エージングタイム内にフレームを受信した場合は、エージングタイムを更新しエントリを保持します。エージングタイムを設定できる範囲を次に示します。

- エージングタイムの範囲：0, 10 ~ 1000000 (秒)  
0 は無限を意味し、エージングしません。
- デフォルト値：300 (秒)

ポートがダウンした場合は該当ポートから学習したエントリをすべて削除します。チャンネルグループで学習したエントリは、そのチャンネルグループがダウンした場合に削除します。

### 18.1.4 MAC アドレスによるレイヤ 2 スイッチング

MAC アドレス学習の結果に基づいてレイヤ 2 スイッチングを行います。宛先 MAC アドレスに対応するエントリを保持している場合、学習したポートだけに中継します。

レイヤ 2 スイッチングの動作仕様を次の表に示します。

表 18-1 レイヤ 2 スイッチングの動作仕様

| 宛先 MAC アドレスの種類 | 動作概要           |
|----------------|----------------|
| 学習済みのユニキャスト    | 学習したポートへ中継します。 |

| 宛先 MAC アドレスの種類 | 動作概要                       |
|----------------|----------------------------|
| 未学習のユニキャスト     | 受信した VLAN に所属する全ポートへ中継します。 |
| ブロードキャスト       | 受信した VLAN に所属する全ポートへ中継します。 |
| マルチキャスト        | 受信した VLAN に所属する全ポートへ中継します。 |

### 18.1.5 スタティックエントリの登録

受信フレームによるダイナミックな学習のほかに、ユーザ指定によってスタティックに MAC アドレスを登録できます。ユニキャスト MAC アドレスに対して一つのポートまたはチャンネルグループを指定できます。

ユニキャスト MAC アドレスに対してスタティックに登録を行うと、そのアドレスについてダイナミックな学習は行いません。すでに学習済みのエントリは MAC アドレステーブルから削除してスタティックエントリを登録します。スタティックエントリの指定パラメータを次の表に示します。

表 18-2 スタティックエントリの指定パラメータ

| 項番 | 指定パラメータ  | 説明                         |
|----|----------|----------------------------|
| 1  | MAC アドレス | ユニキャスト MAC アドレスが指定できます。    |
| 2  | VLAN     | このエントリを登録する VLAN を指定します。   |
| 3  | 送信先ポート   | 一つのポートまたはチャンネルグループを指定できます。 |

### 18.1.6 MAC アドレス学習の制限

受信フレームによるダイナミックな学習に制限を設け、使用する MAC アドレステーブルのエントリ数を管理できます。MAC アドレス学習の制限には、次に説明する機能があります。

#### (1) MAC アドレス学習の抑止

VLAN ごとに、ダイナミックな MAC アドレス学習を抑止できます。ダイナミックな MAC アドレス学習を抑止すると、その VLAN のフレームはフラッドします。

すでに MAC アドレスを学習しているときに MAC アドレス学習抑止すると、学習していた MAC アドレステーブルのエントリは削除します。

#### (2) MAC アドレス学習数の制限

受信ポートまたは VLAN でダイナミックに学習する MAC アドレスの数を制限できます。MAC アドレス学習数が制限値に達すると、ログメッセージを出力してダイナミックな MAC アドレス学習を停止します。MAC アドレス学習数の制限によって送信元 MAC アドレスを学習しなかった受信フレームは、中継しないで廃棄します。

MAC アドレス学習数を制限することで、ポートまたは VLAN に接続する PC などの台数を制限することができます。

ポートでの MAC アドレス学習数制限と、VLAN の MAC アドレス学習数制限はそれぞれ独立して設定できます。フレームを受信したときに、どちらかの学習数が制限に達していた場合は、そのフレームの送信元 MAC アドレスを学習しないで、フレームを廃棄します。

MAC アドレス学習の抑止は、MAC アドレス学習数の制限より優先されます。あるポートで MAC アドレ

ス学習数を制限し、すでに学習数が制限値に達している場合でも、MAC アドレス学習を抑止している VLAN のフレームは廃棄せずにフラディングします。

MAC アドレス学習数が制限値に達して、学習を停止しても、すでに学習している MAC アドレステーブルのエントリは、エージングされるか、運用コマンドなどで削除されるまで有効です。

MAC アドレス学習数を制限する場合、制限を解除する閾値を、制限値とは別に設定できます。MAC アドレス学習の停止は、MAC アドレステーブルのエントリ数が解除の閾値より少なくなったときに解除されます。

### 18.1.7 MAC アドレステーブルのクリア

本装置は運用コマンドやプロトコルの動作などによって MAC アドレステーブルをクリアします。MAC アドレステーブルをクリアする契機を次の表に示します。

表 18-3 MAC アドレステーブルをクリアする契機

| 契機                                    | 説明                                                                                                                                               |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| ポートダウン <sup>1</sup>                   | 該当ポートから学習したエントリを削除します。                                                                                                                           |
| チャンネルグループダウン <sup>2</sup>             | 該当チャンネルグループから学習したエントリを削除します。                                                                                                                     |
| 運用コマンド clear mac-address-table の実行    | パラメータに従って MAC アドレステーブルをクリアします。                                                                                                                   |
| MAC アドレステーブル Clear 用 MIB (プライベート MIB) | セット時に MAC アドレステーブルをクリアします。                                                                                                                       |
| スパンニングツリーのトポロジ変更                      | [ 本装置でスパンニングツリーを構成 ]<br>トポロジ変更を検出した時に MAC アドレステーブルをクリアします。                                                                                       |
|                                       | [ スパンニングツリーと Ring Protocol を併用しているネットワーク構成で本装置がリングノードとして動作 ]<br>Ring Protocol と併用している装置がトポロジ変更を検出した時に送信するフラッシュ制御フレームを受信した場合、MAC アドレステーブルをクリアします。 |
| GSRP のマスタ/バックアップ切り替え                  | [ 本装置が GSRP スイッチとして動作 ]<br>バックアップ状態になった時に MAC アドレステーブルをクリアします。                                                                                   |
|                                       | [ 本装置が GSRP aware として動作 ]<br>GSRP スイッチがマスタ状態になった時に送信される GSRP Flush request フレームを受信した場合、MAC アドレステーブルをクリアします。                                      |
|                                       | [ 本装置が GSRP と Ring Protocol を併用して動作 ]<br>マスタ状態になった時に MAC アドレステーブルをクリアします。                                                                        |
|                                       | [ GSRP と Ring Protocol を併用しているネットワーク構成で本装置がリングノードとして動作 ]<br>Ring Protocol と併用している装置がマスタ状態になった時に送信するフラッシュ制御フレームを受信した場合、MAC アドレステーブルをクリアします。       |
| Ring Protocol による経路の切り替え              | [ 本装置がマスタノードとして動作 ]<br>経路切り替え時に MAC アドレステーブルをクリアします。                                                                                             |
|                                       | [ 本装置がトランジットノードとして動作 ]<br>経路切り替え時にマスタノードから送信されるフラッシュ制御フレームを受信した場合、MAC アドレステーブルをクリアします。<br>フラッシュ制御フレーム受信待ち保護時間のタイムアウト時に MAC アドレステーブルをクリアします。      |
|                                       | 経路切り替え時にマスタノードから送信される隣接リング用フラッシュ制御フレームを受信した場合、MAC アドレステーブルをクリアします。                                                                               |

| 契機                                                     | 説明                                                                                                  |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| VRRP の仮想ルータのマスター / バックアップ切り替え                          | VRRP の仮想ルータがマスター状態になった時に送信される Flush Request フレームを受信した場合、MAC アドレステーブルをクリアします。                        |
| アップリンク・リダンダント機能 <sup>3</sup> によるプライマリポートとセカンダリポートの切り替え | プライマリポートからセカンダリポートへの切り替え時、およびセカンダリポートからプライマリポートへの切り戻し時に送信されるフラッシュ制御フレームを受信した場合、MAC アドレステーブルをクリアします。 |

## 注 1

回線障害、運用コマンド `inactivate` の実行、コンフィグレーションコマンド `shutdown` の設定などによるポートダウン。

## 注 2

LACP、回線障害、コンフィグレーションコマンド `shutdown` の設定などによるチャネルグループダウン。

## 注 3

本装置では、アップリンク・リダンダント機能のうち、フラッシュ制御フレーム受信機能だけをサポートしていません。

## 18.1.8 注意事項

### (1) MAC アドレス学習の抑止と学習数の制限について

MAC アドレス学習の抑止は、MAC アドレス学習数の制限より優先されます。あるポートで MAC アドレス学習数を制限し、すでに学習数が制限値に達している場合でも、MAC アドレス学習を抑止している VLAN のフレームは廃棄しないでフラッドリングします。

## 18.2 MAC アドレス学習のコンフィグレーション

### 18.2.1 コンフィグレーションコマンド一覧

MAC アドレス学習のコンフィグレーションコマンド一覧を次の表に示します。

表 18-4 コンフィグレーションコマンド一覧

| コマンド名                        | 説明                           |
|------------------------------|------------------------------|
| mac-address-table aging-time | MAC アドレス学習のエージングタイムを設定します。   |
| mac-address-table learning   | ダイナミックな MAC アドレス学習可否を設定します。  |
| mac-address-table limit      | ダイナミックな MAC アドレス学習の上限を設定します。 |
| mac-address-table static     | スタティックエントリを設定します。            |

### 18.2.2 エージングタイムの設定

[ 設定のポイント ]

MAC アドレス学習のエージングタイムを変更できます。設定は装置単位および VLAN 単位です。設定しない場合、エージングタイムは 300 秒で動作します。装置単位と VLAN 単位の設定では、VLAN 単位の設定が優先されます。

[ コマンドによる設定 ]

1. (config)# mac-address-table aging-time 100  
エージングタイムを 100 秒に設定します。
2. (config)# mac-address-table aging-time 600 vlan 200  
VLAN200 のエージングタイムを 600 秒に設定します。

### 18.2.3 スタティックエントリの設定

スタティックエントリを登録すると、指定した MAC アドレスについて MAC アドレス学習をしないで、常に登録したエントリに従ってフレームを中継するため、MAC アドレスのエージングによるフラッシュングを回避できます。本装置に直接接続したサーバなどのように、ポートの移動がなく、かつトラフィック量の多い端末などに有効な機能です。

スタティックエントリには、MAC アドレス、VLAN、および出力先を指定します。出力先はポート、チャネルグループのどれかを指定します。

#### (1) 出力先にポートを指定するスタティックエントリ

[ 設定のポイント ]

出力先にポートを指定した例を示します。

[ コマンドによる設定 ]

1. (config)# mac-address-table static 0012.e200.1122 vlan 10 interface gigabitethernet 1/1  
VLAN 10 で、宛先 MAC アドレス 0012.e200.1122 のフレームの出力先をポート 1/1 に設定します。

## (2) 出力先にリンクアグリゲーションを指定するスタティックエントリ

### [ 設定のポイント ]

出力先にリンクアグリゲーションを指定した例を示します。

### [ コマンドによる設定 ]

1. (config)# `mac-address-table static 0012.e200.1122 vlan 10 interface port-channel 5`  
VLAN 10 で、宛先 MAC アドレス 0012.e200.1122 のフレームの出力先をチャンネルグループ 5 に設定します。

## 18.2.4 MAC アドレス学習抑止の設定

### [ 設定のポイント ]

MAC アドレス学習を行う場合はコンフィギュレーションの設定は不要です。MAC アドレス学習をしない VLAN に対してだけ、学習抑止を設定します。

### [ コマンドによる設定 ]

1. (config)# `no mac-address-table learning vlan 100`  
VLAN100 では MAC アドレス学習を抑止します。

## 18.2.5 MAC アドレス学習数制限の設定

### [ 設定のポイント ]

MAC アドレス学習の停止と再開が短い間隔で発生する場合は、学習を再開するための閾値を設定することで、学習の停止と再開のばたつきを防止し、ログメッセージが多量に出力されることを防げます。

### [ コマンドによる設定 ]

1. (config)# `mac-address-table limit interface gigabitethernet 1/1 maximum 50 threshold 45`  
ポート 1/1 で学習する MAC アドレスの制限数を 50 にします。また、学習制限を解除するときの閾値を 45 にします。
2. (config)# `mac-address-table limit vlan 200 maximum 2500 threshold 2490`  
vlan200 で学習する MAC アドレスの制限数を 2500 にします。また、学習制限を解除するときの閾値を 2490 にします。

## 18.3 MAC アドレス学習のオペレーション

### 18.3.1 運用コマンド一覧

MAC アドレス学習の運用コマンド一覧を次の表に示します。

表 18-5 運用コマンド一覧

| コマンド名                   | 説明                                                                                                                                                                    |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show mac-address-table  | MAC アドレステーブルの情報を表示します。<br>learning-counter パラメータを指定すると、MAC アドレス学習の学習アドレス数をポート単位に表示します。<br>learning-counter パラメータと vlan パラメータを指定すると、MAC アドレス学習の学習アドレス数を VLAN 単位に表示します。 |
| clear mac-address-table | MAC アドレステーブルをクリアします。                                                                                                                                                  |

### 18.3.2 MAC アドレス学習の状態の確認

MAC アドレス学習の情報は show mac-address-table コマンドで表示します。MAC アドレステーブルに登録されている MAC アドレスとその MAC アドレスを宛先とするフレームの中継先を確認してください。このコマンドで表示されない MAC アドレスを宛先とするフレームは VLAN 全体にフラッディングされます。

show mac-address-table コマンドでは、MAC アドレス学習によって登録したエントリ、スタティックエントリ、および IEEE802.1X によって登録したエントリを表示します。

図 18-1 show mac-address-table コマンドの実行結果

```
> show mac-address-table
Date 2006/03/11 11:16:46 UTC
MAC address VLAN Aging-Time Type Port-list
0012.e200.1111 100 - Static 1/10
0012.e211.2222 200 - Static 1/10
0012.e200.3333 1 100 Dynamic 1/5
0012.e244.f073 100 230 Dynamic 1/21-22
0012.e244.f072 100 10000 Dynamic 1/21-22
0012.e244.f070 100 10 Dynamic 1/24
```

### 18.3.3 MAC アドレス学習数の確認

show mac-address-table コマンド ( learning-counter パラメータ ) で MAC アドレス学習によって登録したダイナミックエントリの数をポート単位に表示できます。このコマンドで、ポートごとの接続端末数の状態を確認できます。

show mac-address-table コマンドで learning-counter および vlan パラメータを指定すると、ダイナミックエントリの数を VLAN 単位に表示できます。

リンクアグリゲーションを使用している場合、同じチャンネルグループのポートはすべて同じ値を表示します。表示する値はチャンネルグループ上で学習したアドレス数です。

図 18-2 show mac-address-table learning-counter port ( learning-counter パラメータ指定 ) の実行結果

```

> show mac-address-table learning-counter port 1/1-10
Date 2006/03/21 20:00:57 UTC
Port counts:10
Port Count Maximum Threshold Status
1/1 3 - - -
1/2 1000 1000 800 Learning
1/3 0 - - -
1/4 50 60 40 Stop learning
1/5 45 60 40 Learning
1/6 0 60 40 Learning
1/7 22 1000 1000 Learning
1/8 0 - - -
1/9 0 - - -
1/10 0 - - -

```

図 18-3 show mac-address-table learning-counter および vlan パラメータ指定 ) の実行結果

```

> show mac-address-table learning-counter vlan
Date 2006/03/21 20:00:57 UTC
VLAN counts:4
ID Count Maximum Threshold Status
1 3 - - -
100 1000 1000 800 Stop learning
200 0 - - No learning
4095 90 100 100 Learning

```



# 19 VLAN

VLAN はスイッチ内を仮想的なグループに分ける機能です。この章では、VLAN の解説と操作方法について説明します。

- 
- 19.1 VLAN 基本機能の解説
  - 19.2 VLAN 基本機能のコンフィグレーション
  - 19.3 ポート VLAN の解説
  - 19.4 ポート VLAN のコンフィグレーション
  - 19.5 プロトコル VLAN の解説
  - 19.6 プロトコル VLAN のコンフィグレーション
  - 19.7 MAC VLAN の解説
  - 19.8 MAC VLAN のコンフィグレーション
  - 19.9 VLAN インタフェース
  - 19.10 VLAN インタフェースのコンフィグレーション
  - 19.11 VLAN のオペレーション
-

## 19.1 VLAN 基本機能の解説

この節では、VLAN の概要を説明します。

### 19.1.1 VLAN の種類

本装置がサポートする VLAN の種類を次の表に示します。

表 19-1 サポートする VLAN の種類

| 項目         | 概要                                |
|------------|-----------------------------------|
| ポート VLAN   | ポート単位に VLAN のグループを分けます。           |
| プロトコル VLAN | プロトコル単位に VLAN のグループを分けます。         |
| MAC VLAN   | 送信元の MAC アドレス単位に VLAN のグループを分けます。 |

### 19.1.2 ポートの種類

#### (1) 解説

本装置は、ポートの設定によって使用できる VLAN が異なります。使用したい VLAN の種類に応じて各ポートの種類を設定する必要があります。ポートの種類を次の表に示します。

表 19-2 ポートの種類

| ポートの種類    | 概要                                                                                               | 使用する VLAN              |
|-----------|--------------------------------------------------------------------------------------------------|------------------------|
| アクセスポート   | ポート VLAN として Untagged フレームを扱います。このポートでは、すべての Untagged フレームを一つのポート VLAN で扱います。                    | ポート VLAN<br>MAC VLAN   |
| プロトコルポート  | プロトコル VLAN として Untagged フレームを扱います。このポートでは、フレームのプロトコルによって VLAN を決定します。                            | プロトコル VLAN<br>ポート VLAN |
| MAC ポート   | MAC VLAN として Untagged フレームを扱います。このポートでは、フレームの送信元 MAC アドレスによって VLAN を決定します。                       | MAC VLAN<br>ポート VLAN   |
| トランクポート   | すべての種類の VLAN で Tagged フレームを扱います。このポートでは、VLAN Tag によって VLAN を決定します。                               | すべての種類の VLAN           |
| トンネリングポート | VLAN トンネリングのポート VLAN として、フレームの Untagged と Tagged を区別しないで扱います。このポートでは、すべてのフレームを一つのポート VLAN で扱います。 | ポート VLAN               |

アクセスポート、プロトコルポート、MAC ポートは Untagged フレームを扱うポートです。これらのポートで Tagged フレームを扱うことはできません。Tagged フレームを受信したときは廃棄し、また送信することはありません。

Tagged フレームはトランクポートでだけ扱うことができます。トランクポートの Untagged フレームはネイティブ VLAN が扱います。

トンネリングポートは、VLAN トンネリングをするポートで、フレームが Untagged か、Tagged かを区別しないで扱います。

ポートの種類ごとの、使用できる VLAN の種類を次の表に示します。プロトコル VLAN と MAC VLAN は同じポートで使用できません。VLAN Tag を扱うトランクポートはすべての VLAN で同じポートを使用できます。

表 19-3 ポート上で使用できる VLAN

| ポートの種類    | VLAN の種類 |            |          |
|-----------|----------|------------|----------|
|           | ポート VLAN | プロトコル VLAN | MAC VLAN |
| アクセスポート   |          | ×          |          |
| プロトコルポート  |          |            | ×        |
| MAC ポート   |          | ×          |          |
| トランクポート   |          |            |          |
| トンネリングポート |          | ×          | ×        |

(凡例) : 使用できる × : 使用できない

## (2) ポートのネイティブ VLAN

アクセスポート、トンネリングポート以外のポート（プロトコルポート、MAC ポート、トランクポート）では、それぞれの設定と一致しないフレームを受信する場合があります。例えば、プロトコルポートで IPv4 プロトコルだけ設定していたときに IPv6 のフレームを受信した場合です。アクセスポート、トンネリングポート以外ではこのようなフレームを扱うためにポート VLAN を一つ設定することができます。この VLAN のことを、各ポートにおけるネイティブ VLAN と呼びます。

アクセスポート、トンネリングポート以外の各ポートでは、ポートごとに作成済みのポート VLAN をネイティブ VLAN に設定できます。コンフィグレーションで指定がないポートは、VLAN 1（デフォルト VLAN）がネイティブ VLAN になります。

### 19.1.3 デフォルト VLAN

#### (1) 概要

本装置では、コンフィグレーションが未設定の状態であっても、装置の起動後すぐにレイヤ 2 中継ができます。このとき、すべてのポートはアクセスポートとなり、デフォルト VLAN と呼ぶ VLAN ID 1 の VLAN に属します。デフォルト VLAN は常に存在し、VLAN ID 「1」は変更できません。

#### (2) デフォルト VLAN から除外するポート

アクセスポートは、コンフィグレーションが未設定の場合は VLAN 1（デフォルト VLAN）に属します。しかし、コンフィグレーションによってデフォルト VLAN の自動的な所属から除外する場合があります。次に示すポートはデフォルト VLAN に自動的に所属しなくなります。

- アクセスポートで VLAN 1 以外を指定したポート
- VLAN トンネリング機能を設定した場合の全ポート
- ミラーポート

アクセスポート以外のポート（プロトコルポート、MAC ポート、トランクポート、トンネリングポート）は自動的に VLAN に所属することはありません。

## 19.1.4 VLAN の優先順位

### (1) フレーム受信時の VLAN 判定の優先順位

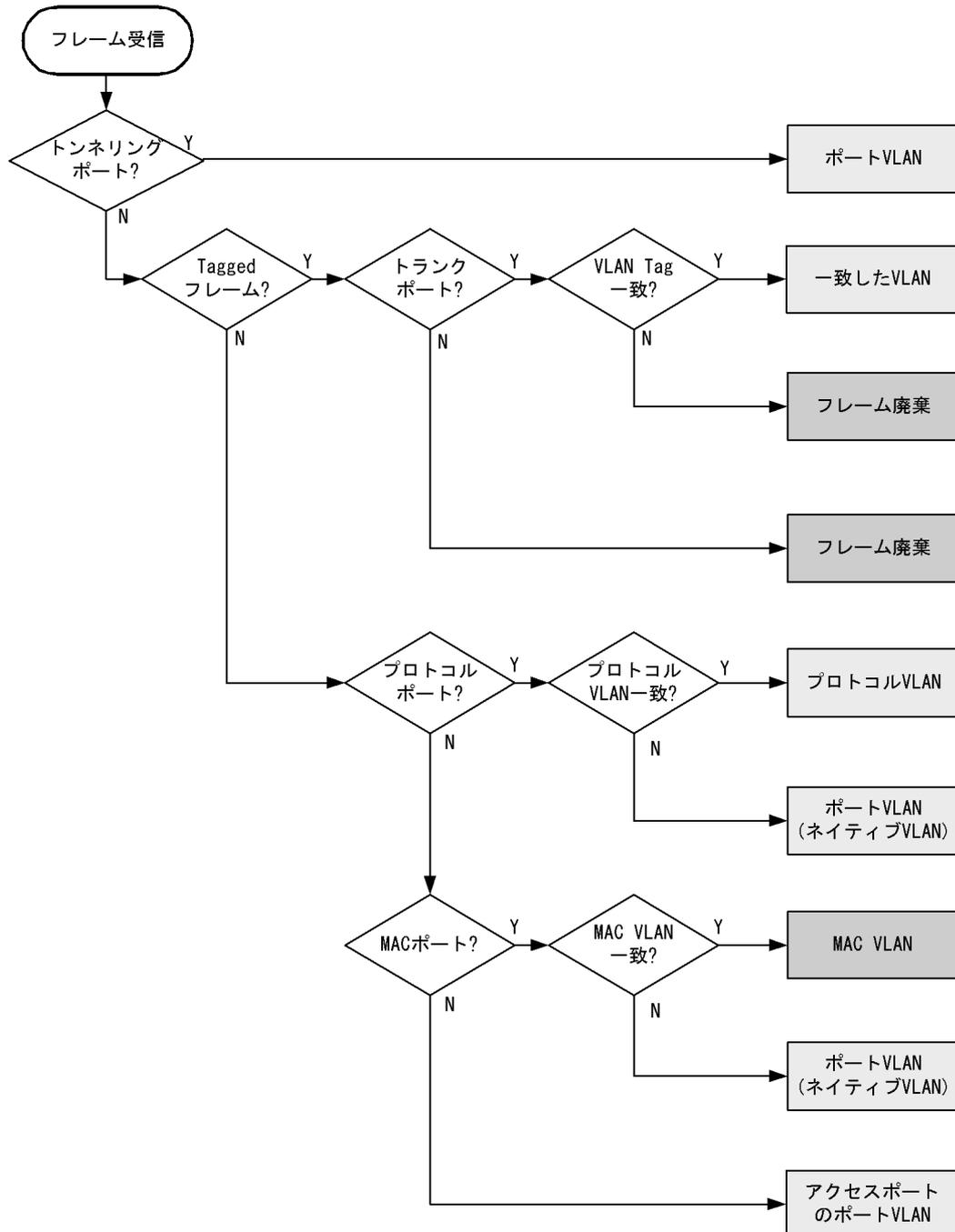
フレームを受信したとき、受信したフレームの VLAN を判定します。VLAN 判定の優先順位を次の表に示します。

表 19-4 VLAN 判定の優先順位

| ポートの種類    | VLAN 判定の優先順位                       |
|-----------|------------------------------------|
| アクセスポート   | ポート VLAN                           |
| プロトコルポート  | プロトコル VLAN > ポート VLAN (ネイティブ VLAN) |
| MAC ポート   | MAC VLAN > ポート VLAN (ネイティブ VLAN)   |
| トランクポート   | VLAN Tag > ポート VLAN (ネイティブ VLAN)   |
| トンネリングポート | ポート VLAN                           |

VLAN 判定のアルゴリズムを次の図に示します。

図 19-1 VLAN 判定のアルゴリズム



### 19.1.5 VLAN Tag

#### (1) 概要

IEEE 802.1Q 規定による VLAN Tag (イーサネットフレーム中に Tag と呼ばれる識別子を挿入する方法) を使用して、一つのポートに複数の VLAN を構築できます。

VLAN Tag はトランクポートで使用します。トランクポートはその対向装置も VLAN Tag を認識できなければなりません。

## (2) プロトコル仕様

VLAN Tag はイーサネットフレームに Tag と呼ばれる識別子を埋め込むことで、VLAN 情報 (=VLAN ID) を離れたセグメントへと伝えることができます。

Tagged フレームのフォーマットを次の図に示します。VLAN Tag を挿入するイーサネットフレームのフォーマットは、Ethernet V2 フォーマットと 802.3 フォーマットの 2 種類があります。

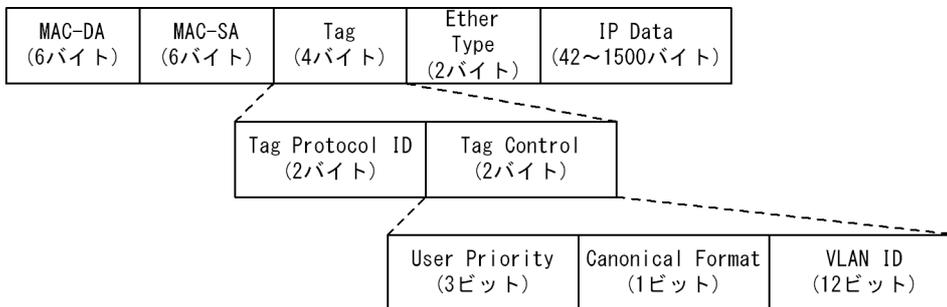
図 19-2 Tagged フレームのフォーマット

### ●Ethernet IIフレーム

通常のフレーム

|                  |                  |                         |                         |
|------------------|------------------|-------------------------|-------------------------|
| MAC-DA<br>(6バイト) | MAC-SA<br>(6バイト) | Ether<br>Type<br>(2バイト) | IP Data<br>(46~1500バイト) |
|------------------|------------------|-------------------------|-------------------------|

Taggedフレーム



### ●802.3LLC/SNAPフレーム

通常のフレーム

|                  |                  |                  |               |                |                         |
|------------------|------------------|------------------|---------------|----------------|-------------------------|
| MAC-DA<br>(6バイト) | MAC-SA<br>(6バイト) | Length<br>(2バイト) | LLC<br>(3バイト) | SNAP<br>(5バイト) | IP Data<br>(38~1492バイト) |
|------------------|------------------|------------------|---------------|----------------|-------------------------|

Taggedフレーム

|                  |                  |               |                  |               |                |                         |
|------------------|------------------|---------------|------------------|---------------|----------------|-------------------------|
| MAC-DA<br>(6バイト) | MAC-SA<br>(6バイト) | Tag<br>(4バイト) | Length<br>(2バイト) | LLC<br>(3バイト) | SNAP<br>(5バイト) | IP Data<br>(34~1492バイト) |
|------------------|------------------|---------------|------------------|---------------|----------------|-------------------------|

VLAN Tag のフィールドの説明を次の表に示します。

表 19-5 VLAN Tag のフィールド

| フィールド                     | 説明                                              | 本装置の条件                                           |
|---------------------------|-------------------------------------------------|--------------------------------------------------|
| TPID<br>(Tag Protocol ID) | IEEE802.1Q VLAN Tag が続くことを示す Ether Type 値を示します。 | ポートごとに任意の値を設定できます。                               |
| User Priority             | IEEE802.1D のプライオリティを示します。                       | コンフィグレーションで 8 段階のプライオリティレベルを選択できます。 <sup>1</sup> |
| CF<br>(Canonical Format)  | MAC ヘッダ内の MAC アドレスが標準フォーマットに従っているかどうかを示します。     | 本装置では標準 (0) だけをサポートします。                          |
| VLAN ID                   | VLAN ID を示します。 <sup>2</sup>                     | ユーザが使用できる VLAN ID は 1 ~ 4095 です。                 |

注 1 コンフィグレーションでプライオリティを指定しない場合、レイヤ 2 中継で Tagged フレームを受信したときは、受信した User Priority を引き継ぎます。レイヤ 2 中継で Untagged フレームを受信したとき、およびレイヤ 3 中継のときは、送信側の User Priority は 0 になります。

注 2 Tag 変換を使用している場合、Tag 変換で設定した VLAN ID を使用します。詳細は、「20.3 Tag 変換の解説」を参照してください。VLAN ID=0 を受信した場合は、Untagged フレームと同様の扱いになります。VLAN ID=0 を送信することはありません。

## 19.1.6 VLAN 使用時の注意事項

### (1) 他機能との共存

「17.3 レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

## 19.2 VLAN 基本機能のコンフィグレーション

### 19.2.1 コンフィグレーションコマンド一覧

VLAN 基本機能のコンフィグレーションコマンド一覧を次の表に示します。

表 19-6 コンフィグレーションコマンド一覧

| コマンド名                      | 説明                                                     |
|----------------------------|--------------------------------------------------------|
| name                       | VLAN の名称を設定します。                                        |
| state                      | VLAN の状態 (停止 / 開始) を設定します。                             |
| switchport access          | アクセスポートの VLAN を設定します。                                  |
| switchport dot1q ethertype | ポートごとに VLAN Tag の TPID を設定します。                         |
| switchport mode            | ポートの種類 (アクセス, プロトコル, MAC, トランク, トンネリング) を設定します。        |
| switchport trunk           | トランクポートの VLAN を設定します。                                  |
| vlan                       | VLAN を作成します。また, VLAN コンフィグレーションモードで VLAN に関する項目を設定します。 |
| vlan-dot1q-ethertype       | VLAN Tag の TPID のデフォルト値を設定します。                         |
| vlan dot1q tag native      | ネイティブ VLAN で Tagged フレームを扱います。                         |

### 19.2.2 VLAN の設定

#### [ 設定のポイント ]

VLAN を作成します。新規に VLAN を作成するためには, VLAN ID と VLAN の種類を指定します。VLAN の種類を省略した場合はポート VLAN を作成します。VLAN ID リストによって複数の VLAN を一括して設定することもできます。

vlan コマンドによって, VLAN コンフィグレーションモードに移行します。作成済みの VLAN を指定した場合は, モードの移行だけとなります。VLAN コンフィグレーションモードでは VLAN のパラメータを設定できます。

なお, ここでは VLAN の種類によらない共通した設定について説明します。ポート VLAN, プロトコル VLAN, MAC VLAN のそれぞれについては次節以降を参照してください。

#### [ コマンドによる設定 ]

##### 1. (config)# vlan 10

VLAN ID 10 のポート VLAN を作成し, VLAN 10 の VLAN コンフィグレーションモードに移行します。

##### 2. (config-vlan)# name "PORT BASED VLAN 10"

```
(config-vlan)# exit
```

作成したポート VLAN 10 の名称を " PORT BASED VLAN 10 " に設定します。

##### 3. (config)# vlan 100-200

VLAN ID 100 ~ 200 のポート VLAN を一括して作成します。また, VLAN 100 ~ 200 の VLAN コンフィグレーションモードに移行します。

4. `(config-vlan)# state suspend`

作成した VLAN ID 100 ~ 200 のポート VLAN を一括して停止状態にします。

## 19.2.3 ポートの設定

### [ 設定のポイント ]

イーサネットインタフェースコンフィグレーションモード，ポートチャンネルインタフェースコンフィグレーションモードでポートの種類を設定します。ポートの種類は使用したい VLAN の種類に合わせて設定します。

なお，ポート VLAN，プロトコル VLAN，MAC VLAN それぞれの詳細な設定方法については次節以降を参照してください。

### [ コマンドによる設定 ]

1. `(config)# interface gigabitethernet 1/1`

ポート 1/1 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. `(config-if)# switchport mode access`

`(config-if)# exit`

ポート 1/1 をアクセスポートに設定します。ポート 1/1 はポート VLAN で Untagged フレームを扱うポートになります。

3. `(config)# interface port-channel 10`

チャンネルグループ 10 のポートチャンネルインタフェースコンフィグレーションモードに移行します。

4. `(config-if)# switchport mode trunk`

チャンネルグループ 10 をトランクポートに設定します。ポートチャンネル 10 は Tagged フレームを扱うポートになります。

## 19.2.4 トランクポートの設定

### [ 設定のポイント ]

トランクポートは VLAN の種類に関係なく，すべての VLAN で使用でき，Tagged フレームを扱います。また，イーサネットインタフェースおよびポートチャンネルインタフェースで使用できます。

トランクポートは，`switchport mode` コマンドを設定しただけではどの VLAN にも所属していません。このポートで扱う VLAN は `switchport trunk allowed vlan` コマンドによって設定します。

VLAN の追加と削除は，`switchport trunk vlan add` コマンドおよび `switchport trunk vlan remove` コマンドによって行います。すでに `switchport trunk allowed vlan` コマンドを設定した状態でもう一度 `switchport trunk allowed vlan` コマンドを実行すると，指定した VLAN ID リストに置き換わります。

### [ コマンドによる設定 ]

1. `(config)# vlan 10-20,100,200-300`

`(config)# interface gigabitethernet 1/1`

`(config-if)# switchport mode trunk`

VLAN 10 ~ 20, 100, 200 ~ 300 を作成します。また，ポート 1/1 のイーサネットインタフェースコンフィグレーションモードに移行し，トランクポートに設定します。この状態では，ポート 1/1 はどの

VLAN にも所属していません。

2. `(config-if)# switchport trunk allowed vlan 10-20`  
ポート 1/1 に VLAN 10 ~ 20 を設定します。ポート 1/1 は VLAN 10 ~ 20 の Tagged フレームを扱います。
3. `(config-if)# switchport trunk allowed vlan add 100`  
ポート 1/1 で扱う VLAN に VLAN 100 を追加します。
4. `(config-if)# switchport trunk allowed vlan remove 15,16`  
ポート 1/1 で扱う VLAN から VLAN 15 および VLAN 16 を削除します。この状態で、ポート 1/1 は VLAN 10 ~ 14, 17 ~ 20, VLAN 100 の Tagged フレームを扱います。
5. `(config-if)# switchport trunk allowed vlan 200-300`  
ポート 1/1 で扱う VLAN を VLAN 200 ~ 300 に設定します。以前の設定はすべて上書きされ、VLAN 200 ~ 300 の Tagged フレームを扱います。

#### [ 注意事項 ]

トランクポートで Untagged フレームを扱うためには、ネイティブ VLAN を設定します。詳しくは、「19.4.3 トランクポートのネイティブ VLAN の設定」を参照してください。

`vlan dot1q tag native` コマンドで、ネイティブ VLAN でも Tagged フレームを扱う設定ができます。その場合は、Untagged フレームは扱わなくなります。

トランクポートで、一度に削除する VLAN 数が 30 以上の場合、および所属している VLAN 数が 30 以上のときにモードをトランクポート以外に変更する場合は、該当ポートの `mac-address-table`、ARP および NDP を削除します。そのため、L3 中継を行っている場合は、いったん ARP/NDP を再学習して通信が中断するので注意してください。

## 19.2.5 VLAN Tag の TPID の設定

#### [ 設定のポイント ]

本装置は、VLAN Tag の TPID を任意の値に設定することができます。`vlan-dot1q-ethertype` コマンドで装置のデフォルト値を、`switchport dot1q ethertype` コマンドでポートごとの値を設定します。

ポートごとの値を設定していないポートは装置のデフォルト値で動作します。

ポートごとの TPID の設定は、イーサネットインタフェースコンフィギュレーションモードで設定します。

装置のデフォルト値を 0x8100 以外に設定したときに、指定したポートの TPID を 0x8100 に戻すことができます。

#### [ コマンドによる設定 ]

1. `(config)# vlan-dot1q-ethertype 9100`  
装置のデフォルト値を 0x9100 に設定します。すべてのポートにおいて VLAN Tag を TPID 9100 として動作します。
2. `(config)# interface gigabitethernet 1/1`  
ポート 1/1 のイーサネットインタフェースコンフィギュレーションモードに移行します。
3. `(config-if)# switchport dot1q ethertype 8100`

ポート 1/1 の TPID を 0x8100 に設定します。ポート 1/1 は 0x8100 を VLAN Tag として認識します。そのほかのポートは装置のデフォルト値である 0x9100 で動作します。

[ 注意事項 ]

TPID は、フレーム上では Untagged フレームの EtherType と同じ位置を使用します。そのため、IPv4 の EtherType である 0x0800 など、EtherType として使用している値を設定するとネットワークが正しく構築できないおそれがあります。EtherType 値として未使用の値を設定してください。

## 19.3 ポート VLAN の解説

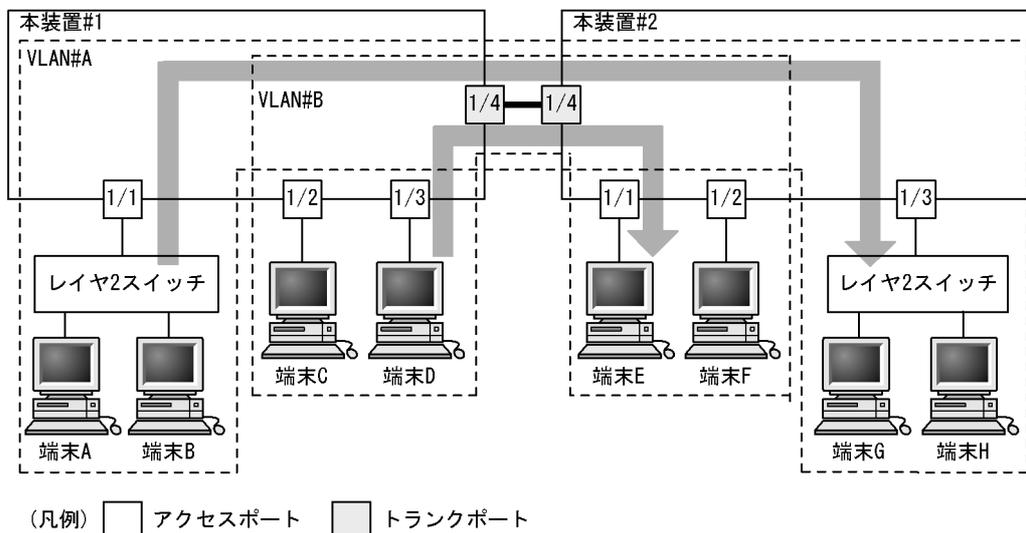
ポート単位に VLAN のグループ分けを行います。

### 19.3.1 アクセスポートとトランクポート

ポート VLAN は一つのポートに一つの VLAN を割り当てます。ポート VLAN として使用するポートはアクセスポートとして設定します。複数のポート VLAN をほかの LAN スイッチなどに接続するためにはトランクポートを使用します。トランクポートは VLAN Tag によって VLAN を識別するため、一つのポートに複数の VLAN を設定できます。

ポート VLAN の構成例を次の図に示します。ポート 1/1 ~ 1/3 はアクセスポートとしてポート VLAN を設定します。2 台の本装置の間はトランクポート（ポート 1/4）で接続します。そのとき、VLAN Tag を使います。

図 19-3 ポート VLAN の構成例



トランクポートは複数のVLANを設定することができます。  
トランクポートではVLAN Tagを付与して中継することでVLANを識別します。

### 19.3.2 ネイティブ VLAN

プロトコルポート、MAC ポート、トランクポートにはコンフィグレーションに一致しないフレームを扱うネイティブ VLAN があります。各ポートのネイティブ VLAN はコンフィグレーションで指定しない場合は VLAN 1 (デフォルト VLAN) です。また、ほかのポート VLAN にコンフィグレーションで変更することもできます。

例えば、「図 19-3 ポート VLAN の構成例」のトランクポートにおいて VLAN#B をネイティブ VLAN に設定すると、VLAN#B はトランクポートでも Untagged フレームで中継します。

### 19.3.3 ポート VLAN 使用時の注意事項

#### (1) アクセスポートでの Tagged フレームに関する注意事項

アクセスポートは Untagged フレームを扱うポートです。Tagged フレームを受信した場合は廃棄します。また、送信することもできません。なお、VLAN Tag 値が 0 の場合は、受信時に Untagged フレームと同じ扱いになります。これらのフレームを送信することはありません。

#### (2) MAC VLAN 混在時の注意事項

同一ポートにポート VLAN と MAC VLAN が混在する場合、マルチキャスト使用時の注意事項があります。詳細は、「19.7.4 VLAN 混在時のマルチキャストについて」を参照してください。

## 19.4 ポート VLAN のコンフィグレーション

### 19.4.1 コンフィグレーションコマンド一覧

ポート VLAN のコンフィグレーションコマンド一覧を次の表に示します。

表 19-7 コンフィグレーションコマンド一覧

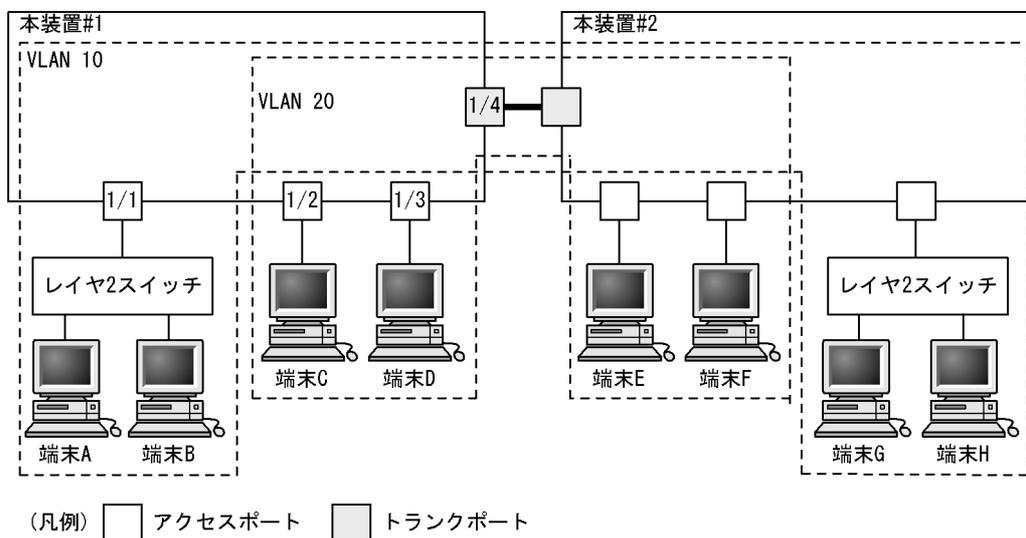
| コマンド名                 | 説明                                                         |
|-----------------------|------------------------------------------------------------|
| switchport access     | アクセスポートの VLAN を設定します。                                      |
| switchport mode       | ポートの種類 (アクセス, トランク) を設定します。                                |
| switchport trunk      | トランクポートの VLAN を設定します。                                      |
| vlan                  | ポート VLAN を作成します。また, VLAN コンフィグレーションモードで VLAN に関する項目を設定します。 |
| vlan dot1q tag native | ネイティブ VLAN でも Tagged フレームを扱います。                            |

### 19.4.2 ポート VLAN の設定

ポート VLAN を設定する手順を以下に示します。ここでは, 次の図に示す本装置 #1 の設定例を示します。

ポート 1/1 はポート VLAN 10 を設定します。ポート 1/2, 1/3 はポート VLAN 20 を設定します。ポート 1/4 はトランクポートでありすべての VLAN を設定します。

図 19-4 ポート VLAN の設定例



#### (1) ポート VLAN の作成

##### [ 設定のポイント ]

ポート VLAN を作成します。VLAN を作成する際に VLAN ID だけを指定して VLAN の種類を指定しないで作成するとポート VLAN となります。

##### [ コマンドによる設定 ]

1. (config)# vlan 10,20

VLAN ID 10, VLAN ID 20 をポート VLAN として作成します。本コマンドで VLAN コンフィグレーションモードに移行します。

## (2) アクセスポートの設定

一つのポートに一つの VLAN を設定して Untagged フレームを扱う場合、アクセスポートとして設定します。

[ 設定のポイント ]

ポートをアクセスポートに設定して、そのアクセスポートで扱う VLAN を設定します。

[ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/1  
ポート 1/1 のイーサネットインタフェースコンフィグレーションモードに移行します。
2. (config-if)# switchport mode access  
(config-if)# switchport access vlan 10  
(config-if)# exit  
ポート 1/1 をアクセスポートに設定します。また, VLAN 10 を設定します。
3. (config)# interface range gigabitethernet 1/2-3  
ポート 1/2, 1/3 のイーサネットインタフェースコンフィグレーションモードに移行します。ポート 1/2, 1/3 は同じコンフィグレーションとなるため, 一括して設定します。
4. (config-if-range)# switchport mode access  
(config-if-range)# switchport access vlan 20  
ポート 1/2, 1/3 をアクセスポートに設定します。また, VLAN 20 を設定します。

## (3) トランクポートの設定

[ 設定のポイント ]

Tagged フレームを扱うポートはトランクポートとして設定し、そのトランクポートに VLAN を設定します。

[ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/4  
ポート 1/4 のイーサネットインタフェースコンフィグレーションモードに移行します。
2. (config-if)# switchport mode trunk  
(config-if)# switchport trunk allowed vlan 10,20  
ポート 1/4 をトランクポートに設定します。また, VLAN 10, 20 を設定します。

### 19.4.3 トランクポートのネイティブ VLAN の設定

[ 設定のポイント ]

トランクポートで Untagged フレームを扱いたい場合、ネイティブ VLAN を設定します。ネイティブ

VLAN はポート VLAN だけを設定できます。

ネイティブ VLAN の VLAN ID を `switchport trunk allowed vlan` コマンドで指定すると、トランクポートで Untagged フレームを扱う VLAN となります。ネイティブ VLAN は、コンフィギュレーションで明示して指定しない場合は VLAN 1 (デフォルト VLAN) です。

トランクポート上で、デフォルト VLAN で Tagged フレーム (VLAN ID 1 の VLAN Tag) を扱いたい場合は、ネイティブ VLAN をほかの VLAN に変更してください。

`vlan dot1q tag native` コマンドで、ネイティブ VLAN でも Tagged フレームを扱う設定ができます。その場合は、Untagged フレームは扱わなくなります。

#### [ コマンドによる設定 ]

1. `(config)# vlan 10,20`

```
(config-vlan)# exit
```

VLAN ID 10, VLAN ID 20 をポート VLAN として作成します。

2. `(config)# interface gigabitethernet 1/1`

```
(config-if)# switchport mode trunk
```

ポート 1/1 のイーサネットインタフェースコンフィギュレーションモードに移行します。また、トランクポートとして設定します。この状態で、トランクポート 1/1 のネイティブ VLAN はデフォルト VLAN です。

3. `(config-if)# switchport trunk native vlan 10`

```
(config-if)# switchport trunk allowed vlan 1,10,20
```

トランクポート 1/1 のネイティブ VLAN を VLAN 10 に設定します。また、VLAN 1, 10, 20 を設定します。ネイティブ VLAN である VLAN 10 が Untagged フレームを扱い、VLAN 1 (デフォルト VLAN), VLAN 20 は Tagged フレームを扱います。

4. `(config)# vlan dot1q tag native`

ネイティブ VLAN でも Tagged フレームを扱うことを設定します。

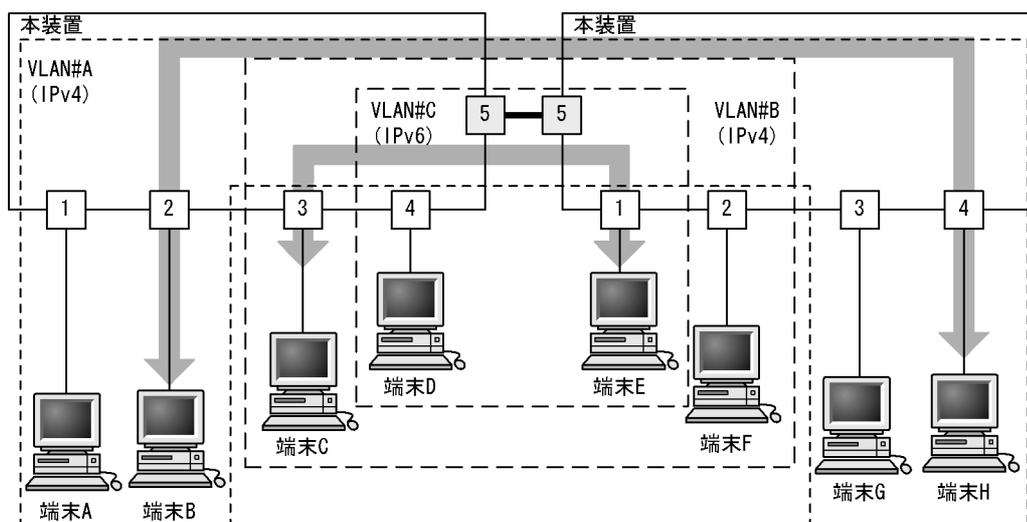
## 19.5 プロトコル VLAN の解説

### 19.5.1 概要

プロトコル単位で VLAN のグループ分けを行います。IPv4 や IPv6 といったプロトコルごとに異なる VLAN を構成できます。複数のプロトコルを同一のプロトコル VLAN に設定することもできます。

プロトコル VLAN の構成例を次の図に示します。VLAN#A, #B を IPv4 プロトコルで構成し, VLAN#C を IPv6 プロトコルで構成した例を示しています。

図 19-5 プロトコル VLAN の構成例



(凡例) □ : プロトコルポート □ : トランクポート

- ・ VLAN#A, #BはIPv4プロトコルのVLANです。
- ・ VLAN#CはIPv6プロトコルのVLANです。
- ・ 端末D, EはVLAN#B, #Cの両方に属しています。
- ・ 矢印は端末Bと端末H間, 端末Cと端末E間で同じVLANで通信している例です。

### 19.5.2 プロトコルの識別

プロトコルの識別には次の3種類の値を使用します。

表 19-8 プロトコルを識別する値

| 識別する値             | 概要                                                                                 |
|-------------------|------------------------------------------------------------------------------------|
| Ether-type 値      | EthernetV2 形式フレームの Ether-type 値によってプロトコルを識別します。                                    |
| LLC 値             | 802.3 形式フレームの LLC 値 (DSAP,SSAP) によってプロトコルを識別します。                                   |
| SNAP Ether-type 値 | 802.3 形式フレームの Ether-type 値によってプロトコルを識別します。フレームの LLC 値が AA AA 03 であるフレームだけが対象となります。 |

プロトコルは、コンフィグレーションによってプロトコルを作成し VLAN に対応付けます。一つのプロトコル VLAN に複数のプロトコルに対応付けることもできます。

### 19.5.3 プロトコルポートとトランクポート

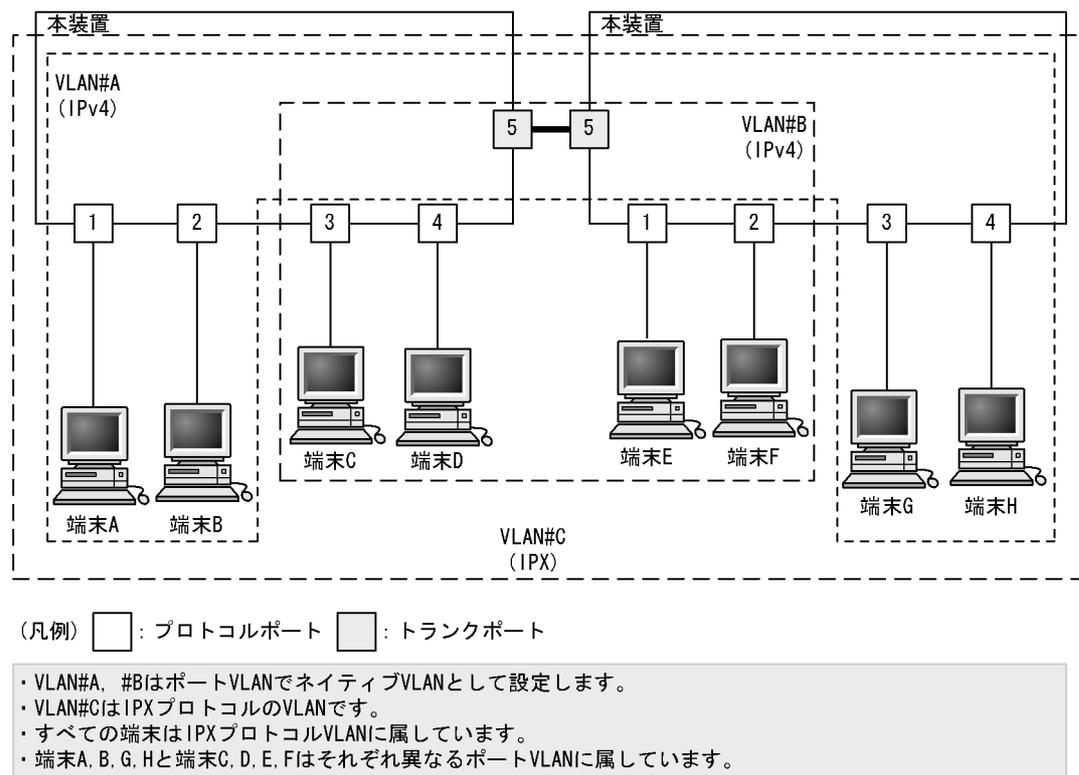
プロトコルポートは Untagged フレームのプロトコルを識別します。プロトコル VLAN として使用するポートはプロトコルポートを設定します。プロトコルポートには複数のプロトコルで異なる VLAN を割り当てることもできます。複数のプロトコル VLAN をほかの LAN スイッチなどに接続するためにはトランクポートを使用します。なお、トランクポートは VLAN Tag によって VLAN を識別するため、プロトコルによる識別は行いません。

### 19.5.4 プロトコルポートのネイティブ VLAN

プロトコルポートでコンフィグレーションに一致しないプロトコルのフレームを受信した場合はネイティブ VLAN で扱います。ネイティブ VLAN は、コンフィグレーションで指定しない場合は VLAN 1 (デフォルト VLAN) です。また、ほかのポート VLAN にコンフィグレーションで変更することもできます。

次の図に、プロトコルポートでネイティブ VLAN を使用する構成例を示します。図の構成は、IPX プロトコルをネットワーク全体で一つの VLAN とし、そのほか (IPv4 など) のプロトコルについてはポート VLAN で VLAN を分ける例です。VLAN#A, VLAN#B を各ポートのネイティブ VLAN として設定します。なお、この構成例では、VLAN#A, VLAN#B も IPv4 のプロトコル VLAN として設定することもできます。

図 19-6 プロトコルポートでネイティブ VLAN を使用する構成例



## 19.6 プロトコル VLAN のコンフィグレーション

### 19.6.1 コンフィグレーションコマンド一覧

プロトコル VLAN のコンフィグレーションコマンド一覧を次の表に示します。

表 19-9 コンフィグレーションコマンド一覧

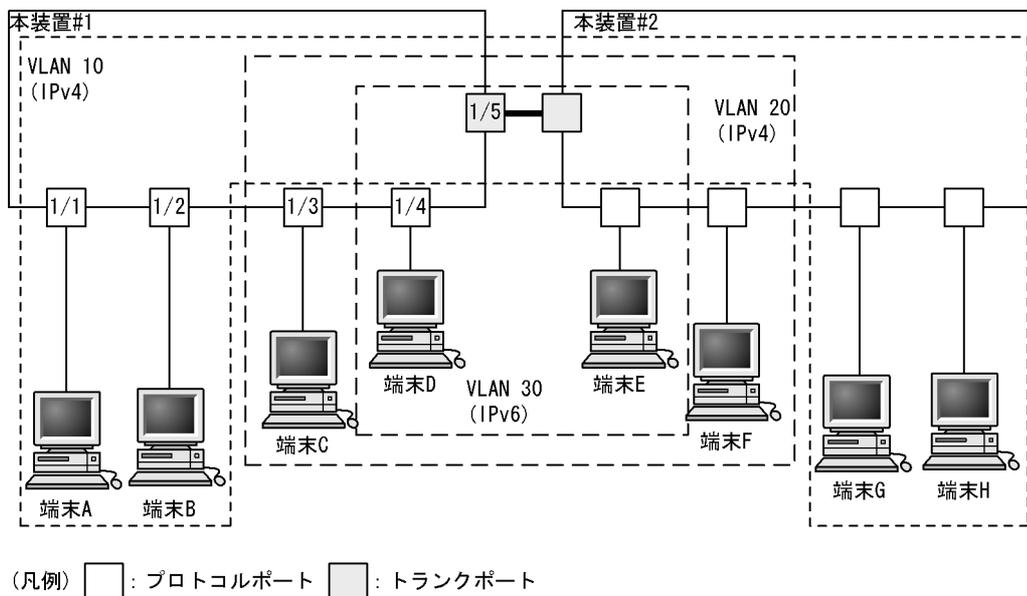
| コマンド名               | 説明                                          |
|---------------------|---------------------------------------------|
| protocol            | プロトコル VLAN で VLAN を識別するプロトコルを設定します。         |
| switchport mode     | ポートの種類（プロトコル、トランク）を設定します。                   |
| switchport protocol | プロトコルポートの VLAN を設定します。                      |
| switchport trunk    | トランクポートの VLAN を設定します。                       |
| vlan                | protocol-based パラメータを指定してプロトコル VLAN を作成します。 |
| vlan-protocol       | プロトコル VLAN 用のプロトコル名称とプロトコル値を設定します。          |

### 19.6.2 プロトコル VLAN の作成

プロトコル VLAN を設定する手順を以下に示します。ここでは、次の図に示す本装置 #1 の設定例を示します。

ポート 1/1, 1/2 は IPv4 プロトコル VLAN 10 を設定します。ポート 1/3, 1/4 は IPv4 プロトコル VLAN 20 を設定します。ポート 1/4 は VLAN 20 と同時に IPv6 プロトコル VLAN 30 にも所属します。ポート 1/5 はトランクポートであり、すべての VLAN を設定します。

図 19-7 プロトコル VLAN の設定例



#### (1) VLAN を識別するプロトコルの作成

[ 設定のポイント ]

プロトコル VLAN は、VLAN を作成する前に識別するプロトコルを `vlan-protocol` コマンドで設定し

ます。プロトコルは、プロトコル名称とプロトコル値を設定します。一つの名称に複数のプロトコル値を関連づけることもできます。

IPv4 プロトコルは、IPv4 の Ether-type と同時に ARP の Ether-type も指定する必要があるため、IPv4 には二つのプロトコル値を関連づけます。

#### [ コマンドによる設定 ]

1. `(config)# vlan-protocol IPV4 ether-type 0800 ether-type 0806`  
 名称 IPV4 のプロトコルを作成します。プロトコル値として、IPv4 の Ether-type 値 0800 と ARP の Ether-type 値 0806 を関連づけます。  
 なお、この設定でのプロトコル判定は EthernetV2 形式のフレームだけとなります。
2. `(config)# vlan-protocol IPV6 ether-type 86dd`  
 名称 IPV6 のプロトコルを作成します。プロトコル値として IPv6 の Ether-type 値 86DD を関連づけます。

## (2) プロトコル VLAN の作成

#### [ 設定のポイント ]

プロトコル VLAN を作成します。VLAN を作成する際に VLAN ID と protocol-based パラメータを指定します。また、VLAN を識別するプロトコルとして、作成したプロトコルを指定します。

#### [ コマンドによる設定 ]

1. `(config)# vlan 10,20 protocol-based`  
 VLAN 10, 20 をプロトコル VLAN として作成します。VLAN 10, 20 は同じ IPv4 プロトコル VLAN とするため一括して設定します。本コマンドで VLAN コンフィグレーションモードに移行します。
2. `(config-vlan)# protocol IPV4`  
`(config-vlan)# exit`  
 VLAN 10, 20 を識別するプロトコルとして、作成した IPv4 プロトコルを指定します。
3. `(config)# vlan 30 protocol-based`  
`(config-vlan)# protocol IPV6`  
 VLAN 30 をプロトコル VLAN として作成します。また、VLAN 30 を識別するプロトコルとして、作成した IPv6 プロトコルを指定します。

## (3) プロトコルポートの設定

#### [ 設定のポイント ]

プロトコル VLAN でプロトコルによって VLAN を識別するポートは、プロトコルポートを設定します。このポートでは Untagged フレームを扱います。

#### [ コマンドによる設定 ]

1. `(config)# interface range gigabitEthernet 1/1-2`  
 ポート 1/1, 1/2 のイーサネットインタフェースコンフィグレーションモードに移行します。ポート 1/1, 1/2 は同じコンフィグレーションとなるため一括して指定します。
2. `(config-if-range)# switchport mode protocol-vlan`

```
(config-if-range)# switchport protocol vlan 10
(config-if-range)# exit
```

ポート 1/1, 1/2 をプロトコルポートに設定します。また, VLAN 10 を設定します。

3. (config)# interface range gigabitethernet 1/3-4
 

```
(config-if-range)# switchport mode protocol-vlan
(config-if-range)# switchport protocol vlan 20
(config-if-range)# exit
```

ポート 1/3, 1/4 をプロトコルポートに設定します。また, VLAN 20 を設定します。

4. (config)# interface gigabitethernet 1/4
 

```
(config-if)# switchport protocol vlan add 30
```

ポート 1/4 に VLAN 30 を追加します。ポート 1/4 は IPv4, IPv6 の 2 種類のプロトコル VLAN を設定しています。

#### [注意事項]

switchport protocol vlan コマンドは, それ以前のコンフィグレーションに追加するコマンドではなく指定した <vlan id list> に設定を置き換えます。すでにプロトコル VLAN を運用中のポートで VLAN の追加や削除を行う場合は, switchport protocol vlan add コマンドおよび switchport protocol vlan remove コマンドを使用してください。

### (4) トランクポートの設定

#### [設定のポイント]

プロトコル VLAN においても, Tagged フレームを扱うポートはトランクポートとして設定し, そのトランクポートに VLAN を設定します。

#### [コマンドによる設定]

1. (config)# interface gigabitethernet 1/5
 

```
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 10,20,30
```

ポート 1/5 をトランクポートに設定します。また, VLAN 10, 20, 30 を設定します。

## 19.6.3 プロトコルポートのネイティブ VLAN の設定

#### [設定のポイント]

プロトコルポートで設定したプロトコルに一致しない Untagged フレームを扱いたい場合, そのフレームを扱う VLAN としてネイティブ VLAN を設定します。ネイティブ VLAN はポート VLAN だけを設定できます。

ネイティブ VLAN の VLAN ID を switchport protocol native vlan コマンドで指定すると, プロトコルポート上で設定したプロトコルに一致しない Untagged フレームを扱う VLAN となります。ネイティブ VLAN は, コンフィグレーションで明示して指定しない場合は VLAN 1 (デフォルト VLAN) です。

ネイティブ VLAN に status suspend が設定されている場合は, 設定したプロトコルと一致しないフ

フレームが中継されません。

[ コマンドによる設定 ]

1. (config)# vlan 10,20 protocol-based  
(config-vlan)# exit  
(config)# vlan 30  
(config-vlan)# exit

VLAN 10, 20 をプロトコル VLAN として作成します。また, VLAN 30 をポート VLAN として作成します。

2. (config)# interface gigabitethernet 1/1  
(config-if)# switchport mode protocol-vlan

ポート 1/1 のイーサネットインタフェースコンフィグレーションモードに移行します。また, プロトコルポートとして設定します。

3. (config-if)# switchport protocol native vlan 30  
(config-if)# switchport protocol vlan 10,20

プロトコルポート 1/1 のネイティブ VLAN をポート VLAN 30 に設定し, 設定したプロトコルに一致しない Untagged フレームを扱う VLAN とします。また, プロトコル VLAN 10, 20 を設定します。

## 19.7 MAC VLAN の解説

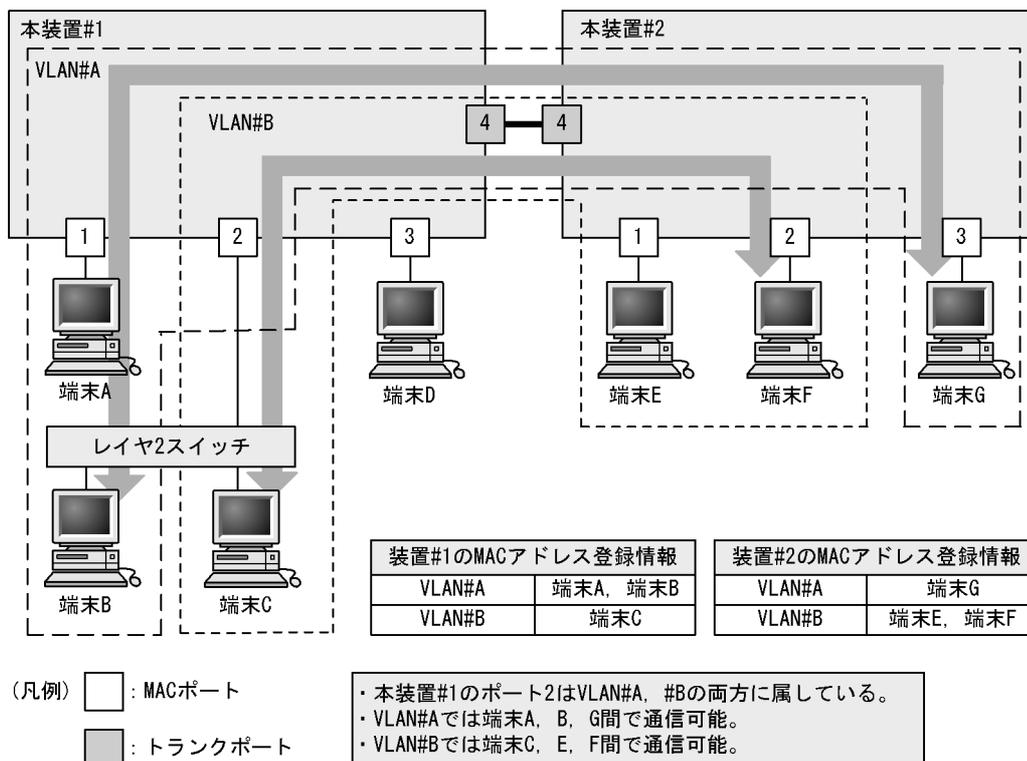
### 19.7.1 概要

送信元の MAC アドレス単位に VLAN のグループ分けを行います。VLAN への MAC アドレスの登録は、コンフィグレーションによる登録と、レイヤ 2 認証機能による動的な登録ができます。

MAC VLAN は、許可した端末の MAC アドレスをコンフィグレーションで登録するか、レイヤ 2 認証機能で認証された MAC アドレスを登録することによって、接続を許可された端末とだけ通信できるように設定できます。

MAC VLAN の構成例を次の図に示します。VLAN を構成する装置間にトランクポートを設定している場合は、送信元 MAC アドレスに関係なく VLAN Tag によって VLAN を決定します。そのため、すべての装置に同じ MAC アドレスの設定をする必要はありません。装置ごとに MAC ポートに接続した端末の MAC アドレスを設定します。

図 19-8 MAC VLAN の構成例



### 19.7.2 装置間の接続と MAC アドレス設定

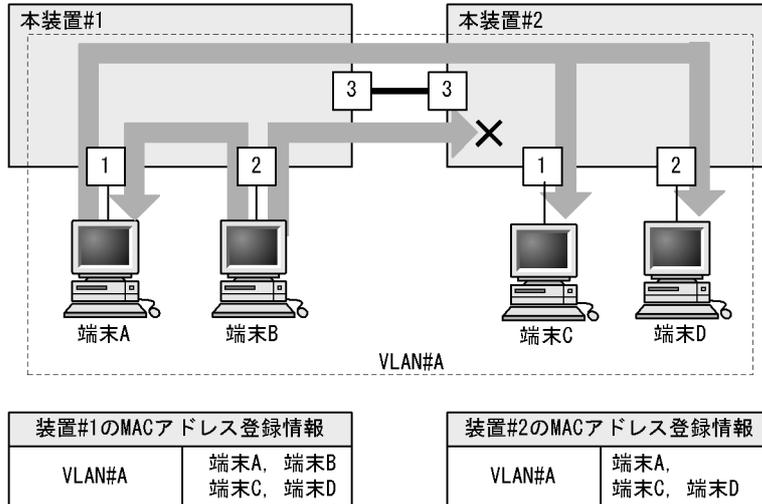
複数の装置で MAC VLAN を構成する場合、装置間の接続はトランクポートをお勧めします。トランクポートで受信したフレームの VLAN 判定は VLAN Tag で行います。そのため、送信元 MAC アドレスが VLAN に設定されていなくても、MAC VLAN で通信できます。トランクポートで装置間を接続した場合については、「図 19-8 MAC VLAN の構成例」を参照してください。

MAC ポートで装置間を接続する場合は、その VLAN に属するすべての MAC アドレスをすべての装置に設定する必要があります。ルータが存在する場合は、ルータの MAC アドレスも登録してください。また、

VRRP を使用している場合は、仮想ルータ MAC アドレスを登録してください。

MAC ポートで装置間を接続した場合の図を次に示します。

図 19-9 装置間を MAC ポートで接続した場合



(凡例) □ : MACポート

- 端末Aは、本装置#1、#2の両方に設定があるため、端末C、端末Dと通信可能。
- 端末Bは、本装置#2に設定がないため、端末C、端末Dと通信不可。  
端末Aとは通信可能。

### 19.7.3 レイヤ 2 認証機能との連携について

MAC VLAN は、レイヤ 2 認証機能と連携して、VLAN への MAC アドレスを動的に登録できます。連携するレイヤ 2 認証機能を次に示します。

- IEEE802.1X
- Web 認証
- MAC 認証
- 認証 VLAN

プリンタやサーバなど、レイヤ 2 認証機能を動作させないで MAC ポートと接続する端末は、その MAC アドレスをコンフィグレーションで VLAN に登録します。

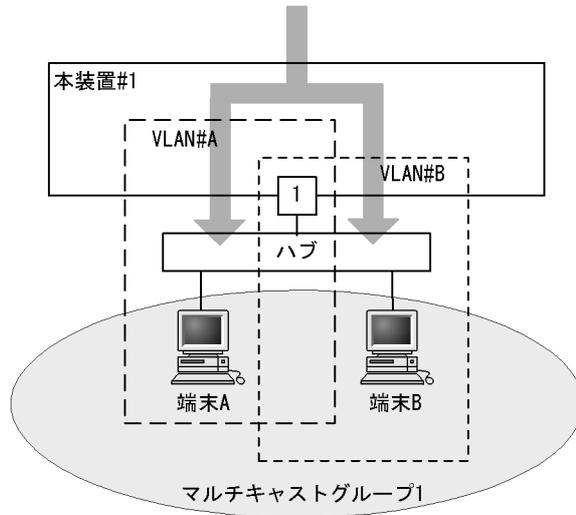
コンフィグレーションとレイヤ 2 認証機能で同じ MAC アドレスを設定した場合、コンフィグレーションの MAC アドレスを登録します。

### 19.7.4 VLAN 混在時のマルチキャストについて

同一ポートに複数の MAC VLAN が混在した場合やポート VLAN と MAC VLAN が混在した場合、それぞれの VLAN に所属する端末が同じマルチキャストグループに所属すると、そのポートへは VLAN ごとに同じマルチキャストフレームを送信するため、端末は同じフレームを重複して受信します。

端末でマルチキャストデータを重複して受信してしまうネットワークの構成例を次に示します。

図 19-10 VLAN 混在時のマルチキャスト



(凡例)  : MACポート

- ・本装置#1のポート1はVLAN#A, #Bの両方に属している。
- ・端末A, Bは同じマルチキャストグループ1に属している。
- ・マルチキャストは, ポート1からVLAN#A, #Bのそれぞれに送信される。

## 19.8 MAC VLAN のコンフィグレーション

### 19.8.1 コンフィグレーションコマンド一覧

MAC VLAN のコンフィグレーションコマンド一覧を次の表に示します。

表 19-10 コンフィグレーションコマンド一覧

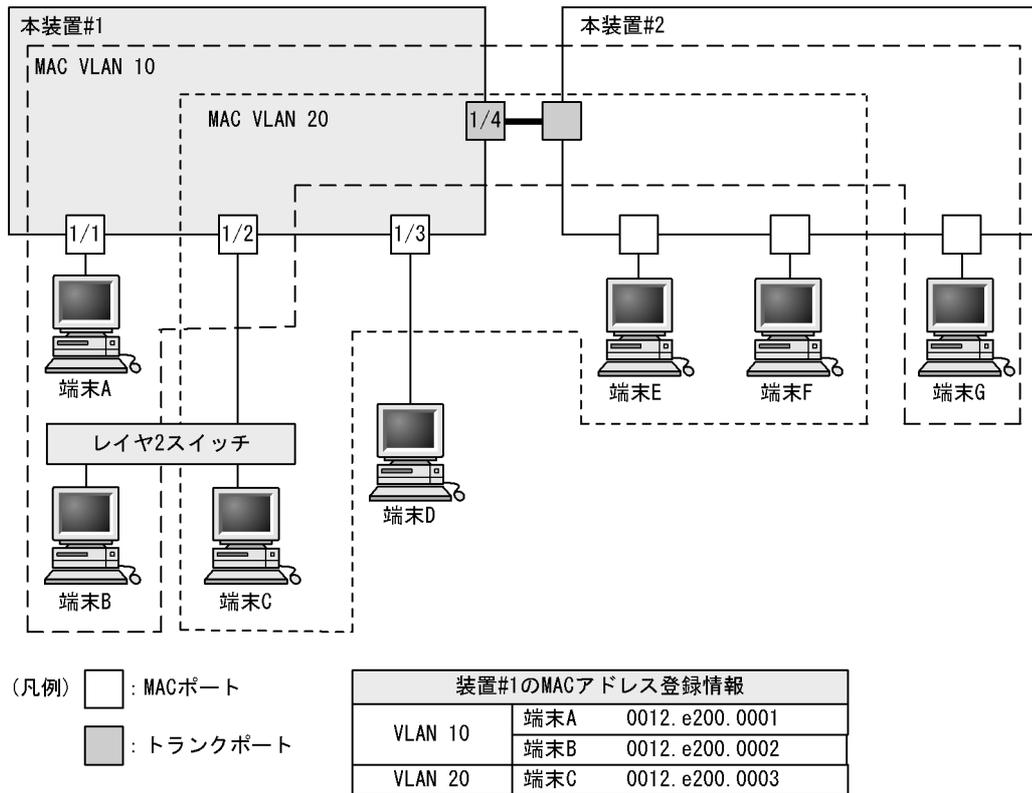
| コマンド名             | 説明                                                     |
|-------------------|--------------------------------------------------------|
| mac-address       | MAC VLAN で VLAN に所属する端末の MAC アドレスをコンフィグレーションによって設定します。 |
| switchport access | アクセスポートの VLAN を設定します。                                  |
| switchport mac    | MAC ポートの VLAN を設定します。                                  |
| switchport mode   | ポートの種類 (MAC, トランク, アクセス) を設定します。                       |
| switchport trunk  | トランクポートの VLAN を設定します。                                  |
| vlan              | mac-based パラメータを指定して MAC VLAN を作成します。                  |

### 19.8.2 MAC VLAN の設定

MAC VLAN を設定する手順を次に示します。ここでは、MAC VLAN と VLAN に所属する MAC アドレスをコンフィグレーションで設定する場合の例を示します。IEEE802.1X との連携については、マニュアル「コンフィグレーションガイド Vol.2 9. IEEE802.1X の設定と運用」を参照してください。

次の図に示す本装置 #1 の設定例を示します。ポート 1/1 は MAC VLAN 10 を設定します。ポート 1/2 は MAC VLAN 10 および 20、1/3 は MAC VLAN 20 を設定します。ただし、ポート 1/3 には MAC アドレスを登録していない端末 D を接続しています。

図 19-11 MAC VLAN の設定例



## (1) MAC VLAN の作成と MAC アドレスの登録

### [ 設定のポイント ]

MAC VLAN を作成します。VLAN を作成する際に VLAN ID と mac-based パラメータを指定します。

また、VLAN に所属する MAC アドレスを設定します。構成例の端末 A ~ C をそれぞれの VLAN に登録します。端末 D は MAC VLAN での通信を許可しない端末にするので登録しません。

### [ コマンドによる設定 ]

#### 1. (config)# vlan 10 mac-based

VLAN 10 を MAC VLAN として作成します。本コマンドで VLAN コンフィグレーションモードに移行します。

#### 2. (config-vlan)# mac-address 0012.e200.0001

```
(config-vlan)# mac-address 0012.e200.0002
```

```
(config-vlan)# exit
```

端末 A (0012.e200.0001), 端末 B (0012.e200.0002) を MAC VLAN 10 に登録します。

#### 3. (config)# vlan 20 mac-based

```
(config-vlan)# mac-address 0012.e200.0003
```

VLAN 20 を MAC VLAN として作成し、端末 C (0012.e200.0003) を MAC VLAN 20 に登録します。

### [ 注意事項 ]

MAC VLAN に登録する MAC アドレスでは、同じ MAC アドレスを複数の VLAN に登録できません。

## (2) MAC ポートの設定

### [ 設定のポイント ]

MAC VLAN で送信元 MAC アドレスによって VLAN を識別するポートは、MAC ポートを設定します。このポートでは Untagged フレームを扱います。

### [ コマンドによる設定 ]

1. (config)# interface range gigabitethernet 1/1-2

ポート 1/1, 1/2 のイーサネットインタフェースコンフィグレーションモードに移行します。ポート 1/1, 1/2 に MAC VLAN 10 を設定するため一括して指定します。

2. (config-if-range)# switchport mode mac-vlan

```
(config-if-range)# switchport mac vlan 10
```

```
(config-if-range)# exit
```

ポート 1/1, 1/2 を MAC ポートに設定します。また、VLAN 10 を設定します。

3. (config)# interface range gigabitethernet 1/2-3

```
(config-if-range)# switchport mode mac-vlan
```

```
(config-if-range)# switchport mac vlan add 20
```

ポート 1/2, 1/3 を MAC ポートに設定します。また、VLAN 20 を設定します。ポート 1/2 にはすでに VLAN 10 を設定しているため、switchport mac vlan add コマンドで追加します。ポート 1/3 は新規の設定と同じ意味になります。

### [ 注意事項 ]

switchport mac vlan コマンドは、それ以前のコンフィグレーションに追加するコマンドではなく指定した <vlan id list> に設定を置き換えます。すでに MAC VLAN を運用中のポートで VLAN の追加や削除を行う場合は、switchport mac vlan add コマンドおよび switchport mac vlan remove コマンドを使用してください。

## (3) トランクポートの設定

### [ 設定のポイント ]

MAC VLAN においても、Tagged フレームを扱うポートはトランクポートとして設定し、そのトランクポートに VLAN を設定します。

### [ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/4

ポート 1/4 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. (config-if)# switchport mode trunk

```
(config-if)# switchport trunk allowed vlan 10,20
```

ポート 1/4 をトランクポートに設定します。また、VLAN 10, 20 を設定します。

### 19.8.3 MAC ポートのネイティブ VLAN の設定

#### [ 設定のポイント ]

MAC ポートで MAC VLAN に登録した MAC アドレスに一致しない Untagged フレームを扱いたい場合、そのフレームを扱う VLAN としてネイティブ VLAN を設定します。ネイティブ VLAN はポート VLAN だけが設定できます。

ネイティブ VLAN の VLAN ID を `switchport mac native vlan` コマンドで指定すると、MAC ポート上で登録した MAC アドレスに一致しない Untagged フレームを扱う VLAN となります。ネイティブ VLAN は、コンフィグレーションで明示して指定しない場合は VLAN 1 (デフォルト VLAN) です。ネイティブ VLAN に `status suspend` が設定されていた場合は、登録した MAC アドレスに一致しないフレームが中継されません。

#### [ コマンドによる設定 ]

1. 

```
(config)# vlan 10,20 mac-based
(config-vlan)# exit
(config)# vlan 30
(config-vlan)# exit
```

VLAN 10,20 を MAC VLAN として作成します。また、VLAN 30 をポート VLAN として作成します。
2. 

```
(config)# interface gigabitethernet 1/1
(config-if)# switchport mode mac-vlan
```

ポート 1/1 のイーサネットインタフェースコンフィグレーションモードに移行します。また、MAC ポートとして設定します。
3. 

```
(config-if)# switchport mac vlan 10,20
```

ポート 1/1 に MAC VLAN 10, 20 を設定します。  
この状態で、ポート 1/1 は MAC VLAN 10, 20 だけ通信を許可するポートとなります。登録されていない MAC アドレスは通信することはできません。登録されていない MAC アドレスから通信するためには、ネイティブ VLAN が通信可能となるように設定します。
4. 

```
(config-if)# switchport mac native vlan 30
```

ポート 1/1 のネイティブ VLAN をポート VLAN 30 に設定します。VLAN 30 はポート 1/1 で登録されていない MAC アドレスからの Untagged フレームを扱う VLAN となります。

## 19.9 VLAN インタフェース

---

### 19.9.1 IP アドレスを設定するインタフェース

本装置をレイヤ 3 スイッチとして使用するためには、VLAN に IP アドレスを設定します。複数の VLAN を作成し、各 VLAN に IP アドレスを設定することで本装置はレイヤ 3 スイッチとして動作します。

IP アドレスはコンフィグレーションコマンド `interface vlan` によって設定します。このインタフェースのことを VLAN インタフェースと呼びます。

### 19.9.2 VLAN インタフェースの MAC アドレス

IP アドレスを設定した VLAN インタフェースは、本装置の持つ MAC アドレスの一つをそのインタフェースの MAC アドレスとして使用します。使用する MAC アドレスを次に示します。

- 装置 MAC アドレス
- VLAN ごとの MAC アドレス

デフォルトでは装置 MAC アドレスを使用します。コンフィグレーションによって VLAN ごとの MAC アドレスを設定できます。

VLAN インタフェースの MAC アドレスは、コンフィグレーションによって運用中に変更できます。運用中に変更すると、隣接するレイヤ 3 装置（ルータ、レイヤ 3 スイッチ、端末など）が ARP や NDP で学習した MAC アドレスと、本装置の MAC アドレスが不一致となり、一時的に通信ができなくなる場合があります。そのため注意してください。

## 19.10 VLAN インタフェースのコンフィグレーション

### 19.10.1 コンフィグレーションコマンド一覧

VLAN インタフェースに IP アドレスを設定し、レイヤ 3 スイッチとして使用するための基本的なコンフィグレーションコマンド一覧を次の表に示します。

表 19-11 コンフィグレーションコマンド一覧

| コマンド名           | 説明                                      |
|-----------------|-----------------------------------------|
| interface vlan  | VLAN インタフェースを設定します。また、インタフェースモードへ移行します。 |
| vlan mac        | VLAN ごとの MAC アドレスを使用することを設定します。         |
| vlan mac prefix | VLAN ごとの MAC アドレスのプレフィックスを設定します。        |
| ip address      | インタフェースの IPv4 アドレスを設定します。               |

注

「コンフィグレーションコマンドリファレンス Vol.3 2. IPv4・ARP・ICMP」を参照してください。

### 19.10.2 レイヤ 3 インタフェースとしての VLAN の設定

[ 設定のポイント ]

VLAN は IP アドレスを設定してレイヤ 3 インタフェースとして使用できます。interface vlan コマンドおよび VLAN インタフェースコンフィグレーションモードでさまざまなレイヤ 3 機能を設定できます。

ここでは、VLAN インタフェースに IPv4 アドレスを設定する例を示します。VLAN インタフェースで設定できるレイヤ 3 機能については、使用する各機能の章を参照してください。

[ コマンドによる設定 ]

1. (config)# interface vlan 10

VLAN 10 の VLAN インタフェースコンフィグレーションモードに移行します。interface vlan コマンドで指定した VLAN ID が未設定の VLAN ID の場合、自動的にポート VLAN を作成して vlan コマンドが設定されます。

2. (config-if)# ip address 192.168.1.1 255.255.255.0

VLAN 10 に IPv4 アドレス 192.168.1.1、サブネットマスク 255.255.255.0 を設定します。

### 19.10.3 VLAN インタフェースの MAC アドレスの設定

本装置の VLAN インタフェースの MAC アドレスは、デフォルトではすべての VLAN で装置 MAC アドレスを使用します。通常、LAN スイッチは VLAN ごとに MAC アドレス学習を行うため、異なる VLAN で同じ MAC アドレスを使用できます。しかし、VLAN ごとではなく装置単位に一つの MAC アドレステーブルを管理する LAN スイッチを同じネットワーク上で使用している場合、異なる VLAN で同じ MAC アドレスを使用すると MAC アドレス学習が安定しなくなる場合があります。そのような場合に VLAN インタフェースの MAC アドレスを VLAN ごとに変更することによってネットワークを安定させることができます。

## [ 設定のポイント ]

VLAN をレイヤ 3 インタフェースとして使用する場合、VLAN インタフェースの MAC アドレスを変更できます。MAC アドレスは `vlan-mac-prefix` コマンドおよび `vlan-mac` コマンドで設定します。VLAN ごとの MAC アドレスは、`vlan-mac-prefix` コマンドで上位 34bit までのプレフィックスを指定し、かつ VLAN ごとに `vlan-mac` コマンドで、VLAN ごとの MAC アドレスを使用することを設定します。MAC アドレスは下位 12bit に VLAN ID を使用します。

## [ コマンドによる設定 ]

1. `(config)# vlan-mac-prefix 0012.e200.0000 ffff.ffff.c000`

VLAN ごと MAC アドレスに使用するプレフィックス (上位 34bit) を指定します。マスクは 34bit で指定する場合 `ffff.ffff.c000` になります。

2. `(config)# vlan 10`

VLAN 10 の VLAN コンフィグレーションモードに移行します。

3. `(config-vlan)# vlan-mac`

VLAN 10 で VLAN ごと MAC アドレスを使用することを設定します。MAC アドレスは下位 12bit に VLAN ID を使用し、この場合 VLAN 10 の MAC アドレスは `0012.e200.000a` になります。

MAC アドレスの値は運用コマンド `show vlan` で確認できます。

## [ 注意事項 ]

VLAN ごと MAC アドレスの設定で、VLAN インタフェースの MAC アドレスが変更になります。これによって、隣接するレイヤ 3 装置 (ルータ、レイヤ 3 スイッチ、端末など) が ARP や NDP で学習した MAC アドレスと本装置の VLAN インタフェースの MAC アドレスが不一致となり、一時的に通信できなくなる場合があります。本機能の設定は VLAN インタフェースの運用開始前に設定するか、または通信の影響が少ないときに行うことをお勧めします。

## 19.11 VLAN のオペレーション

### 19.11.1 運用コマンド一覧

VLAN の運用コマンド一覧を次の表に示します。

表 19-12 運用コマンド一覧

| コマンド名               | 説明                                                 |
|---------------------|----------------------------------------------------|
| show vlan           | VLAN の各種情報を表示します。                                  |
| show vlan mac-vlan  | MAC VLAN に登録されている MAC アドレスを表示します。                  |
| show vlan rate      | VLAN のトラフィックを表示します。                                |
| restart vlan        | VLAN プログラムを再起動します。                                 |
| dump protocols vlan | VLAN プログラムで採取している詳細イベントトレース情報および制御テーブルをファイルへ出力します。 |

### 19.11.2 VLAN の状態の確認

#### (1) VLAN の設定状態の確認

VLAN の情報は show vlan コマンドで確認できます。VLAN ID , Type , IP Address などによって VLAN に関する設定が正しいことを確認してください。また , Untagged はその VLAN で Untagged フレームを扱うポート , Tagged はその VLAN で Tagged フレームを扱うポートになります。VLAN に設定されているポートの設定が正しいことを確認してください。

図 19-12 show vlan コマンドの実行結果

```

> show vlan
Date 2007/01/26 17:01:40 UTC
VLAN counts:4
VLAN ID:1 Type:Port based Status:Up
 Learning:On Tag-Translation:
 BPDU Forwarding: EAPOL Forwarding:
 Router Interface Name:VLAN0001
 IP Address:10.215.201.1/24
 Source MAC address: 0012.e205.0800 (System)
 Description:VLAN0001
 Spanning Tree:PVST+(802.1D)
 AXRP RING ID: AXRP VLAN group:
 GSRP ID: GSRP VLAN group: L3:
 IGMP snooping: MLD snooping:
 Flow mode:
 Untagged(18) :1/1-4,13-26
VLAN ID:3 Type:Port based Status:Up
 Learning:On Tag-Translation:On
 BPDU Forwarding: EAPOL Forwarding:
 Router Interface Name:VLAN0003
 IP Address:10.215.196.1/23
 ee80::220:afff:fed7:8f0a/64
 Source MAC address: 0012.e205.0800 (System)
 Description:VLAN0003
 Spanning Tree:Single(802.1D)
 AXRP RING ID: AXRP VLAN group:
 GSRP ID: GSRP VLAN group: L3:
 IGMP snooping: MLD snooping:
 Flow mode:MAC
 Untagged(8) :1/5-12
 Tagged(2) :1/25-26
 Tag-Trans (2) :1/25-26
VLAN ID:120 Type:Protocol based Status:Up
 Protocol VLAN Information Name:ipv6
 EtherType:08dd LLC: Snap-EtherType:
 Learning:On Tag-Translation:
 BPDU Forwarding: EAPOL Forwarding:
 Router Interface Name:VLAN0120
 IP Address:
 Source MAC address: 0012.e205.0800 (System)
 Description:VLAN0120
 Spanning Tree:
 AXRP RING ID: AXRP VLAN group:
 GSRP ID: GSRP VLAN group: L3:
 IGMP snooping: MLD snooping:
 Flow mode:MAC
 Untagged(3) :1/5,7,9
 Tagged(2) :1/25-26
VLAN ID:1340 Type:Mac based Status:Up
 Learning:On Tag-Translation:
 BPDU Forwarding: EAPOL Forwarding:
 Router Interface Name:VLAN1340
 IP Address:10.215.202.1/24
 Source MAC address: 0012.e2de.053c (VLAN)
 Description:VLAN1340
 Spanning Tree:
 AXRP RING ID: AXRP VLAN group:
 GSRP ID: GSRP VLAN group: L3:
 IGMP snooping: MLD snooping:
 Flow mode:
 Untagged(6) :1/13-18
 Tagged(2) :1/25-26
>

```

## (2) VLAN の通信状態の確認

VLAN の通信状態は show vlan detail コマンドで確認できます。Port Information でポートの Up/Down , Forwarding/Blocking を確認してください。Blocking 状態の場合、括弧内に Blocking の要因が示されています。

図 19-13 show vlan detail コマンドの実行結果

```
>show vlan 3,1000-1500 detail
Date 2007/01/26 17:01:40 UTC
VLAN counts:2
VLAN ID:3 Type:Port based Status:Up
 Learning:On Tag-Translation:On
 BPDU Forwarding: EAPOL Forwarding:
 Router Interface Name:VLAN0003
 IP Address:10.215.196.1/23
 ee80::220:afff:fed7:8f0a/64
 Source MAC address: 0012.e205.0800 (System)
 Description:VLAN0003
 Spanning Tree:Single(802.1D)
 AXRP RING ID: AXRP VLAN group:
 GSRP ID: GSRP VLAN group: L3:
 IGMP snooping: MLD snooping:
 Flow mode:
 Port Information
 1/5 Up Forwarding Untagged
 1/6 Up Blocking (STP) Untagged
 1/7 Up Forwarding Untagged
 1/8 Up Forwarding Untagged
 1/9 Up Forwarding Untagged
 1/10 Up Forwarding Untagged
 1/11 Up Forwarding Untagged
 1/12 Up Forwarding Untagged
 1/25 (CH:9) Up Forwarding Tagged Tag-Translation:103
 1/26 (CH:9) Up Blocking (CH) Tagged Tag-Translation:103
VLAN ID:1340 Type:Mac based Status:Up
 Learning:On Tag-Translation:
 BPDU Forwarding: EAPOL Forwarding:
 Router Interface Name:VLAN1340
 IP Address:10.215.202.1/24
 Source MAC address: 0012.e2de.053c (VLAN)
 Description:VLAN1340
 Spanning Tree:
 AXRP RING ID: AXRP VLAN group:
 GSRP ID: GSRP VLAN group: L3:
 IGMP snooping: MLD snooping:
 Flow mode:MAC
 Port Information
 1/13 Up Forwarding Untagged
 1/14 Up Forwarding Untagged
 1/15 Up Forwarding Untagged
 1/16 Up Forwarding Untagged
 1/17 Up Forwarding Untagged
 1/18 Up Forwarding Untagged
 1/25 (CH:9) Up Forwarding Tagged
 1/26 (CH:9) Up Blocking (CH) Tagged
```

## (3) VLAN ID 一覧の確認

show vlan summary コマンドで、設定した VLAN の種類とその数、VLAN ID を確認できます。

図 19-14 show vlan summary コマンドの実行結果

```
> show vlan summary
Date 2006/03/15 14:15:00 UTC
Total(18) :1,3-5,8,10-20,100,2000
Port based(10) :1,3-5,8,10,12,14,16,18
Protocol based(8) :11,13,15,17,19-20,100,2000
MAC based(0) :
>
```

#### (4) VLAN のリスト表示による確認

show vlan list コマンドは VLAN の設定状態の概要を 1 行に表示します。本コマンドによって、VLAN の設定状態やレイヤ 2 冗長機能、IP アドレスの設定状態を一覧で確認できます。また、VLAN、ポートまたはチャネルグループをパラメータとして指定することで、指定したパラメータの VLAN の状態だけを一覧で確認できます。

図 19-15 show vlan list コマンドの実行結果

```
> show vlan list
Date 2007/01/26 17:01:40 UTC
VLAN counts:4
ID Status Fwd/Up /Cfg Name Type Protocol Ext. IP
 1 Up 16/ 18/ 18 VLAN0001 Port STP PVST+:1D - - - 4
 3 Up 9/ 10/ 10 VLAN0003 Port STP Single:1D - - T M 4/6
120 Up 4/ 5/ 5 VLAN0120 Proto - - - - -
1340 Disable 0/ 8/ 8 VLAN1340 Mac - - - - M 4
AXRP (Control-VLAN)
GSRP GSRP ID:VLAN Group ID(Master/Backup)
S:IGMP/MLD snooping T:Tag Translation M:Flow MAC mode
4:IPv4 address configured 6:IPv6 address configured
>
```

#### (5) MAC VLAN の登録 MAC アドレスの確認

MAC VLAN に登録されている MAC アドレスを、show vlan mac-vlan コマンドで確認できます。

括弧内は MAC アドレスを登録した機能を示しています。

- 「static」はコンフィグレーションで登録した MAC アドレス
- 「dot1x」は IEEE802.1X で登録した MAC アドレス

図 19-16 show vlan mac-vlan コマンドの実行結果

```
> show vlan mac-vlan
Date 2006/03/14 12:16:04 UTC
VLAN counts:2 Total MAC Counts:5
VLAN ID:20 MAC Counts:4
 0012.e200.0001 (static) 0012.e200.0002 (static)
 0012.e200.0003 (static) 0012.e200.0004 (dot1x)
VLAN ID:200 MAC Counts:1
 0012.e200.1111 (dot1x)
>
```

#### (6) VLAN のトラフィックの確認

VLAN のトラフィックを、show vlan rate コマンドで確認できます。

show vlan rate コマンドで表示する VLAN のトラフィックは、装置内の VLAN レイヤで送受信したトラフィックです。したがって、LAN の送受信とは次のような違いがあります。

- 本装置が受信したトラフィックのうち、ストームコントロール機能や、フィルタ・QoS 機能などで廃棄されたトラフィックは、show vlan rate コマンドではカウントされません。
- VLAN が送信したトラフィックのうち、フィルタ・QoS 機能などで廃棄されたり、出力回線の帯域を超えたなどの理由で送信できなかったりしたトラフィックは、show vlan rate コマンドではカウントされますが、LAN には出力されません。

図 19-17 show vlan rate コマンドの実行結果

```
>show vlan rate
Date 2006/10/15 14:15:00
VLAN counts:3
ID Out octets rate (bps) In octets rate (bps)
 1 4400 35.2M 320 25.6k
 10 12345600 98.8M 66540 532.3k
 100 200 1600 123456 987.6k
>
```



# 20 VLAN 拡張機能

この章では、VLAN に適用する拡張機能の解説と操作方法について説明します。

- 
- 20.1 VLAN トンネリングの解説

---

  - 20.2 VLAN トンネリングのコンフィグレーション

---

  - 20.3 Tag 変換の解説

---

  - 20.4 Tag 変換のコンフィグレーション

---

  - 20.5 L2 プロトコルフレーム透過機能の解説

---

  - 20.6 L2 プロトコルフレーム透過機能のコンフィグレーション

---

  - 20.7 VLAN debounce 機能の解説

---

  - 20.8 VLAN debounce 機能のコンフィグレーション

---

  - 20.9 レイヤ 2 中継遮断機能の解説

---

  - 20.10 レイヤ 2 中継遮断機能のコンフィグレーション

---

  - 20.11 VLAN 拡張機能のオペレーション
-

## 20.1 VLAN トンネリングの解説

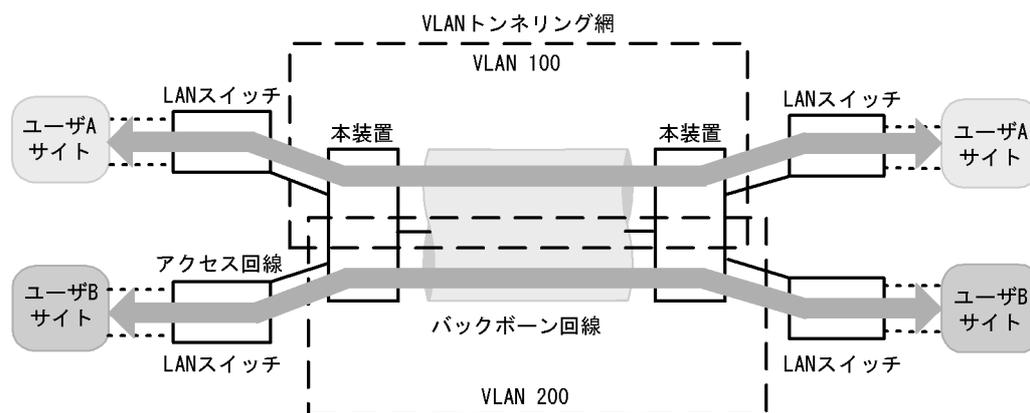
### 20.1.1 概要

VLAN トンネリング機能とは、複数ユーザの VLAN をほかの VLAN の中に集約して「トンネル」する機能です。IEEE802.1Q VLAN Tag をスタックすることで一つの VLAN 内にほかの VLAN に属するフレームをトランスペアレントに通すことができます。トンネルは 3 か所以上のサイトを接続するマルチポイント接続ができます。

VLAN トンネリング概要（広域イーサネットサービス適用例）を次の図に示します。VLAN トンネリングでは、VLAN Tag をスタックすることで VLAN トンネリング網内の VLAN を識別します。

この適用例は、レイヤ 2 VPN サービスである広域イーサネットサービスに適用する場合の例です。本装置に VLAN トンネリング機能を適用します。VLAN トンネリングでは、VLAN Tag をスタックすることで VLAN トンネリング網内の VLAN を識別します。ユーザサイトを収容するポートをアクセス回線、VLAN トンネリング網内に接続するポートをバックボーン回線と呼びます。アクセス回線からのフレームに VLAN Tag を追加してバックボーン回線に中継します。バックボーン回線からのフレームは VLAN Tag を外しアクセス回線へ中継します。

図 20-1 VLAN トンネリング概要（広域イーサネットサービス適用例）



### 20.1.2 VLAN トンネリングを使用するための必須条件

VLAN トンネリング機能を使用する場合は、次の条件に合わせてネットワークを構築する必要があります。

- ポート VLAN を使用します。
- VLAN トンネリング機能を実現する VLAN では、アクセス回線側はトンネリングポートとし、バックボーン回線側をトランクポートとします。
- VLAN トンネリング網内のバックボーン回線では VLAN Tag をスタックするため、通常より 4 バイト大きいサイズのフレームを扱える必要があります。

### 20.1.3 VLAN トンネリング使用時の注意事項

#### (1) 他機能との共存

「17.3 レイヤ2スイッチ機能と他機能の共存について」を参照してください。

#### (2) デフォルト VLAN について

デフォルト VLAN の自動加入を行いません。すべての VLAN を明示的に設定してください。

#### (3) トランクポートのネイティブ VLAN について

VLAN トンネリングのトランクポートは VLAN Tag をスタックするポートとなりますが、ネイティブ VLAN では VLAN Tag をスタックしません。本装置からフレームを送信するときはアクセスポートと同様に動作して、フレームを受信するときは Untagged フレームだけを扱います。ほかの VLAN と異なる動作となるので、VLAN トンネリング網のバックボーン回線の VLAN としては使用できません。VLAN トンネリングを使用する場合、コンフィグレーションコマンド `vlan dot1q tag native` でトランクポートのネイティブ VLAN でも Tagged フレームを扱う設定とすることをお勧めします。

トランクポートのネイティブ VLAN は、コンフィグレーションコマンド `switchport trunk native vlan` で設定しない場合デフォルト VLAN です。デフォルト VLAN で VLAN トンネリング機能を使用する場合は、コンフィグレーションコマンド `vlan dot1q tag native` でトランクポートのネイティブ VLAN でも Tagged フレームを扱う設定とするか、`switchport trunk native vlan` コマンドでネイティブ VLAN にデフォルト VLAN 以外の VLAN を設定してください。

## 20.2 VLAN トンネリングのコンフィグレーション

### 20.2.1 コンフィグレーションコマンド一覧

VLAN トンネリングのコンフィグレーションコマンド一覧を次の表に示します。

表 20-1 コンフィグレーションコマンド一覧

| コマンド名             | 説明                                    |
|-------------------|---------------------------------------|
| switchport access | アクセス回線を設定します。                         |
| switchport mode   | アクセス回線, バックボーン回線を設定するためにポートの種類を設定します。 |
| switchport trunk  | バックボーン回線を設定します。                       |
| mtu               | バックボーン回線でジャンボフレームを設定します。              |

注

「コンフィグレーションコマンドレファレンス Vol.1 12. イーサネット」を参照してください。

### 20.2.2 VLAN トンネリングの設定

#### (1) アクセス回線, バックボーン回線の設定

[ 設定のポイント ]

VLAN トンネリング機能はポート VLAN を使用し, アクセス回線をトンネリングポート, バックボーン回線をトランクポートで設定します。

[ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/1  
ポート 1/1 のイーサネットインタフェースコンフィグレーションモードに移行します。
2. (config-if)# switchport mode dot1q-tunnel  
(config-if)# switchport access vlan 10  
ポート 1/1 をトンネリングポートに設定します。また, VLAN 10 を設定します。

トランクポートのコンフィグレーションについては, 「19.4 ポート VLAN のコンフィグレーション」を参照してください。

#### (2) バックボーン回線のジャンボフレームの設定

[ 設定のポイント ]

バックボーン回線は VLAN Tag をスタックするため通常より 4 バイト以上大きいサイズのフレームを扱います。そのため, ジャンボフレームを設定する必要があります。

[ コマンドによる設定 ]

ジャンボフレームのコンフィグレーションについては, 「15.2.4 ジャンボフレームの設定」を参照してください。

## 20.3 Tag 変換の解説

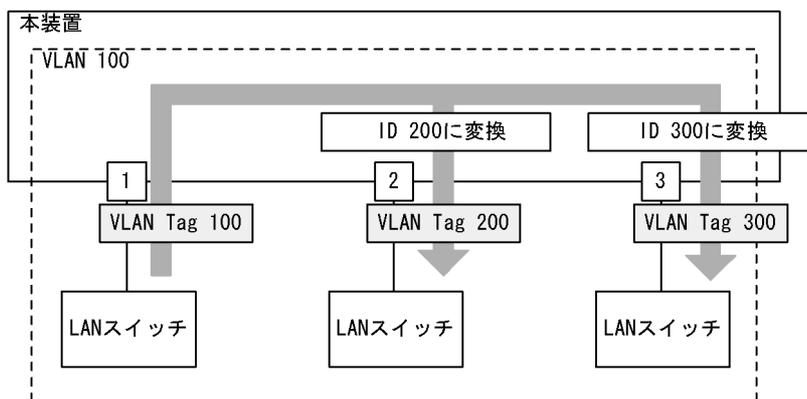
### 20.3.1 概要

Tag 変換は、Tagged フレームをレイヤ 2 スイッチ中継する際に、フレームの VLAN Tag の VLAN ID フィールドを別の値に変換する機能です。この機能によって、異なる VLAN ID で設定した既設の VLAN を一つの VLAN として接続できるようになります。

Tag 変換は、トランクポートで指定します。Tag 変換を使用しない場合は、VLAN Tag の VLAN ID フィールドにその VLAN の VLAN ID を使用します。Tag 変換を指定した場合はその ID を使用します。

Tag 変換の構成例を次の図に示します。図では、ポート 1 で Tag 変換が未指定であり、ポート 2 およびポート 3 にそれぞれ Tag 変換を設定し、VLAN Tag の VLAN ID フィールドを変換して中継します。また、フレームを受信する際にも、各ポートで設定した ID の VLAN Tag のフレームを VLAN 100 で扱います。

図 20-2 Tag 変換の構成例



### 20.3.2 Tag 変換使用時の注意事項

#### (1) 他機能との共存

「17.3 レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

## 20.4 Tag 変換のコンフィグレーション

### 20.4.1 コンフィグレーションコマンド一覧

Tag 変換のコンフィグレーションコマンド一覧を次の表に示します。

表 20-2 コンフィグレーションコマンド一覧

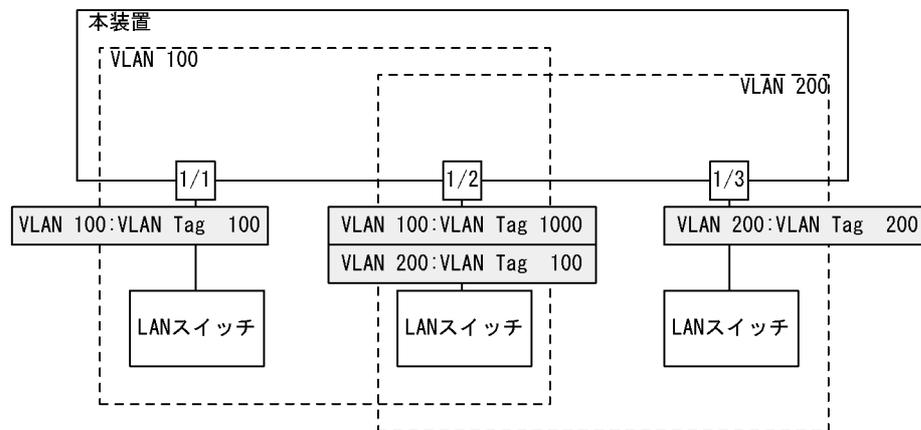
| コマンド名                          | 説明                      |
|--------------------------------|-------------------------|
| switchport vlan mapping        | 変換する ID を設定します。         |
| switchport vlan mapping enable | 指定したポートで Tag 変換を有効にします。 |

### 20.4.2 Tag 変換の設定

Tag 変換を設定する手順を次の図に示します。ここでは、図に示す構成のポート 1/2 の設定例を示します。

構成例では、ポート 1/2 に Tag 変換を適用します。ポート 1/2 では、VLAN 100 のフレームの送受信は VLAN Tag 1000 で行い、VLAN 200 のフレームの送受信は VLAN Tag 100 で行います。このように、VLAN 100 で Tag 変換を行った場合、ほかの VLAN で VLAN Tag 100 を使用することもできます。また、ポート 1/2 では VLAN Tag 200 のフレームを VLAN 200 として扱わないで、未設定の VLAN Tag として廃棄します。

図 20-3 Tag 変換の設定例



#### [ 設定のポイント ]

Tag 変換は、Tag 変換を有効にする設定と、変換する ID を設定することによって動作します。Tag 変換の設定はトランクポートだけ有効です。

Tag 変換は switchport vlan mapping コマンドで設定します。設定した変換を有効にするためには、switchport vlan mapping enable コマンドを設定します。

#### [ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/2  
 (config-if)# switchport mode trunk  
 (config-if)# switchport trunk allowed vlan 100,200  
 ポート 1/2 をトランクポートに設定して、VLAN 100, 200 を設定します。

2. (config-if)# **switchport vlan mapping 1000 100**

(config-if)# **switchport vlan mapping 100 200**

ポート 1/2 で VLAN 100 , 200 に Tag 変換を設定します。VLAN 100 では VLAN Tag 1000 でフレームを送受信して , VLAN 200 では VLAN Tag 100 でフレームを送受信するように設定します。

3. (config-if)# **switchport vlan mapping enable**

ポート 1/2 で Tag 変換を有効にします。本コマンドを設定するまでは Tag 変換は動作しません。

## 20.5 L2 プロトコルフレーム透過機能の解説

### 20.5.1 概要

この機能は、レイヤ 2 のプロトコルフレームを中継する機能です。中継するフレームにはスパンニングツリーの BPDU、IEEE802.1X の EAPOL があります。通常、これらレイヤ 2 のプロトコルフレームは中継しません。

中継するフレームは本装置では単なるマルチキャストフレームとして扱い、本装置のプロトコルには使用しません。

#### (1) BPDU フォワーディング機能

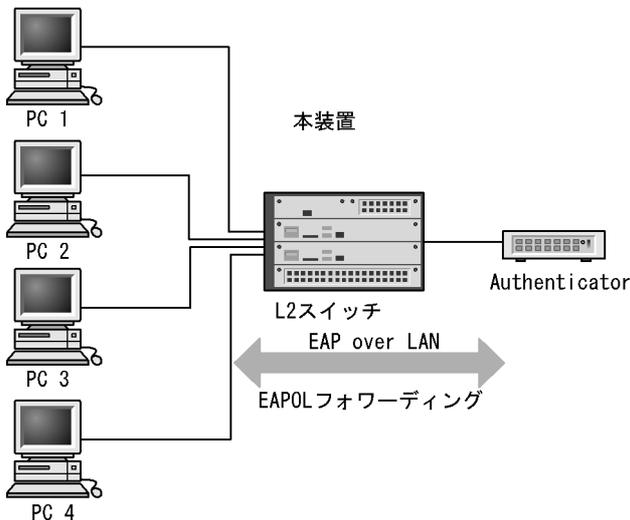
本装置でスパンニングツリーを使用しない場合に BPDU を中継できます。VLAN トンネリングでこの機能を使用すると、ユーザの BPDU を通過させることができます。その際、VLAN トンネリング網のすべてのエッジ装置、コア装置で BPDU フォワーディング機能を設定する必要があります。

アクセスポートまたはトンネリングポートに設定した VLAN およびネイティブ VLAN に BPDU フォワーディング機能を設定すると、シングルスパンニングツリーまたはマルチプルスパンニングツリーの BPDU を中継します。中継する送信側のポートが Tagged フレームを送信する設定になっている場合は、シングルスパンニングツリーまたはマルチプルスパンニングツリーの BPDU に Tag を付けて送信します。

#### (2) EAPOL フォワーディング機能

本装置で IEEE802.1X を使用しない場合に EAPOL を中継できます。本装置を、Authenticator と端末 (Supplicant) の間の L2 スイッチとして用いるときにこの機能を使用します。

図 20-4 EAPOL フォワーディング機能の適用例



### 20.5.2 L2 プロトコルフレーム透過機能の注意事項

#### (1) 他機能との共存

「17.3 レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

## 20.6 L2 プロトコルフレーム透過機能のコンフィグレーション

### 20.6.1 コンフィグレーションコマンド一覧

L2 プロトコルフレーム透過機能のコンフィグレーションコマンド一覧を次の表に示します。

表 20-3 コンフィグレーションコマンド一覧

| コマンド名                 | 説明                         |
|-----------------------|----------------------------|
| l2protocol-tunnel eap | IEEE802.1X の EAPOL を中継します。 |
| l2protocol-tunnel stp | スパンニングツリーの BPDU を中継します。    |

### 20.6.2 L2 プロトコルフレーム透過機能の設定

#### (1) BPDU フォワーディング機能の設定

[ 設定のポイント ]

本機能の設定は VLAN 単位で有効になります。設定した VLAN では、BPDU を中継します。BPDU フォワーディング機能は、対象の VLAN で PVST+ を停止してから設定する必要があります。

[ コマンドによる設定 ]

- (config)# no spanning-tree vlan 20  
(config)# interface vlan 20  
(config-if)# l2protocol-tunnel stp

VLAN20 に BPDU フォワーディング機能を設定します。事前に PVST+ を停止し、BPDU フォワーディング機能を設定します。VLAN20 では BPDU をプロトコルフレームとして扱わないで中継します。

#### (2) EAPOL フォワーディング機能の設定

[ 設定のポイント ]

本機能の設定は VLAN 単位で有効になります。設定した VLAN では EAPOL を中継します。EAPOL フォワーディング機能と IEEE802.1X は同時に使用できません。

[ コマンドによる設定 ]

- (config)# interface vlan 20  
(config-if)# l2protocol-tunnel eap

EAPOL フォワーディング機能を設定します。VLAN20 では EAPOL をプロトコルフレームとして扱わないで中継します。

## 20.7 VLAN debounce 機能の解説

### 20.7.1 概要

VLAN インタフェースは VLAN が通信可能な状態になったときにアップし、VLAN のポートがダウンした場合や、スパンニングツリーなどの機能でブロッキング状態になり通信できなくなった場合にダウンします。

VLAN debounce 機能は、VLAN インタフェースのアップやダウンを遅延させて、ネットワークトポロジーの変更や、ログメッセージ、SNMP Trapなどを削減する機能です。

スパンニングツリーや Ring Protocol などレイヤ 2 での冗長構成を使用したときに障害が発生した場合、通常レイヤ 3 のトポロジー変更と比べて短い時間で代替経路へ切り替わります。VLAN debounce 機能によってレイヤ 2 での代替経路への切替時間まで VLAN インタフェースのダウンを遅延させると、レイヤ 3 のトポロジーを変化させずにすみ、通信の可用性を確保できます。

レイヤ 3 での冗長構成を使用する場合、マスター側に障害が発生したあとの回復時に、両系がマスターとして動作することを防ぐために VLAN インタフェースのアップを遅延させたいとき、VLAN debounce 機能で VLAN インタフェースのアップを遅延できます。

### 20.7.2 VLAN debounce 機能の動作契機

#### (1) VLAN インタフェースのダウンに対する動作契機

VLAN で通信できるポートがなくなった場合に、VLAN インタフェースのダウンに対する VLAN debounce 機能が動作します。VLAN インタフェースのダウンに対する VLAN debounce 機能の動作契機を次の表に示します。

表 20-4 VLAN インタフェースのダウンに対する VLAN debounce 機能の動作契機

| 契機                                      | 備考                                               |
|-----------------------------------------|--------------------------------------------------|
| ポートのリンクダウン                              | -                                                |
| VLAN ポートのブロッキング状態への変更                   | -                                                |
| リンクアップしているポートを VLAN から削除（コンフィグレーションの変更） | VLAN に所属するポートが 0 になった場合は、すぐに VLAN インタフェースもダウンします |

(凡例) - : 該当なし

注 スパンニングツリー、Ring Protocol などによります

#### (2) VLAN インタフェースのアップに対する動作契機

VLAN で通信できるポートが一つできた場合に、VLAN インタフェースのアップに対する VLAN debounce 機能が動作します。ただし、コンフィグレーションコマンド up-debounce の extend パラメータの有無によって動作契機が異なります。VLAN インタフェースのアップに対する VLAN debounce 機能の動作契機を次の表に示します。

表 20-5 VLAN インタフェースのアップに対する VLAN debounce 機能の動作契機

| 契機         | extend パラメータあり | extend パラメータなし |
|------------|----------------|----------------|
| 装置起動および再起動 |                | ×              |

| 契機                                                | extend パラメータあり | extend パラメータなし |
|---------------------------------------------------|----------------|----------------|
| ポートのリンクアップ                                        |                |                |
| VLAN ポートのフォワーディング状態への変更                           |                |                |
| コンフィグレーションコマンド state active で VLAN を enable 状態へ変更 |                | ×              |
| リンクアップしているポートを VLAN に追加 (コンフィグレーションの変更)           |                |                |
| 運用コマンド copy によってランニングコンフィグレーションを変更                |                | ×              |
| 運用コマンド restart vlan の実行                           |                | ×              |

(凡例) : VLAN debounce 機能が動作する × : VLAN debounce 機能が動作しない

注 スパニングツリー, Ring Protocol などによります

## 20.7.3 VLAN debounce 機能と他機能との関係

### (1) スパニングツリー

スパニングツリーでは、ポートに障害が発生して代替経路へ変更されるまでに、スパニングツリーのトポロジへの変更に必要な時間が掛かります。この間に VLAN インタフェースをダウンさせたくない場合は、VLAN インタフェースのダウン遅延時間をトポロジへの変更に必要な時間以上に設定してください。

### (2) Ring Protocol

Ring Protocol を使用する場合、マスタノードではプライマリポートがフォワーディング、セカンダリポートがブロッキングとなっています。VLAN debounce 機能を使わない場合、プライマリポートで障害が発生するといったん VLAN インタフェースがダウンし、セカンダリポートのブロッキングが解除されると再び VLAN インタフェースがアップします。

このようなときに VLAN がいったんダウンすることを防ぐためには、VLAN インタフェースのダウン遅延時間を設定してください。なお、ダウン遅延時間は health-check holdtime コマンドで設定する保護時間以上に設定してください。

### (3) その他の冗長化機能

スパニングツリーや Ring Protocol 以外の冗長化を使用する場合でも、VLAN が短時間にアップやダウンを繰り返すときには、VLAN debounce 機能を使用するとアップやダウンを抑止できます。

## 20.7.4 VLAN debounce 機能使用時の注意事項

### (1) ダウン遅延時間の注意事項

ダウン遅延時間を設定すると、回復しない障害が発生した場合でも VLAN のダウンが遅延します。VLAN debounce 機能でダウンが遅延している間は、通信できない状態です。ダウン遅延時間は、ネットワークの構成や運用に応じて必要な値を設定してください。

VLAN に status コマンドで suspend を設定した場合や VLAN のポートをすべて削除した場合など、コンフィグレーションを変更しないとその VLAN が通信可能とならない場合には、ダウン遅延時間を設定していても VLAN のダウンは遅延しません。

## (2) アップ遅延時間の注意事項

アップ遅延時間を設定すると、いったんアップした VLAN がダウンしたあと、再度アップするときにアップが遅延します。装置を再起動したり、`restart vlan` コマンドで VLAN プログラムを再起動したりすると、VLAN は初期状態になるため、アップ遅延時間を設定していても VLAN のアップは遅延しません。

## (3) 遅延時間の誤差に関する注意事項

アップまたはダウン遅延時間は、ソフトウェアのタイマを使用しているため、CPU 利用率が高い場合には設定した時間より大きくなる場合があります。

## (4) 二重化構成での注意事項

VLAN インタフェースがアップしている状態で系が切り替わると、新たに待機系となったシステムでは VLAN インタフェースがダウンし、新たに運用系となったシステムで VLAN インタフェースがアップします。このとき運用系システムでは、アップ遅延時間が設定されていても VLAN インタフェースのアップは遅延しません。

## 20.8 VLAN debounce 機能のコンフィグレーション

### 20.8.1 コンフィグレーションコマンド一覧

VLAN debounce 機能のコンフィグレーションコマンド一覧を次の表に示します。

表 20-6 コンフィグレーションコマンド一覧

| コマンド名         | 説明                          |
|---------------|-----------------------------|
| down-debounce | VLAN インタフェースのダウン遅延時間を指定します。 |
| up-debounce   | VLAN インタフェースのアップ遅延時間を指定します。 |

### 20.8.2 VLAN debounce 機能の設定

VLAN debounce 機能を設定する手順を次に示します。

#### [ 設定のポイント ]

VLAN debounce 機能の遅延時間は、ネットワーク構成および運用に合わせて最適な値を設定します。

#### [ コマンドによる設定 ]

1. `(config)# interface vlan 100`  
VLAN 100 の VLAN インタフェースモードに移行します。
2. `(config-if)# down-debounce 2`  
`(config-if)# exit`  
VLAN 100 のダウン遅延時間を 2 秒に設定します。
3. `(config)# interface range vlan 201-300`  
VLAN 201-300 の複数 VLAN インタフェースモードに移行します。
4. `(config-if-range)# down-debounce 3`  
`(config-if-range)# exit`  
VLAN 201-300 のダウン遅延時間を 3 秒に設定します。

## 20.9 レイヤ 2 中継遮断機能の解説

---

### 20.9.1 概要

レイヤ 2 中継遮断機能は、本装置内でレイヤ 2 中継をしないで、レイヤ 3 中継だけをする機能です。本機能を使用すると、VLAN 内でブロードキャストフレームやマルチキャストフレームを含むすべてのフレームをレイヤ 2 中継しません。

本機能は、ホテルやマンションなどで端末間の通信を遮断したい場合に利用できます。また、本機能を設定して、複数の端末を一つの VLAN に収容することで、IP アドレスも有効に活用できます。

## 20.10 レイヤ 2 中継遮断機能のコンフィグレーション

---

### 20.10.1 コンフィグレーションコマンド一覧

レイヤ 2 中継遮断機能のコンフィグレーションコマンド一覧を次の表に示します。

表 20-7 コンフィグレーションコマンド一覧

| コマンド名                     | 説明                     |
|---------------------------|------------------------|
| <code>l2-isolation</code> | VLAN 内のレイヤ 2 中継を遮断します。 |

### 20.10.2 レイヤ 2 中継遮断機能の設定

レイヤ 2 中継遮断機能を設定する手順を次に示します。

[ コマンドによる設定 ]

1. `(config)# l2-isolation`  
レイヤ 2 中継遮断機能を設定します。

## 20.11 VLAN 拡張機能のオペレーション

### 20.11.1 運用コマンド一覧

VLAN 拡張機能の運用コマンド一覧を次の表に示します。

表 20-8 運用コマンド一覧

| コマンド名     | 説明                    |
|-----------|-----------------------|
| show vlan | VLAN 拡張機能の設定状態を確認します。 |

### 20.11.2 VLAN 拡張機能の確認

#### (1) VLAN の通信状態の確認

VLAN 拡張機能の設定状態を show vlan detail コマンドで確認できます。show vlan detail コマンドによる VLAN 拡張機能の確認方法を次の表に示します。

表 20-9 show vlan detail コマンドによる VLAN 拡張機能の確認方法

| 機能               | 確認方法                                           |
|------------------|------------------------------------------------|
| VLAN トンネリング      | 先頭に " VLAN tunneling enabled " を表示します。         |
| Tag 変換           | Port Information で " Tag-Translation " を表示します。 |
| L2 プロトコルフレーム透過機能 | BPDU Forwarding , EAPOL Forwarding の欄に表示します。   |

図 20-5 show vlan detail コマンドの実行結果

```
>show vlan 10 detail
Date 2006/03/15 16:28:23 UTC
VLAN counts:1 VLAN tunneling enabled ...1
VLAN ID:10 Type:Port based Status:Up
 Learning:On Tag-Translation:On
 BPDU Forwarding:On EAPOL Forwarding: ...3
 .
 .
 .
Port Information
 1/5 Up Forwarding Tagged Tag-Translation:1000 ...2
 1/6 Down - Tagged Tag-Translation:2000 ...2
 1/7 Up Forwarding Tagged
>
```

1. VLAN トンネリングが有効であることを示します。
2. このポートに Tag 変換が設定されていることを示します。
3. BPDU フォワーディング機能が設定され、EAPOL フォワーディング機能が設定されていないことを示します。

# 21 スパニングツリー

この章では、スパニングツリー機能の解説と操作方法について説明します。

- 
- 21.1 スパニングツリーの概説

---

  - 21.2 スパニングツリー動作モードのコンフィグレーション

---

  - 21.3 PVST+ 解説

---

  - 21.4 PVST+ のコンフィグレーション

---

  - 21.5 PVST+ のオペレーション

---

  - 21.6 シングルスパニングツリー解説

---

  - 21.7 シングルスパニングツリーのコンフィグレーション

---

  - 21.8 シングルスパニングツリーのオペレーション

---

  - 21.9 マルチプルスパニングツリー解説

---

  - 21.10 マルチプルスパニングツリーのコンフィグレーション

---

  - 21.11 マルチプルスパニングツリーのオペレーション

---

  - 21.12 スパニングツリー共通機能解説

---

  - 21.13 スパニングツリー共通機能のコンフィグレーション

---

  - 21.14 スパニングツリー共通機能のオペレーション
-

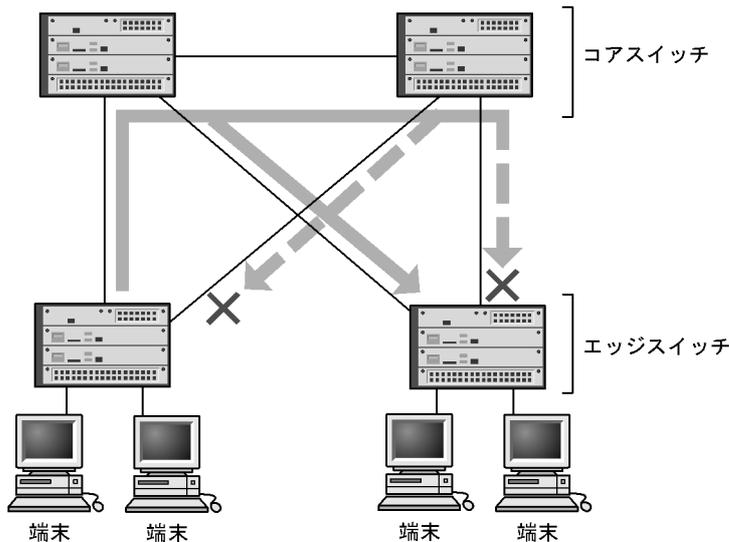
## 21.1 スパニングツリーの概説

### 21.1.1 概要

スパニングツリープロトコルは、レイヤ 2 のループ防止プロトコルです。スパニングツリープロトコルを使用することで、レイヤ 2 ネットワークを冗長化し、ループを防止できます。

スパニングツリーを適用したネットワークの概要を次の図に示します。

図 21-1 スパニングツリーを適用したネットワークの概要



(凡例) × : Blocking状態

図の構成は、ネットワークのコアを担うスイッチを冗長化し、また、端末を収容するエッジスイッチからの通信経路を冗長化しています。装置および通信経路を冗長化することで、通常の通信経路に障害が発生しても代替の経路で通信を継続できます。

レイヤ 2 ネットワークを冗長化するとレイヤ 2 ループの構成になります。レイヤ 2 のループはブロードキャストストームの発生や MAC アドレス学習が安定しないなどの問題を引き起こします。スパニングツリーは、冗長化してループ構成になったレイヤ 2 ネットワークで、通信を止める場所を選択して Blocking 状態とすることでループを防止するプロトコルです。

### 21.1.2 スパニングツリーの種類

本装置では、PVST+、シングルスパニングツリーおよびマルチプルスパニングツリーの 3 種類のスパニングツリーをサポートします。各スパニングツリーは構築の単位が異なります。スパニングツリーの種類と概要について次の表に示します。

表 21-1 スパニングツリーの種類

| 名称    | 構築単位    | 概要                                                                    |
|-------|---------|-----------------------------------------------------------------------|
| PVST+ | VLAN 単位 | VLAN 単位にツリーを構築します。一つのポートに複数の VLAN が所属している場合、VLAN ごとに異なるツリー構築結果を適用します。 |

| 名称            | 構築単位         | 概要                                                                                                         |
|---------------|--------------|------------------------------------------------------------------------------------------------------------|
| シングルスパニングツリー  | 装置単位         | 装置全体のポートを対象としツリーを構築します。VLAN 構成とは無関係に装置のすべてのポートにツリー構築結果を適用します。                                              |
| マルチプルスパニングツリー | MST インスタンス単位 | 複数の VLAN をまとめた MST インスタンスというグループごとにスパニングツリーを構築します。一つのポートに複数の VLAN が所属している場合、MST インスタンス単位に異なるツリー構築結果を適用します。 |

本装置では、上記で記述したスパニングツリーを単独または組み合わせて使用できます。スパニングツリーの組み合わせと適用範囲を次の表に示します。

表 21-2 スパニングツリーの組み合わせと適用範囲

| ツリー構築条件                   | トポロジー計算結果の適用範囲                                                                                                     |
|---------------------------|--------------------------------------------------------------------------------------------------------------------|
| PVST+ 単独                  | PVST+ が動作している VLAN には VLAN ごとのスパニングツリーを適用します。そのほかの VLAN はスパニングツリーを適用しません。<br>本装置では、デフォルトでポート VLAN 上で PVST+ が動作します。 |
| シングルスパニングツリー単独            | 全 VLAN にシングルスパニングツリーを適用します。PVST+ をすべて停止した構成です。                                                                     |
| PVST+ とシングルスパニングツリーの組み合わせ | PVST+ が動作している VLAN には VLAN ごとのスパニングツリーを適用します。そのほかの VLAN にはシングルスパニングツリーを適用します。                                      |
| マルチプルスパニングツリー単独           | 全 VLAN にマルチプルスパニングツリーを適用します。                                                                                       |

注 マルチプルスパニングツリーはほかのツリーと組み合わせて使用できません。

### 21.1.3 スパニングツリーと高速スパニングツリー

PVST+、シングルスパニングツリーには IEEE802.1D のスパニングツリーと IEEE802.1w の高速スパニングツリーの 2 種類があります。それぞれ、PVST+ と Rapid PVST+、STP と Rapid STP と呼びます。

スパニングツリープロトコルのトポロジー計算は、通信経路を変更する際にいったんポートを通信不可状態（Blocking 状態）にしてから複数の状態を遷移して通信可能状態（Forwarding 状態）になります。IEEE 802.1D のスパニングツリーはこの状態遷移においてタイマによる状態遷移を行うため、通信可能となるまでに一定の時間が掛かります。IEEE 802.1w の高速スパニングツリーはこの状態遷移でタイマによる待ち時間を省略して高速な状態遷移を行うことで、トポロジー変更によって通信が途絶える時間を最小限にします。

なお、マルチプルスパニングツリーは IEEE802.1s として規格化されたもので、状態遷移の時間は IEEE802.1w と同等です。それぞれのプロトコルの状態遷移とそれに必要な時間を以下に示します。

表 21-3 PVST+、STP(シングルスパニングツリー)の状態遷移

| 状態       | 状態の概要                                                                      | 次の状態への遷移               |
|----------|----------------------------------------------------------------------------|------------------------|
| Disable  | ポートが使用できない状態です。使用可能となるとすぐに Blocking に遷移します。                                | -                      |
| Blocking | 通信不可の状態で、MAC アドレス学習も行いません。リンクアップ直後またはトポロジーが安定して Blocking になるポートもこの状態になります。 | 20 秒（変更可能）または BPDU を受信 |

| 状態         | 状態の概要                                                                        | 次の状態への遷移    |
|------------|------------------------------------------------------------------------------|-------------|
| Listening  | 通信不可の状態です。MAC アドレス学習も行いません。該当ポートが Learning になる前に、トポロジーが安定するまで待つ期間です。         | 15 秒 (変更可能) |
| Learning   | 通信不可の状態です。しかし、MAC アドレス学習は行います。該当ポートが Forwarding になる前に、事前に MAC アドレス学習を行う期間です。 | 15 秒 (変更可能) |
| Forwarding | 通信可能な状態です。トポロジーが安定した状態です。                                                    | -           |

(凡例) - : 該当なし

表 21-4 Rapid PVST+ , Rapid STP( シングルスパニングツリー ) の状態遷移

| 状態         | 状態の概要                                                                        | 次の状態への遷移          |
|------------|------------------------------------------------------------------------------|-------------------|
| Disable    | ポートが使用できない状態です。使用可能となるとすぐに Discarding に遷移します。                                | -                 |
| Discarding | 通信不可の状態です。MAC アドレス学習も行いません。該当ポートが Learning になる前に、トポロジーが安定するまで待つ期間です。         | 省略または 15 秒 (変更可能) |
| Learning   | 通信不可の状態です。しかし、MAC アドレス学習は行います。該当ポートが Forwarding になる前に、事前に MAC アドレス学習を行う期間です。 | 省略または 15 秒 (変更可能) |
| Forwarding | 通信可能な状態です。トポロジーが安定した状態です。                                                    | -                 |

(凡例) - : 該当なし

Rapid PVST+ , Rapid STP では、対向装置からの BPDU 受信によって Discarding と Learning 状態を省略します。この省略により、高速なトポロジー変更を行います。

高速スパニングツリーを使用する際は、以下の条件に従って設定してください。条件を満たさない場合、Discarding , Learning を省略しないで高速な状態遷移を行わない場合があります。

- トポロジーの全体を同じプロトコル ( Rapid PVST+ または Rapid STP ) で構築する ( Rapid PVST+ と Rapid STP の相互接続は、「21.3.2 アクセスポートの PVST+」を参照してください)。
- スパニングツリーが動作する装置間は Point-to-Point 接続する。
- スパニングツリーが動作する装置を接続しないポートでは PortFast を設定する。

### 21.1.4 スパニングツリートポロジーの構成要素

スパニングツリーのトポロジーを設計するためには、ブリッジやポートの役割およびそれらの役割を決定するために用いる識別子などのパラメータがあります。これらの構成要素とトポロジー設計における利用方法を以下に示します。

#### (1) ブリッジの役割

ブリッジの役割を次の表に示します。スパニングツリーのトポロジー設計はルートブリッジを決定することから始まります。

表 21-5 ブリッジの役割

| ブリッジの役割 | 概要                                            |
|---------|-----------------------------------------------|
| ルートブリッジ | トポロジーを構築する上で論理的な中心となるスイッチです。トポロジー内に一つだけ存在します。 |

| ブリッジの役割 | 概要                                              |
|---------|-------------------------------------------------|
| 指定ブリッジ  | ルートブリッジ以外のスイッチです。ルートブリッジの方向からのフレームを転送する役割を担います。 |

## (2) ポートの役割

ポートの役割を次の表に示します。指定ブリッジは3種類のポートの役割を持ちます。ルートブリッジは、以下の役割のうち、すべてのポートが指定ポートとなります。

表 21-6 ポートの役割

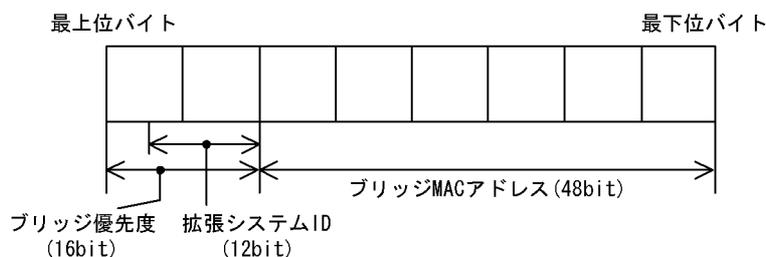
| ポートの役割 | 概要                                                              |
|--------|-----------------------------------------------------------------|
| ルートポート | 指定ブリッジからルートブリッジへ向かう通信経路のポートです。通信可能なポートとなります。                    |
| 指定ポート  | ルートポート以外の通信可能なポートです。ルートブリッジからの通信経路でトポロジーの下流へ接続するポートです。          |
| 非指定ポート | ルートポート、指定ポート以外のポートで、通信不可の状態のポートです。障害が発生した際に通信可能になり代替経路として使用します。 |

## (3) ブリッジ識別子

トポロジー内の装置を識別するパラメータをブリッジ識別子と呼びます。ブリッジ識別子が最も小さい装置が優先度が高く、ルートブリッジとして選択されます。

ブリッジ識別子はブリッジ優先度 (16bit) とブリッジ MAC アドレス (48bit) で構成されます。ブリッジ優先度の下位 12bit は拡張システム ID です。拡張システム ID には、シングルスパニングツリー、マルチプルスパニングツリーの場合は 0 が設定され、PVST+ の場合は VLAN ID が設定されます。ブリッジ識別子を次の図に示します。

図 21-2 ブリッジ識別子



## (4) パスコスト

スイッチ上の各ポートの通信速度に対応するコスト値をパスコストと呼びます。指定ブリッジからルートブリッジへ到達するために経由するすべてのポートのコストを累積した値をルートパスコストと呼びます。ルートブリッジへ到達するための経路が2種類以上ある場合、ルートパスコストが最も小さい経路を使用します。

速度が速いポートほどパスコストを低くすることをお勧めしています。パスコストはデフォルト値がポートの速度に応じた値となっていて、コンフィグレーションで変更することもできます。

## (5) ポート識別子

スイッチ内の各ポートを識別するパラメータをポート識別子と呼びます。ポート識別子は2台のスイッチ間で2本以上の冗長接続をし、かつ各ポートでパスコストを変更できない場合に通信経路の選択に使用し

ます。ただし、2 台のスイッチ間の冗長接続はリンクアグリゲーションを使用することをお勧めします。リンクアグリゲーションをサポートしていない装置と冗長接続するためにはスパニングツリーを使用してください。

ポート識別子はポート優先度（4bit）とポート番号（12bit）によって構成されます。ポート識別子を次の図に示します。

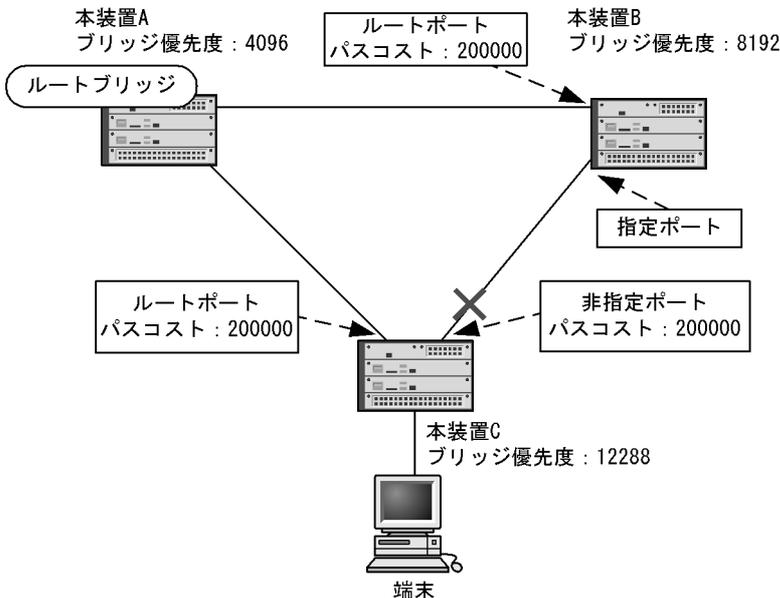
図 21-3 ポート識別子



### 21.1.5 スパニングツリーのトポロジー設計

スパニングツリーは、ブリッジ識別子、パスコストによってトポロジーを構築します。次の図に、トポロジー設計の基本的な手順を示します。図の構成は、コアスイッチとして 2 台を冗長化して、エッジスイッチとして端末を収容するスイッチを配置する例です。

図 21-4 スパニングツリーのトポロジー設計



#### (1) ブリッジ識別子によるルートブリッジの選出

ルートブリッジは、ブリッジ識別子の最も小さい装置を選出します。通常、ルートブリッジにしたい装置のブリッジ優先度を最も小さい値（最高優先度）に設定します。図の例では、本装置 A がルートブリッジになるように設定します。本装置 B、本装置 C は指定ブリッジとなります。

また、ルートブリッジに障害が発生した場合に代替のルートブリッジとして動作するスイッチを本装置 B になるように設定します。本装置 C は最も低い優先度として設定します。

スパニングツリーのトポロジー設計では、図の例のようにネットワークのコアを担う装置をルートブリッジとし、代替のルートブリッジとしてコアを冗長化する構成をお勧めします。

## (2) 通信経路の設計

ルートブリッジを選出した後、各指定ブリッジからルートブリッジに到達するための通信経路を決定します。

### (a) パスコストによるルートポートの選出

本装置 B、本装置 C では、ルートブリッジに到達するための経路を最も小さいルートパスコスト値になるよう決定します。図の例は、すべてのポートがパスコスト 200000 としています。それぞれ直接接続したポートが最もルートパスコストが小さく、ルートポートとして選出します。

ルートパスコストの計算は、指定ブリッジからルートブリッジへ向かう経路で、各装置がルートブリッジの方向で送信するポートのパスコストの総和で比較します。例えば、本装置 C の本装置 B を経由する経路はパスコストが 400000 となりルートポートには選択されません。

パスコストは、ポートの速度が速いほど小さい値をデフォルト値に持ちます。また、ルートポートの選択にはルートブリッジまでのコストの総和で比較します。そのため、速度の速いポートや経由する装置の段数が少ない経路を優先して使用したい場合、通常はパスコスト値を変更する必要はありません。速度の遅いポートを速いポートより優先して経路として使用したい場合はコンフィグレーションで変更することによって通信したい経路を設計します。

### (b) 指定ポート、非指定ポートの選出

本装置 B、本装置 C 間の接続はルートポート以外のポートでの接続になります。このようなポートではどれかのポートが非指定ポートとなって Blocking 状態になります。スパニングツリーは、このように片側が Blocking 状態となることでループを防止します。

指定ポート、非指定ポートは次のように選出します。

- 装置間でルートパスコストが小さい装置が指定ポート、大きい装置が非指定ポートになります。
- ルートパスコストが同一の場合、ブリッジ識別子の小さい装置が指定ポート、大きい装置が非指定ポートになります。

図の例では、ルートパスコストは同一です。ブリッジ優先度によって本装置 B が指定ポート、本装置 C が非指定ポートとなり、本装置 C が Blocking 状態となります。Blocking 状態になるポートを本装置 B にしたい場合は、パスコストを調整して本装置 B のルートパスコストが大きくなるように設定します。

## 21.1.6 STP 互換モード

### (1) 概要

Rapid PVST+、Rapid STP、およびマルチプルスパニングツリーで、対向装置が PVST+ または STP の場合、該当するポートは STP 互換モードで動作します。

STP 互換モードで動作すると、該当するポートで高速遷移が行われなくなり、通信復旧に時間が掛かるようになります。

対向装置が Rapid PVST+、Rapid STP、およびマルチプルスパニングツリーに変わった場合、STP 互換モードから復旧し、再び高速遷移が行われるようになりますが、タイミングによって該当するポートと対向装置が STP 互換モードで動作し続けることがあります。

STP 互換モード復旧機能は、STP 互換モードで動作しているポートを強制的に復旧させ、正常に高速遷移

ができるようにします。

## (2) 復旧機能

運用コマンド `clear spanning-tree detected-protocol` を実行することで、STP 互換モードから強制的に復旧します。該当するポートのリンクタイプが `point-to-point`、`shared` のどちらの場合でも動作します。

## (3) 自動復旧機能

該当するポートのリンクタイプが `point-to-point` の場合、STP 互換モード復旧機能が自動で動作します。

該当するポートが非指定ポートで STP 互換モードで動作した場合、該当するポートから RST BPDU または MST BPDU を送信することで、STP 互換モードを解除します。

該当するポートのリンクタイプが `shared` の場合、自動復旧モードが正しく動作できないため、自動復旧モードは動作しません。

## 21.1.7 スパニングツリー共通の注意事項

### (1) CPU の過負荷について

CPU が過負荷な状態になった場合、本装置が送受信する BPDU の廃棄が発生して、タイムアウトのメッセージ出力、トポロジー変更、一時的な通信断となることがあります。

### (2) 二重化構成で BPDU ガード機能を使用する場合について

BPDU ガード機能によってポートがダウンした場合、系切替が発生すると新運用系システムでそのポートがダウンしたままになります。この状態でコマンドによってスパニングツリーの状態を出力すると、BPDU ガードでポートがダウンしたのではなく、最初からポートがダウンしていたように出力されます。

### (3) VLAN トンネリングについて

VLAN トンネリング設定時、アクセスポート（VLAN トンネリングのアクセス回線側）はスパニングツリーの対象外になります。トランクポート（バックボーン回線側）だけがスパニングツリーを使用できません。

### (4) VLAN のダウンを伴うコンフィグレーションコマンドの設定について

コンフィグレーションコマンド `no spanning-tree disable` で本装置にスパニングツリー機能を適用すると、全 VLAN が一時的にダウンします。

## 21.2 スパニングツリー動作モードのコンフィグレーション

スパニングツリーの動作モードを設定します。

コンフィグレーションを設定しない状態で本装置を起動すると、動作モードは `pvst` で動作します。

### 21.2.1 コンフィグレーションコマンド一覧

スパニングツリー動作モードのコンフィグレーションコマンド一覧を次の表に示します。

表 21-7 コンフィグレーションコマンド一覧

| コマンド名                                  | 説明                                    |
|----------------------------------------|---------------------------------------|
| <code>spanning-tree disable</code>     | スパニングツリー機能の停止を設定します。                  |
| <code>spanning-tree mode</code>        | スパニングツリー機能の動作モードを設定します。               |
| <code>spanning-tree single mode</code> | シングルスパニングツリーの STP と Rapid STP を選択します。 |
| <code>spanning-tree vlan mode</code>   | VLAN ごとに PVST+ と Rapid PVST+ を選択します。  |

### 21.2.2 動作モードの設定

スパニングツリーは装置の動作モードを設定することで各種スパニングツリーを使用することができます。装置の動作モードを次の表に示します。動作モードを設定しない場合、`pvst` モードで動作します。

動作モードに `rapid-pvst` を指定しても、シングルスパニングツリーのデフォルトは STP であることに注意してください。

表 21-8 スパニングツリー動作モード

| コマンド名                                      | 説明                                                                                          |
|--------------------------------------------|---------------------------------------------------------------------------------------------|
| <code>spanning-tree disable</code>         | スパニングツリーを停止します。                                                                             |
| <code>spanning-tree mode pvst</code>       | PVST+ とシングルスパニングツリーを使用できます。デフォルトで PVST+ が動作します。シングルスパニングツリーはデフォルトでは動作しません。                  |
| <code>spanning-tree mode rapid-pvst</code> | PVST+ とシングルスパニングツリーを使用できます。デフォルトで高速スパニングツリーの Rapid PVST+ が動作します。シングルスパニングツリーはデフォルトでは動作しません。 |
| <code>spanning-tree mode mst</code>        | マルチプルスパニングツリーが動作します。                                                                        |

#### (1) 動作モード `pvst` の設定

##### [ 設定のポイント ]

装置の動作モードを `pvst` に設定します。ポート VLAN を作成すると、その VLAN で自動的に PVST+ が動作します。VLAN ごとに Rapid PVST+ に変更することもできます。

シングルスパニングツリーはデフォルトでは動作しないで、設定することで動作します。その際、デフォルトでは STP で動作し、Rapid STP に変更することもできます。

##### [ コマンドによる設定 ]

##### 1. (config)# `spanning-tree mode pvst`

スパニングツリーの動作モードを `pvst` に設定します。ポート VLAN で自動的に PVST+ が動作しま

す。

2. `(config)# spanning-tree vlan 10 mode rapid-pvst`  
VLAN 10 の動作モードを Rapid PVST+ に変更します。ほかのポート VLAN は PVST+ で動作し、VLAN 10 は Rapid PVST+ で動作します。
3. `(config)# spanning-tree single`  
シングルスパニングツリーを動作させます。PVST+ を使用していない VLAN に適用します。デフォルトでは STP で動作します。
4. `(config)# spanning-tree single mode rapid-stp`  
シングルスパニングツリーを Rapid STP に変更します。

## (2) 動作モード rapid-pvst の設定

### [ 設定のポイント ]

装置の動作モードを rapid-pvst に設定します。ポート VLAN を作成すると、その VLAN で自動的に Rapid PVST+ が動作します。VLAN ごとに PVST+ に変更することもできます。

シングルスパニングツリーはデフォルトでは動作しないで、設定することで動作します。動作モードに rapid-pvst を指定しても、シングルスパニングツリーのデフォルトは STP であることに注意してください。

### [ コマンドによる設定 ]

1. `(config)# spanning-tree mode rapid-pvst`  
スパニングツリーの動作モードを rapid-pvst に設定します。ポート VLAN で自動的に Rapid PVST+ が動作します。
2. `(config)# spanning-tree vlan 10 mode pvst`  
VLAN 10 の動作モードを PVST+ に変更します。ほかのポート VLAN は Rapid PVST+ で動作し、VLAN 10 は PVST+ で動作します。
3. `(config)# spanning-tree single`  
シングルスパニングツリーを動作させます。PVST+ を使用していない VLAN に適用します。デフォルトでは STP で動作します。
4. `(config)# spanning-tree single mode rapid-stp`  
シングルスパニングツリーを Rapid STP に変更します。

## (3) 動作モード mst の設定

### [ 設定のポイント ]

マルチプルスパニングツリーを使用する場合、装置の動作モードを mst に設定します。マルチプルスパニングツリーはすべての VLAN に適用します。PVST+ やシングルスパニングツリーとは併用できません。

### [ コマンドによる設定 ]

1. `(config)# spanning-tree mode mst`

マルチブルスパニングツリーを動作させます。

#### (4) スパニングツリーを停止する設定

##### [ 設定のポイント ]

スパニングツリーを使用しない場合、`disable` を設定することで本装置のスパニングツリーをすべて停止します。

##### [ コマンドによる設定 ]

1. `(config)# spanning-tree disable`  
スパニングツリーの動作を停止します。

## 21.3 PVST+ 解説

PVST+ は、VLAN 単位にツリーを構築します。VLAN 単位にツリーを構築できるため、ロードバランシングが可能です。また、アクセスポートでは、シングルスパニングツリーで動作しているスイッチと接続できます。

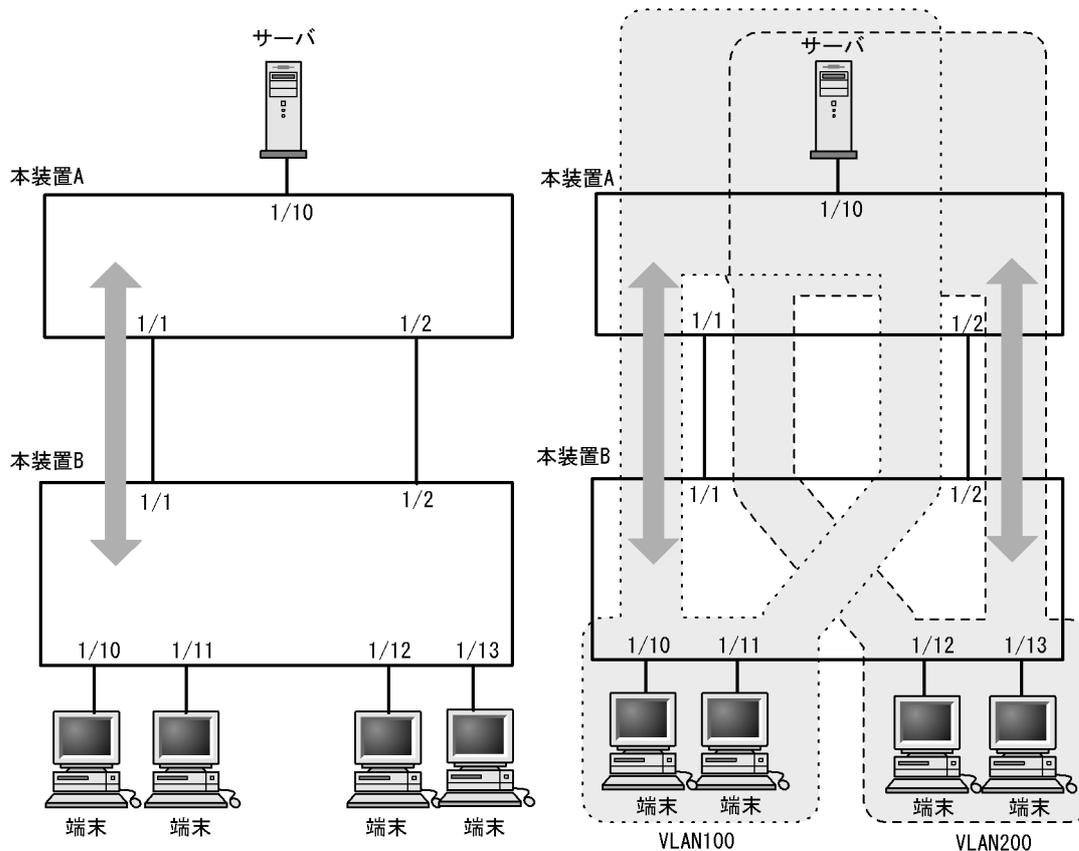
### 21.3.1 PVST+ によるロードバランシング

次の図に示すような本装置 A、B 間で冗長パスを組んだネットワークにおいてシングルスパニングツリーを組んだ場合、各端末からサーバへのアクセスは本装置 A、B 間のポート 1 に集中します。そこで、複数の VLAN を組み、PVST+ によって VLAN ごとに別々のトポロジーとなるように設定することで冗長パスとして使用できるようになり、さらに負荷分散を図れます。ポート優先度によるロードバランシングの例を次の図に示します。

この例では、VLAN100 に対してはポート 1/1 のポート優先度をポート 1/2 より高く設定し、逆に VLAN200 に対しては 1/2 のポート優先度をポート 1/1 より高く設定することで、各端末からサーバに対するアクセスを VLAN ごとに負荷分散を行っています。

図 21-5 PVST+ によるロードバランシング

- (1) シングルスパニングツリー時ポート1/2は冗長パスとして通常は未使用のためポート1/1に負荷が集中する。 (2) PVST+でVLANごとに別々のトポロジーとすることで本装置A、B間の負荷分散が可能になる。



## 21.3.2 アクセスポートのPVST+

### (1) 解説

シングルスパニングツリーを使用している装置、または装置で一つのツリーを持つシングルスパニングツリーに相当する機能をサポートしている装置（以降、単にシングルスパニングツリーと表記します）とPVST+を用いてネットワークを構築できます。シングルスパニングツリーで運用している装置をエッジスイッチ、本装置をコアスイッチに配置して使います。このようなネットワークを構築することで、次のメリットがあります。

- エッジスイッチに障害が発生しても、ほかのエッジスイッチにトポロジー変更の影響が及ばない。
- コアスイッチ間でロードバランスができる。

シングルスパニングツリーとは、アクセスポートで接続できます。構成例を次の図に示します。この例では、エッジスイッチでシングルスパニングツリーを動作させ、コアスイッチでPVST+を動作させています。コアスイッチではエッジスイッチと接続するポートをアクセスポートとしています。各エッジスイッチはそれぞれ単一のVLANを設定しています。

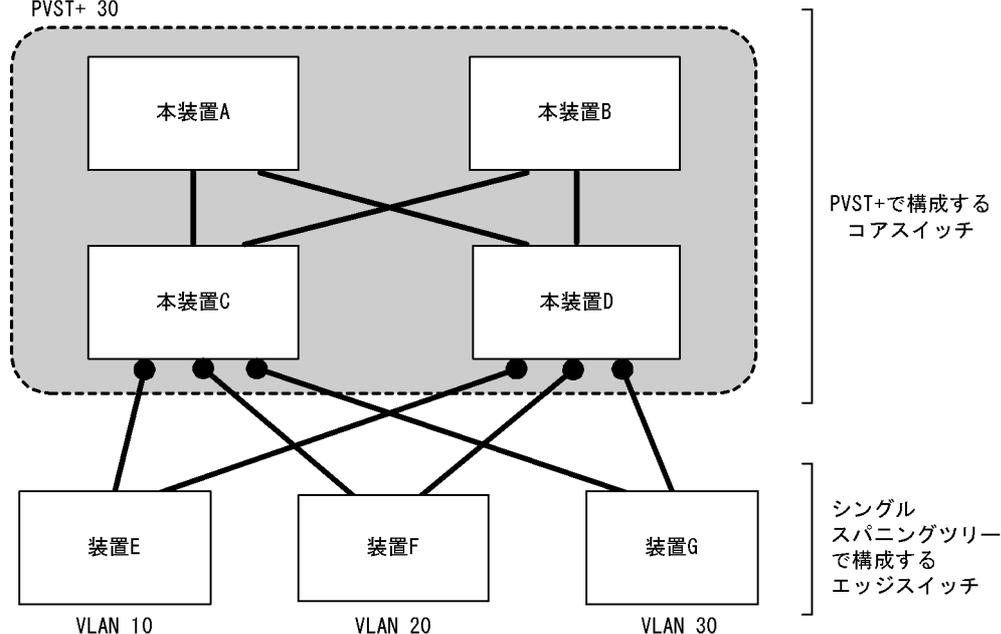
図 21-6 シングルスパニングツリーとの接続

全装置で以下を設定

PVST+ 10

PVST+ 20

PVST+ 30



装置Eで障害が発生した場合、コアスイッチ側をPVST+で動作させているため、装置F、装置Gにトポロジー変更通知が波及しません。

(凡例) ● : アクセスポート

### (2) アクセスポートでシングルスパニングツリーを混在させた場合

PVST+ とシングルスパニングツリーを混在して設定している場合、アクセスポートでは、シングルスパニングツリーは停止状態 (Disable) になります。

### 21.3.3 PVST+ 使用時の注意事項

#### (1) 他機能との共存

「17.3 レイヤ2スイッチ機能と他機能の共存について」を参照してください。

#### (2) VLAN 1 (デフォルト VLAN) の PVST+ とシングルスパニングツリーについて

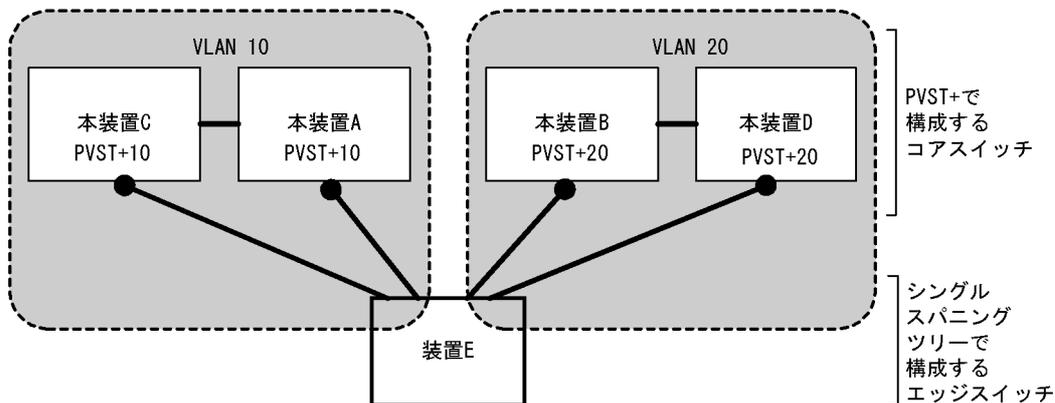
シングルスパニングツリーと VLAN 1 の PVST+ を同時に動作させることはできません。シングルスパニングツリーを動作させると VLAN 1 の PVST+ は停止します。

#### (3) 禁止構成

本装置とシングルスパニングツリーで動作する装置は、単一のスパニングツリーで構成してください。複数のスパニングツリーで構成すると正しいトポロジーになりません。

禁止構成の例を次の図に示します。この例では、装置 E のシングルスパニングツリーが複数の PVST+ スパニングツリーとトポロジーを構成しているため、正しいトポロジーになりません。

図 21-7 シングルスパニングツリーとの禁止構成例



(凡例) ● : アクセスポート

装置Eは単一のスパニングツリーで構成されていないため、正しいトポロジーになりません。

## 21.4 PVST+ のコンフィグレーション

### 21.4.1 コンフィグレーションコマンド一覧

PVST+ のコンフィグレーションコマンド一覧を次の表に示します。

表 21-9 コンフィグレーションコマンド一覧

| コマンド名                                 | 説明                                   |
|---------------------------------------|--------------------------------------|
| spanning-tree cost                    | ポートごとにパスコストのデフォルト値を設定します。            |
| spanning-tree pathcost method         | ポートごとにパスコストに使用する値の幅のデフォルト値を設定します。    |
| spanning-tree port-priority           | ポートごとにポート優先度のデフォルト値を設定します。           |
| spanning-tree vlan                    | PVST+ の動作, 停止を設定します。                 |
| spanning-tree vlan cost               | VLAN ごとにパスコスト値を設定します。                |
| spanning-tree vlan forward-time       | ポートの状態遷移に必要な時間を設定します。                |
| spanning-tree vlan hello-time         | BPDU の送信間隔を設定します。                    |
| spanning-tree vlan max-age            | 送信 BPDU の最大有効時間を設定します。               |
| spanning-tree vlan pathcost method    | VLAN ごとにパスコストに使用する値の幅を設定します。         |
| spanning-tree vlan port-priority      | VLAN ごとにポート優先度を設定します。                |
| spanning-tree vlan priority           | ブリッジ優先度を設定します。                       |
| spanning-tree vlan transmission-limit | hello-time 当たりに送信できる最大 BPDU 数を設定します。 |

### 21.4.2 PVST+ の設定

#### [ 設定のポイント ]

動作モード `pvst`, `rapid-pvst` を設定するとポート VLAN で自動的に PVST+ が動作しますが, VLAN ごとにモードの変更や PVST+ の動作, 停止を設定できます。停止する場合は, `no spanning-tree vlan` コマンドを使用します。

VLAN を作成するときその VLAN で PVST+ を動作させたくない場合, `no spanning-tree vlan` コマンドを VLAN 作成前にあらかじめ設定しておくことができます。

#### [ コマンドによる設定 ]

1. `(config)# no spanning-tree vlan 20`

VLAN 20 の PVST+ の動作を停止します。

2. `(config)# spanning-tree vlan 20`

停止した VLAN 20 の PVST+ を動作させます。

#### [ 注意事項 ]

- PVST+ はコンフィグレーションに表示がないときは自動的に動作しています。 `no spanning-tree vlan` コマンドで停止すると, 停止状態であることがコンフィグレーションで確認できます。
- PVST+ は最大 250 個のポート VLAN まで動作します。それ以上のポート VLAN を作成しても自動的に動作しません。

## 21.4.3 PVST+ のトポロジ－設定

### (1) ブリッジ優先度の設定

ブリッジ優先度は、ルートブリッジを決定するためのパラメータです。トポロジ－を設計する際に、ルートブリッジにしたい装置を最高の優先度に設定し、ルートブリッジに障害が発生したときのために、次にルートブリッジにしたい装置を2番目の優先度に設定します。

#### [ 設定のポイント ]

ブリッジ優先度は値が小さいほど高い優先度となり、最も小さい値を設定した装置がルートブリッジになります。ルートブリッジはブリッジ優先度と装置のMACアドレスから成るブリッジ識別子で判定するため、本パラメータを設定しない場合は装置のMACアドレスが最も小さい装置がルートブリッジになります。

#### [ コマンドによる設定 ]

1. (config)# spanning-tree vlan 10 priority 4096  
VLAN 10 の PVST+ のブリッジ優先度を 4096 に設定します。

### (2) パスコストの設定

パスコストは通信経路を決定するためのパラメータです。スパニングツリーのトポロジ－設計において、ブリッジ優先度決定後に、指定ブリッジのルートポート（指定ブリッジからルートブリッジへの通信経路）を本パラメータで設計します。

#### [ 設定のポイント ]

パスコスト値は指定ブリッジの各ポートに設定します。小さい値で設定することによってルートポートに選択されやすくなります。設定しない場合、ポートの速度ごとに異なるデフォルト値になり、高速なポートほどルートポートに選択されやすくなります。

パスコストは、速度の遅いポートを速いポートより優先して経路として使用したい場合に設定します。速いポートを優先したトポロジ－とする場合は設定する必要はありません。

パスコスト値には short ( 16bit 値 ), long ( 32bit 値 ) の 2 種類があり、トポロジ－の全体で合わせる必要があります。10 ギガビットイーサネットを使用する場合は long ( 32bit 値 ) を使用することをお勧めします。デフォルトでは short ( 16bit 値 ) で動作します。イーサネットインタフェースの速度による自動的な設定は、short ( 16bit 値 ) か long ( 32bit 値 ) かで設定内容が異なります。パスコストのデフォルト値を次の表に示します。

表 21-10 パスコストのデフォルト値

| ポートの速度    | パスコストのデフォルト値   |               |
|-----------|----------------|---------------|
|           | short(16bit 値) | long(32bit 値) |
| 10Mbit/s  | 100            | 2000000       |
| 100Mbit/s | 19             | 200000        |
| 1Gbit/s   | 4              | 20000         |
| 10Gbit/s  | 2              | 2000          |

#### [ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/1  
(config-if)# spanning-tree cost 100

```
(config-if)# exit
```

ポート 1/1 のパスコストを 100 に設定します。

2. (config)# spanning-tree pathcost method long  
(config)# interface gigabitethernet 1/1  
(config-if)# spanning-tree vlan 10 cost 200000  
long (32bit 値) のパスコストを使用するように設定した後に、ポート 1/1 の VLAN 10 をコスト値 200000 に変更します。ポート 1/1 では VLAN 10 だけパスコスト 200000 となり、そのほかの VLAN は 100 で動作します。

[ 注意事項 ]

リンクアグリゲーションを使用する場合、チャンネルグループのパスコストのデフォルト値は、チャンネルグループ内の全ポートの合計ではなく一つのポートの速度の値となります。リンクアグリゲーションの異速度混在モードを使用している場合は、最も遅いポートの速度の値となります。

### (3) ポート優先度の設定

ポート優先度は 2 台の装置間での接続をスパニングツリーで冗長化し、パスコストも同じ値とする場合に、どちらのポートを使用するかを決定するために設定します。

2 台の装置間の接続を冗長化する機能にはリンクアグリゲーションがあり、通常はリンクアグリゲーションを使用することをお勧めします。接続する対向の装置がリンクアグリゲーションをサポートしていなくスパニングツリーで冗長化する必要がある場合に本機能を使用してください。

[ 設定のポイント ]

ポート優先度は値が小さいほど高い優先度となります。2 台の装置間で冗長化している場合に、ルートブリッジに近い側の装置でポート優先度の高いポートが通信経路として使われます。本パラメータを設定しない場合はポート番号の小さいポートが優先されます。

[ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/1  
(config-if)# spanning-tree port-priority 64  
(config-if)# exit  
ポート 1/1 のポート優先度を 64 に設定します。
2. (config)# interface gigabitethernet 1/1  
(config-if)# spanning-tree vlan 10 port-priority 144  
ポート 1/1 の VLAN 10 をポート優先度 144 に変更します。ポート 1/1 では VLAN 10 だけポート優先度 144 となり、そのほかの VLAN は 64 で動作します。

## 21.4.4 PVST+ のパラメータ設定

各パラメータは「 $2 \times (\text{forward-time} - 1) \text{ max-age} \ 2 \times (\text{hello-time} + 1)$ 」という関係を満たすように設定する必要があります。パラメータを変える場合は、スパニングツリーを構築するすべての装置でパラメータを合わせる必要があります。

### (1) BPDU の送信間隔の設定

BPDU の送信間隔は、短くした場合はトポロジー変更を検知しやすくなります。長くした場合はトポロジー変更の検知までに時間が掛かるようになる一方で、BPDU トラフィックや本装置のスパニングツリープログラムの負荷を軽減できます。

[ 設定のポイント ]

設定しない場合、2 秒間隔で BPDU を送信します。通常は設定する必要はありません。

[ コマンドによる設定 ]

1. (config)# spanning-tree vlan 10 hello-time 3  
VLAN 10 の PVST+ の BPDU 送信間隔を 3 秒に設定します。

[ 注意事項 ]

BPDU の送信間隔を短くすると、トポロジー変更を検知しやすくなる一方で BPDU トラフィックが増加することによりスパニングツリープログラムの負荷が増加します。本パラメータをデフォルト値 (2 秒) より短くすることでタイムアウトのメッセージ出力やトポロジー変更が頻発する場合は、デフォルト値に戻して使用してください。

### (2) 送信する最大 BPDU 数の設定

スパニングツリーでは、CPU 負荷の増大を抑えるために、hello-time (BPDU 送信間隔) 当たりに送信する最大 BPDU 数を決めることができます。トポロジー変更が連続的に発生すると、トポロジー変更を通知、収束するために大量の BPDU が送信され、BPDU トラフィックの増加、CPU 負荷の増大につながります。送信する BPDU の最大数を制限することでこれらを抑えます。

[ 設定のポイント ]

設定しない場合、hello-time (BPDU 送信間隔) 当たりの最大 BPDU 数は 3 で動作します。本パラメータのコンフィグレーションは Rapid PVST+ だけ有効であり、PVST+ は 3 (固定) で動作します。通常は設定する必要はありません。

[ コマンドによる設定 ]

1. (config)# spanning-tree vlan 10 transmission-limit 5  
VLAN 10 の Rapid PVST+ の hello-time 当たりの最大送信 BPDU 数を 5 に設定します。

### (3) BPDU の最大有効時間の設定

ルートブリッジから送信する BPDU の最大有効時間を設定します。BPDU のカウンタは装置を経由するたびに増加し、最大有効時間を超えた BPDU は無効な BPDU となって無視されます。

[ 設定のポイント ]

最大有効時間を大きく設定することで、多くの装置に BPDU が届くようになります。設定しない場合、最大有効時間は 20 で動作します。

[ コマンドによる設定 ]

1. (config)# spanning-tree vlan 10 max-age 25  
VLAN 10 の PVST+ の BPDU の最大有効時間を 25 に設定します。

#### (4) 状態遷移時間の設定

PVST+ モードまたは Rapid PVST+ モードでタイマによる動作となる場合、ポートの状態が一定時間ごとに遷移します。PVST+ モードの場合は Blocking から Listening, Learning, Forwarding と遷移し、Rapid PVST+ モードの場合は Discarding から Learning, Forwarding と遷移します。この状態遷移に必要な時間を設定できます。小さい値を設定すると、より早く Forwarding 状態に遷移できます。

##### [ 設定のポイント ]

設定しない場合、状態遷移時間は 15 秒で動作します。本パラメータを短い時間に変更する場合、BPDU の最大有効時間 (max-age)、送信間隔 (hello-time) との関係が「 $2 \times (\text{forward-time} - 1) \times \text{max-age} \geq 2 \times (\text{hello-time} + 1)$ 」を満たすように設定してください。

##### [ コマンドによる設定 ]

1. (config)# `spanning-tree vlan 10 forward-time 10`  
VLAN 10 の PVST+ の状態遷移時間を 10 に設定します。

## 21.5 PVST+ のオペレーション

### 21.5.1 運用コマンド一覧

PVST+ の運用コマンド一覧を次の表に示します。

表 21-11 運用コマンド一覧

| コマンド名                                 | 説明                                                 |
|---------------------------------------|----------------------------------------------------|
| show spanning-tree                    | スパニングツリー情報を表示します。                                  |
| show spanning-tree statistics         | スパニングツリーの統計情報を表示します。                               |
| clear spanning-tree statistics        | スパニングツリーの統計情報をクリアします。                              |
| clear spanning-tree detected-protocol | スパニングツリーの STP 互換モードを強制回復します。                       |
| show spanning-tree port-count         | スパニングツリーの収容数を表示します。                                |
| restart spanning-tree                 | スパニングツリープログラムを再起動します。                              |
| dump protocols spanning-tree          | スパニングツリーで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。 |

### 21.5.2 PVST+ の状態の確認

PVST+ の情報は show spanning-tree コマンドの実行結果で示されます。Mode で PVST+ , Rapid PVST+ の動作モードを確認できます。トポロジが正しく構築されていることを確認するためには、Root Bridge ID の内容が正しいこと、Port Information の Status , Role が正しいことを確認してください。

図 21-8 show spanning-tree コマンドの実行結果

```
> show spanning-tree vlan 1
Date 2006/03/04 11:39:43 UTC
VLAN 1 PVST+ Spanning Tree:Enabled Mode:PVST+
 Bridge ID Priority:32769 MAC Address:0012.e205.0900
 Bridge Status:Designated
 Root Bridge ID Priority:32769 MAC Address:0012.e201.0900
 Root Cost:1000
 Root Port:1/1
 Port Information
 1/1 Up Status:Forwarding Role:Root
 1/2 Up Status:Forwarding Role:Designated
 1/3 Up Status:Blocking Role:Alternate
 1/4 Down Status:Disabled Role:-
 1/10 Up Status:Forwarding Role:Designated PortFast
 1/11 Up Status:Forwarding Role:Designated PortFast
 1/12 Up Status:Forwarding Role:Designated PortFast
>
```

## 21.6 シングルスパニングツリー解説

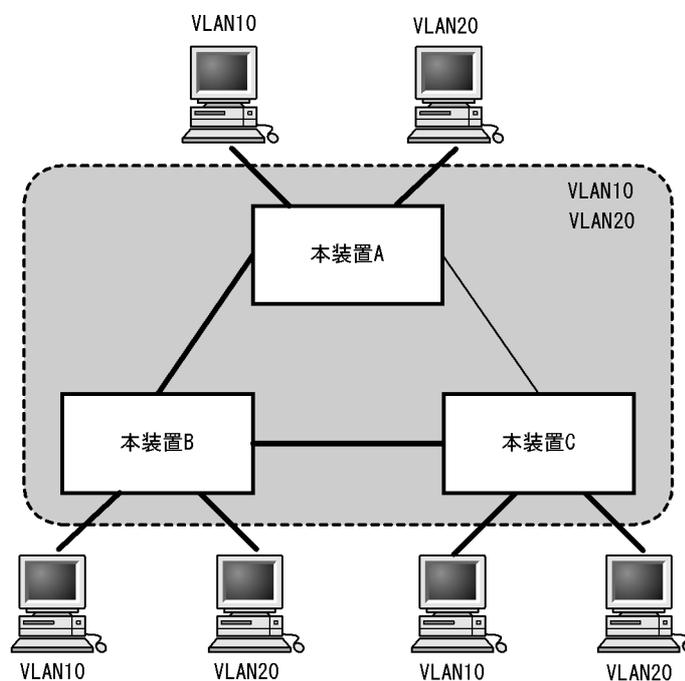
シングルスパニングツリーは装置全体を対象としたトポロジーを構築します。

### 21.6.1 概要

シングルスパニングツリーは、一つのスパニングツリーですべての VLAN のループを回避できます。VLAN ごとに制御する PVST+ よりも多くの VLAN を扱えます。

シングルスパニングツリーによるネットワーク構成を次の図に示します。この図では、本装置 A, B, C に対して、VLAN 10 および VLAN 20 を設定し、すべての VLAN で PVST+ を停止しシングルスパニングツリーを適用しています。すべての VLAN で一つのトポロジーを使用して通信します。

図 21-9 シングルスパニングツリーによるネットワーク構成



(凡例)

- : 通信する接続
- - - - : ループ検出接続

### 21.6.2 PVST+ との併用

プロトコル VLAN, MAC VLAN では PVST+ を使用できません。また、PVST+ が動作可能な VLAN 数は 250 個であり、それ以上の VLAN で使用することはできません。シングルスパニングツリーを使用することで、PVST+ を使用しながらこれらの VLAN にもスパニングツリーを適用できます。

シングルスパニングツリーは、PVST+ が動作していないすべての VLAN に対し適用します。次の表に、シングルスパニングツリーを PVST+ と併用したときにシングルスパニングツリーの対象になる VLAN を示します。

表 21-12 シングルスパニングツリー対象の VLAN

| 項目                   | VLAN                                                         |
|----------------------|--------------------------------------------------------------|
| PVST+ 対象の VLAN       | PVST+ が動作している VLAN。<br>最大 250 個のポート VLAN は自動的に PVST+ が動作します。 |
| シングルスパニングツリー対象の VLAN | 251 個目以上のポート VLAN。                                           |
|                      | PVST+ を停止 ( no spanning-tree vlan コマンドで指定 ) している VLAN。       |
|                      | デフォルト VLAN ( VLAN ID 1 のポート VLAN )。                          |
|                      | プロトコル VLAN。                                                  |
|                      | MAC VLAN。                                                    |

### 21.6.3 シングルスパニングツリー使用時の注意事項

#### (1) 他機能との共存

「17.3 レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

#### (2) VLAN 1 (デフォルト VLAN) の PVST+ とシングルスパニングツリーについて

シングルスパニングツリーと VLAN 1 の PVST+ を同時に動作させることはできません。シングルスパニングツリーを動作させると VLAN 1 の PVST+ は停止します。

## 21.7 シングルスパニングツリーのコンフィギュレーション

### 21.7.1 コンフィギュレーションコマンド一覧

シングルスパニングツリーのコンフィギュレーションコマンド一覧を次の表に示します。

表 21-13 コンフィギュレーションコマンド一覧

| コマンド名                                   | 説明                                   |
|-----------------------------------------|--------------------------------------|
| spanning-tree cost                      | ポートごとにパスコストのデフォルト値を設定します。            |
| spanning-tree pathcost method           | ポートごとにパスコストに使用する値の幅のデフォルト値を設定します。    |
| spanning-tree port-priority             | ポートごとにポート優先度のデフォルト値を設定します。           |
| spanning-tree single                    | シングルスパニングツリーの動作、停止を設定します。            |
| spanning-tree single cost               | シングルスパニングツリーのパスコストを設定します。            |
| spanning-tree single forward-time       | ポートの状態遷移に必要な時間を設定します。                |
| spanning-tree single hello-time         | BPDU の送信間隔を設定します。                    |
| spanning-tree single max-age            | 送信 BPDU の最大有効時間を設定します。               |
| spanning-tree single pathcost method    | シングルスパニングツリーのパスコストに使用する値の幅を設定します。    |
| spanning-tree single port-priority      | シングルスパニングツリーのポート優先度を設定します。           |
| spanning-tree single priority           | ブリッジ優先度を設定します。                       |
| spanning-tree single transmission-limit | hello-time 当たりに送信できる最大 BPDU 数を設定します。 |

### 21.7.2 シングルスパニングツリーの設定

#### [ 設定のポイント ]

シングルスパニングツリーの動作、停止を設定します。シングルスパニングツリーは、動作モード `pvst`、`rapid-pvst` を設定しただけでは動作しません。設定することによって動作を開始します。

VLAN 1 (デフォルト VLAN) とシングルスパニングツリーは同時に使用できません。シングルスパニングツリーを設定すると VLAN 1 の PVST+ は停止します。

#### [ コマンドによる設定 ]

##### 1. (config)# spanning-tree single

シングルスパニングツリーを動作させます。この設定によって、VLAN 1 の PVST+ が停止し、VLAN 1 はシングルスパニングツリーの対象となります。

##### 2. (config)# no spanning-tree single

シングルスパニングツリーを停止します。VLAN 1 の PVST+ を停止に設定していないで、かつすでに 250 個の PVST+ が動作している状態でない場合、VLAN 1 の PVST+ が自動的に動作を開始します。

### 21.7.3 シングルスパニングツリーのトポロジー設定

#### (1) ブリッジ優先度の設定

ブリッジ優先度は、ルートブリッジを決定するためのパラメータです。トポロジーを設計する際に、ルートブリッジにしたい装置を最高の優先度に設定し、ルートブリッジに障害が発生したときのために、次にルートブリッジにしたい装置を2番目の優先度に設定します。

##### [ 設定のポイント ]

ブリッジ優先度は値が小さいほど高い優先度となり、最も小さい値を設定した装置がルートブリッジになります。ルートブリッジはブリッジ優先度と装置のMACアドレスから成るブリッジ識別子で判定するため、本パラメータを設定しない場合は装置のMACアドレスが最も小さい装置がルートブリッジになります。

##### [ コマンドによる設定 ]

1. (config)# spanning-tree single priority 4096  
シングルスパニングツリーのブリッジ優先度を4096に設定します。

#### (2) パスコストの設定

パスコストは通信経路を決定するためのパラメータです。スパニングツリーのトポロジー設計において、ブリッジ優先度決定後に、指定ブリッジのルートポート（指定ブリッジからルートブリッジへの通信経路）を本パラメータで設計します。

##### [ 設定のポイント ]

パスコスト値は指定ブリッジの各ポートに設定します。小さい値で設定することによりルートポートに選択されやすくなります。設定しない場合、ポートの速度ごとに異なるデフォルト値になり、高速なポートほどルートポートに選択されやすくなります。

パスコストは、速度の遅いポートを速いポートより優先して経路として使用したい場合に設定します。速いポートを優先したトポロジーとする場合は設定する必要はありません。

パスコスト値には short (16bit 値)、long (32bit 値) の2種類があり、トポロジーの全体で合わせる必要があります。10ギガビットイーサネットを使用する場合は long (32bit 値) を使用することをお勧めします。デフォルトでは short (16bit 値) で動作します。イーサネットインタフェースの速度による自動的な設定は、short (16bit 値) か long (32bit 値) かで設定内容が異なります。パスコストのデフォルト値を次の表に示します。

表 21-14 パスコストのデフォルト値

| ポートの速度    | パスコストのデフォルト値   |               |
|-----------|----------------|---------------|
|           | short(16bit 値) | long(32bit 値) |
| 10Mbit/s  | 100            | 2000000       |
| 100Mbit/s | 19             | 200000        |
| 1Gbit/s   | 4              | 20000         |
| 10Gbit/s  | 2              | 2000          |

##### [ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/1  
(config-if)# spanning-tree cost 100  
(config-if)# exit

ポート 1/1 のパスコストを 100 に設定します。

2. (config)# spanning-tree pathcost method long  
 (config)# interface gigabitethernet 1/1  
 (config-if)# spanning-tree single cost 200000  
 long (32bit 値) のパスコストを使用するように設定した後に、シングルスパニングツリーのポート 1/1 のパスコストを 200000 に変更します。ポート 1/1 ではシングルスパニングツリーだけパスコスト 200000 となり、同じポートで使用している PVST+ は 100 で動作します。

#### [ 注意事項 ]

リンクアグリゲーションを使用する場合、チャンネルグループのパスコストのデフォルト値は、チャンネルグループ内の全ポートの合計ではなく一つのポートの速度の値になります。リンクアグリゲーションの異速度混在モードを使用している場合は、最も遅いポートの速度の値になります。

### (3) ポート優先度の設定

ポート優先度は 2 台の装置間での接続をスパニングツリーで冗長化し、パスコストも同じ値とする場合に、どちらのポートを使用するかを決定するために設定します。

2 台の装置間の接続を冗長化する機能にはリンクアグリゲーションがあり、通常はリンクアグリゲーションを使用することをお勧めします。接続する対向の装置がリンクアグリゲーションをサポートしていないで、スパニングツリーで冗長化する必要がある場合に本機能を使用してください。

#### [ 設定のポイント ]

ポート優先度は値が小さいほど高い優先度となります。2 台の装置間で冗長化している場合に、ルートブリッジに近い側の装置でポート優先度の高いポートが通信経路として使われます。本パラメータを設定しない場合はポート番号の小さいポートが優先されます。

#### [ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/1  
 (config-if)# spanning-tree port-priority 64  
 (config-if)# exit  
 ポート 1/1 のポート優先度を 64 に設定します。
2. (config)# interface gigabitethernet 1/1  
 (config-if)# spanning-tree single port-priority 144  
 シングルスパニングツリーのポート 1/1 のポート優先度を 144 に変更します。ポート 1/1 ではシングルスパニングツリーだけポート優先度 144 となり、同じポートで使用している PVST+ は 64 で動作します。

## 21.7.4 シングルスパニングツリーのパラメータ設定

各パラメータは「 $2 \times (\text{forward-time} - 1) \text{ max-age} \ 2 \times (\text{hello-time} + 1)$ 」という関係が成立するように設定する必要があります。パラメータを変える場合はトポロジ全体でパラメータを合わせる必要があります。

### (1) BPDU の送信間隔の設定

BPDU の送信間隔は、短くした場合はトポロジ変更を検知しやすくなります。長くした場合はトポロ

ジー変更の検知までに時間が掛かるようになる一方で、BPDU トラフィックや本装置のスパニングツリープログラムの負荷を軽減できます。

[ 設定のポイント ]

設定しない場合、2 秒間隔で BPDU を送信します。通常は設定する必要はありません。

[ コマンドによる設定 ]

1. (config)# spanning-tree single hello-time 3  
シングルスパニングツリーの BPDU 送信間隔を 3 秒に設定します。

[ 注意事項 ]

BPDU の送信間隔を短くすると、トポロジー変更を検知しやすくなる一方で BPDU トラフィックが増加することによりスパニングツリープログラムの負荷が増加します。本パラメータをデフォルト値 (2 秒) より短くすることによってタイムアウトのメッセージ出力やトポロジー変更が頻発する場合は、デフォルト値に戻して使用してください。

## (2) 送信する最大 BPDU 数の設定

スパニングツリーでは、CPU 負荷の増大を抑えるために、hello-time (BPDU 送信間隔) 当たりに送信する最大 BPDU 数を決めることができます。トポロジー変更が連続的に発生すると、トポロジー変更を通知、収束するために大量の BPDU が送信され、BPDU トラフィックの増加、CPU 負荷の増大につながります。送信する BPDU の最大数を制限することでこれらを抑えます。

[ 設定のポイント ]

設定しない場合、hello-time (BPDU 送信間隔) 当たりの最大 BPDU 数は 3 で動作します。本パラメータのコンフィギュレーションは Rapid STP だけ有効であり、STP は 3 (固定) で動作します。通常は設定する必要はありません。

[ コマンドによる設定 ]

1. (config)# spanning-tree single transmission-limit 5  
シングルスパニングツリーの hello-time 当たりの最大送信 BPDU 数を 5 に設定します。

## (3) BPDU の最大有効時間

ルートブリッジから送信する BPDU の最大有効時間を設定します。BPDU のカウンタは装置を経由するたびに増加し、最大有効時間を超えた BPDU は無効な BPDU となって無視されます。

[ 設定のポイント ]

最大有効時間を大きく設定することで、多くの装置に BPDU が届くようになります。設定しない場合、最大有効時間は 20 で動作します。

[ コマンドによる設定 ]

1. (config)# spanning-tree single max-age 25  
シングルスパニングツリーの BPDU の最大有効時間を 25 に設定します。

## (4) 状態遷移時間の設定

STP モードまたは Rapid STP モードでタイマによる動作となる場合、ポートの状態が一定時間ごとに遷

移します。STP モードの場合は Blocking から Listening , Learning , Forwarding と遷移し , Rapid STP モードの場合は Discarding から Learning , Forwarding と遷移します。この状態遷移に必要な時間を設定できます。小さい値を設定すると , より早く Forwarding 状態に遷移できます。

[ 設定のポイント ]

設定しない場合 , 状態遷移時間は 15 秒で動作します。本パラメータを短い時間に変更する場合 , BPDU の最大有効時間 ( max-age ) , 送信間隔 ( hello-time ) との関係が「 $2 \times (\text{forward-time} - 1)$   
 $\text{max-age} \quad 2 \times (\text{hello-time} + 1)$ 」を満たすように設定してください。

[ コマンドによる設定 ]

1. (config)# **spanning-tree single forward-time 10**  
シングルスパニングツリーの状態遷移時間を 10 に設定します。

## 21.8 シングルスパニングツリーのオペレーション

### 21.8.1 運用コマンド一覧

シングルスパニングツリーの運用コマンド一覧を次の表に示します。

表 21-15 運用コマンド一覧

| コマンド名                                 | 説明                                                 |
|---------------------------------------|----------------------------------------------------|
| show spanning-tree                    | スパニングツリー情報を表示します。                                  |
| show spanning-tree statistics         | スパニングツリーの統計情報を表示します。                               |
| clear spanning-tree statistics        | スパニングツリーの統計情報をクリアします。                              |
| clear spanning-tree detected-protocol | スパニングツリーの STP 互換モードを強制回復します。                       |
| show spanning-tree port-count         | スパニングツリーの収容数を表示します。                                |
| restart spanning-tree                 | スパニングツリープログラムを再起動します。                              |
| dump protocols spanning-tree          | スパニングツリーで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。 |

### 21.8.2 シングルスパニングツリーの状態の確認

シングルスパニングツリーの情報は show spanning-tree コマンドで確認してください。Mode で STP , Rapid STP の動作モードを確認できます。トポロジが正しく構築されていることを確認するためには、Root Bridge ID の内容が正しいこと、Port Information の Status , Role が正しいことを確認してください。

図 21-10 シングルスパニングツリーの情報

```
> show spanning-tree single
Date 2006/03/04 11:42:06 UTC
Single Spanning Tree:Enabled Mode:Rapid STP
 Bridge ID Priority:32768 MAC Address:0012.e205.0900
 Bridge Status:Designated
 Root Bridge ID Priority:32768 MAC Address:0012.e205.0900
 Root Cost:0
 Root Port:-
 Port Information
 1/1 Up Status:Forwarding Role:Root
 1/2 Up Status:Forwarding Role:Designated
 1/3 Up Status:Blocking Role:Alternate
 1/4 Down Status:Disabled Role:-
 1/10 Up Status:Forwarding Role:Designated PortFast
 1/11 Up Status:Forwarding Role:Designated PortFast
 1/12 Up Status:Forwarding Role:Designated PortFast
>
```

## 21.9 マルチプルスパニングツリー解説

---

### 21.9.1 概要

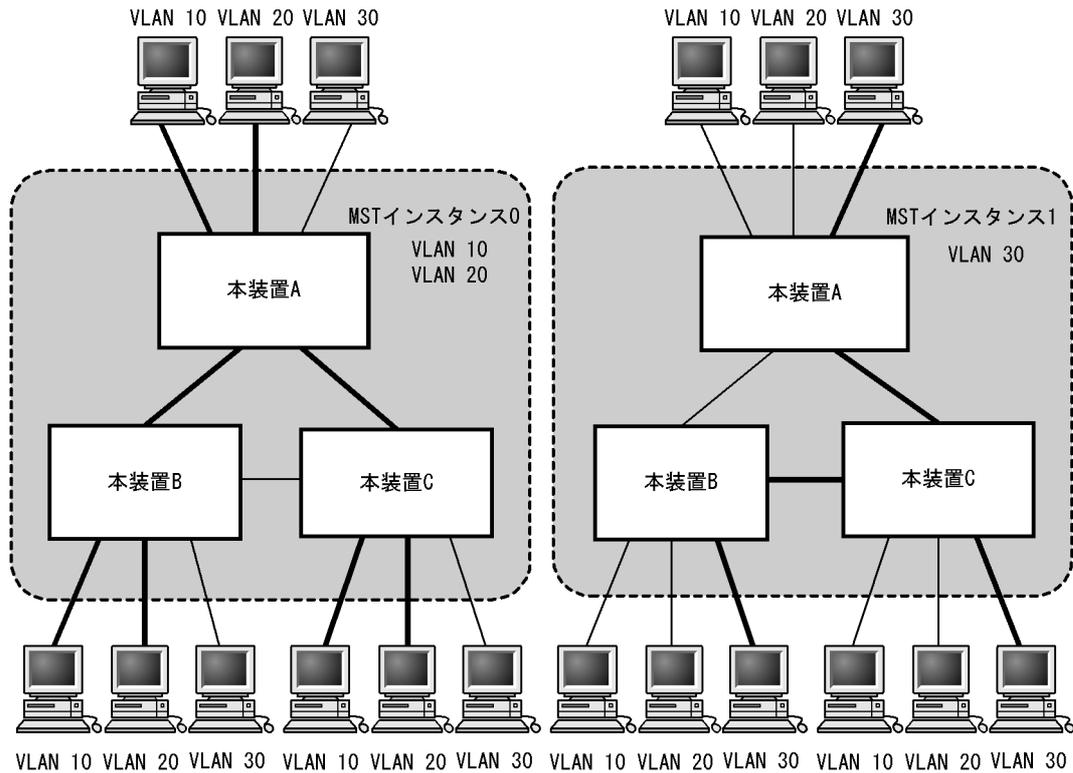
マルチプルスパニングツリーには、次の特長があります。MST インスタンスによってロードバランシングを可能にしています。また、MST リージョンによって、大規模なネットワーク構成を中小構成に分割することでネットワーク設計が容易になります。以降、これらを実現するためのマルチプルスパニングツリーの機能概要を説明します。

#### (1) MST インスタンス

マルチプルスパニングツリーは、複数の VLAN をまとめた MST インスタンス (MSTI : Multiple Spanning Tree Instance) というグループごとにスパニングツリーを構築でき、MST インスタンスごとにロードバランシングが可能です。PVST+ によるロードバランシングでは、VLAN 数分のツリーが必要でしたが、マルチプルスパニングツリーでは MST インスタンスによって、計画したロードバランシングに従ったツリーだけで済みます。その結果、PVST+ とは異なり VLAN 数の増加に比例した CPU 負荷およびネットワーク負荷の増加を抑えられます。本装置では最大 16 個の MST インスタンスが設定できます。

MST インスタンスイメージを次の図に示します。

図 21-11 MST インスタンスイメージ



ネットワーク上に、二つのインスタンスを定義して、ロードバランシングしています。  
 インスタンス0には、VLAN 10, 20を所属させ、インスタンス1には、VLAN 30を所属させています。

(凡例)

- : 通信する接続
- - - : ループ検出接続、および通信しない接続

## (2) MST リージョン

マルチプルスパニングツリーでは、複数の装置をグルーピングして MST リージョンとして扱えます。同一の MST リージョンに所属させるには、リージョン名、リージョン番号、MST インスタンス ID と VLAN の対応を同じにする必要があります。これらはコンフィグレーションで設定します。ツリーの構築は MST リージョン間と MST リージョン内で別々に行い、MST リージョン内のトポロジーは MST インスタンス単位に構築できます。

次に、MST リージョン間や MST リージョン内で動作するスパニングツリーについて説明します。

### CST

CST ( Common Spanning Tree ) は、MST リージョン間や、シングルスパニングツリーを使用しているブリッジ間の接続を制御するスパニングツリーです。このトポロジーはシングルスパニングツリーと同様に物理ポートごとに計算するのでロードバランシングすることはできません。

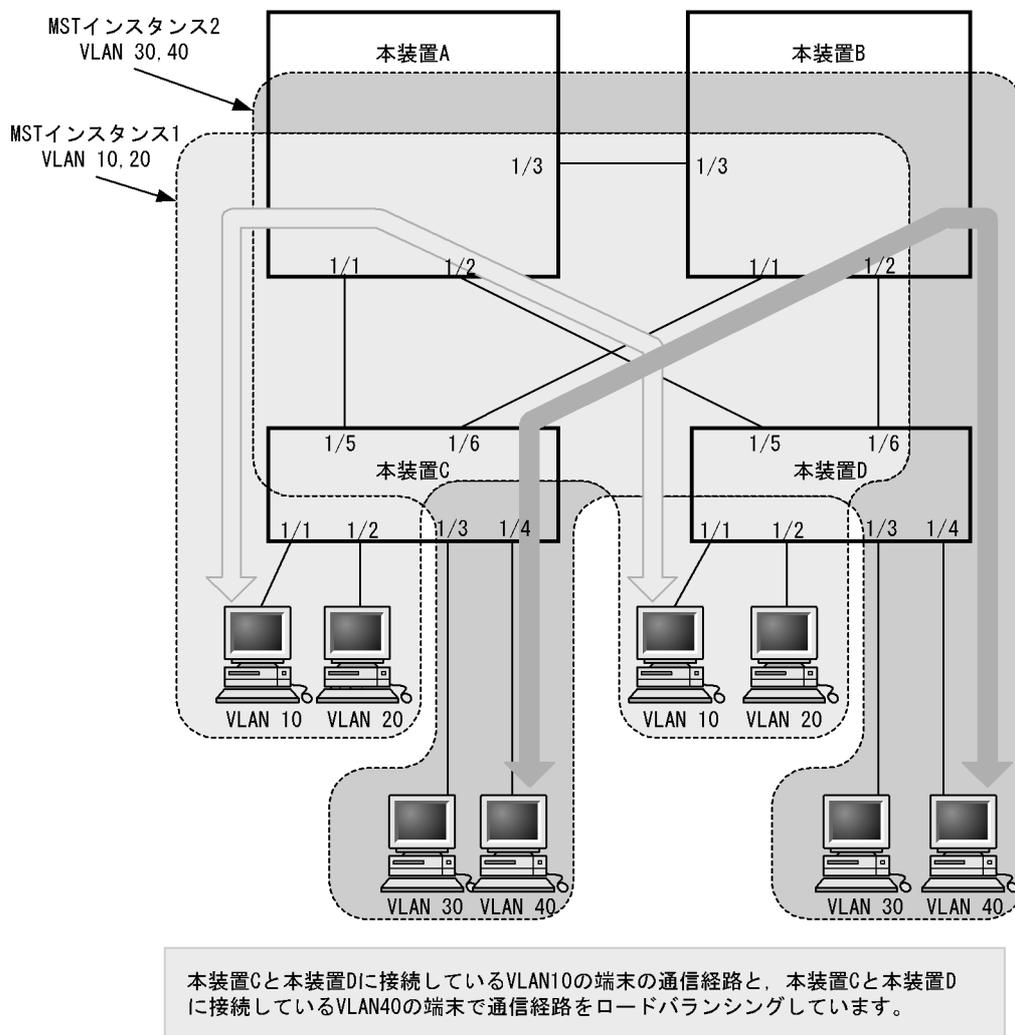
### IST

IST ( Internal Spanning Tree ) は、MST リージョン外と接続するために、MST リージョン内で Default 動作するトポロジーのことを指し、MST インスタンス ID0 が割り当てられます。MST リージョン外と接続しているポートを境界ポートと呼びます。また、リージョン内、リージョン間で MST



ンシング構成の例を次の図に示します。この例では、VLAN 10, 20 を MST インスタンス 1 に、VLAN 30, 40 を MST インスタンス 2 に設定して、二つのロードバランシングを行っています。マルチプルスパニングツリーでは、この例のように四つの VLAN であっても二つのツリーだけを管理することでロードバランシングができます。

図 21-13 マルチプルスパニングツリーのロードバランシング構成

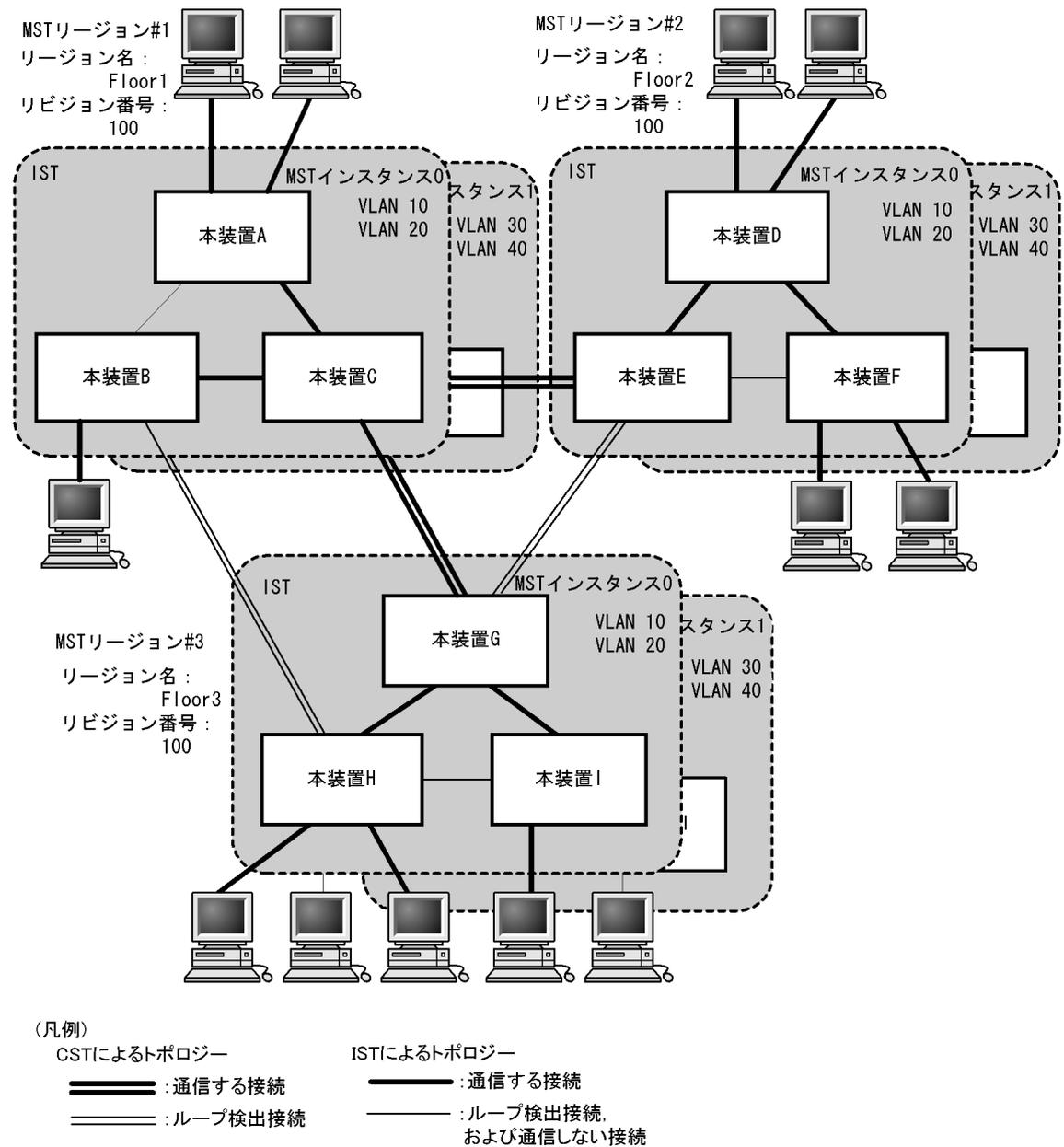


## (2) MST リージョンによるネットワーク設計

ネットワーク構成が大規模になるに従ってネットワーク設計は複雑になりますが、MST リージョンによって中小規模構成に分割することで、例えば、ロードバランシングを MST リージョン単位に実施できるため、ネットワーク設計が容易になります。

MST リージョンによるネットワーク設計例を次の図に示します。この例では、装置 A, B, C を MST リージョン #1, 装置 D, E, F を MST リージョン #2, 本装置 G, H, I を MST リージョン #3 に設定して、ネットワークを三つの MST リージョンに分割しています。

図 21-14 MST リージョンによるネットワーク構成



## 21.9.3 ほかのスパニングツリーとの互換性

### (1) シングルスパニングツリーとの互換性

マルチプルスパニングツリーは、シングルスパニングツリーで動作する STP, Rapid STP と互換性があります。これらと接続した場合、別の MST リージョンと判断し接続します。Rapid STP と接続した場合は高速な状態遷移を行います。

### (2) PVST+ との互換性

マルチプルスパニングツリーは、PVST+ と互換性はありません。ただし、PVST+ が動作している装置のアクセスポートはシングルスパニングツリーと同等の動作をするため、マルチプルスパニングツリーと接

続きます。

## 21.9.4 マルチプルスパニングツリー使用時の注意事項

### (1) 他機能との共存

「17.3 レイヤ2スイッチ機能と他機能の共存について」を参照してください。

### (2) MST リージョンについて

本装置と他装置で扱える VLAN の範囲が異なることがあります。そのような装置を同じ MST リージョンとして扱いたい場合は、該当 VLAN を MST インスタンス 0 に所属させてください。

### (3) トポロジーの収束に時間が掛かる場合について

CIST のルートブリッジまたは MST インスタンスのルートブリッジで、次の表に示すイベントが発生すると、トポロジーが落ち着くまでに時間が掛かる場合があります。その間、通信が途絶えたり、MAC アドレステーブルのクリアが発生したりします。

表 21-16 ルートブリッジでのイベント発生

| イベント                         | 内容                                                                                                                                                                                                      | イベントの発生したルートブリッジ種別           | 影響トポロジー       |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|---------------|
| コンフィグレーション変更                 | リージョン名 (1)、リビジョン番号 (2)、またはインスタンス番号と VLAN の対応 (3) をコンフィグレーションで変更し、リージョンを分割または同じにする場合<br>(1) MST コンフィグレーションモードの name コマンド<br>(2) MST コンフィグレーションモードの revision コマンド<br>(3) MST コンフィグレーションモードの instance コマンド | CIST のルートブリッジ                | CIST          |
|                              |                                                                                                                                                                                                         | MST インスタンス 0 (IST) でのルートブリッジ | CIST          |
|                              |                                                                                                                                                                                                         | MST インスタンス 1 以降でのルートブリッジ     | 当該 MST インスタンス |
|                              | ブリッジ優先度を spanning-tree mst root priority コマンドで下げた (現状より大きな値を設定した) 場合                                                                                                                                    | CIST のルートブリッジ                | CIST          |
|                              |                                                                                                                                                                                                         | MST インスタンス 1 以降でのルートブリッジ     | 当該 MST インスタンス |
|                              |                                                                                                                                                                                                         |                              |               |
| その他                          | 本装置が停止した場合                                                                                                                                                                                              | CIST のルートブリッジ                | CIST          |
|                              |                                                                                                                                                                                                         | MST インスタンス 0 (IST) でのルートブリッジ | CIST          |
|                              |                                                                                                                                                                                                         | MST インスタンス 1 以降でのルートブリッジ     | 当該 MST インスタンス |
|                              |                                                                                                                                                                                                         |                              |               |
|                              | 本装置と接続している対向装置で、ループ構成となっている本装置の全ポートがダウンした場合 (本装置が当該ループ構成上ルートブリッジではなくなった場合)                                                                                                                              | CIST のルートブリッジ                | CIST          |
| MST インスタンス 0 (IST) でのルートブリッジ |                                                                                                                                                                                                         | CIST                         |               |

| イベント | 内容 | イベントの発生したルートブリッジ種別       | 影響トポロジー       |
|------|----|--------------------------|---------------|
|      |    | MST インスタンス 1 以降でのルートブリッジ | 当該 MST インスタンス |

## 21.10 マルチプルスパニングツリーのコンフィグレーション

### 21.10.1 コンフィグレーションコマンド一覧

マルチプルスパニングツリーのコンフィグレーションコマンド一覧を次の表に示します。

表 21-17 コンフィグレーションコマンド一覧

| コマンド名                                | 説明                                          |
|--------------------------------------|---------------------------------------------|
| instance                             | マルチプルスパニングツリーの MST インスタンスに所属する VLAN を設定します。 |
| name                                 | マルチプルスパニングツリーのリージョンを識別するための文字列を設定します。       |
| revision                             | マルチプルスパニングツリーのリージョンを識別するためのリビジョン番号を設定します。   |
| spanning-tree cost                   | ポートごとにパスコストのデフォルト値を設定します。                   |
| spanning-tree mode                   | スパニングツリー機能の動作モードを設定します。                     |
| spanning-tree mst configuration      | マルチプルスパニングツリーの MST リージョンの形成に必要な情報を設定します。    |
| spanning-tree mst cost               | マルチプルスパニングツリーの MST インスタンスごとのパスコストを設定します。    |
| spanning-tree mst forward-time       | ポートの状態遷移に必要な時間を設定します。                       |
| spanning-tree mst hello-time         | BPDU の送信間隔を設定します。                           |
| spanning-tree mst max-age            | 送信 BPDU の最大有効時間を設定します。                      |
| spanning-tree mst max-hops           | MST リージョン内での最大ホップ数を設定します。                   |
| spanning-tree mst port-priority      | マルチプルスパニングツリーの MST インスタンスごとのポート優先度を設定します。   |
| spanning-tree mst root priority      | MST インスタンスごとのブリッジ優先度を設定します。                 |
| spanning-tree mst transmission-limit | hello-time 当たりに送信できる最大 BPDU 数を設定します。        |
| spanning-tree port-priority          | ポートごとにポート優先度のデフォルト値を設定します。                  |

### 21.10.2 マルチプルスパニングツリーの設定

#### (1) マルチプルスパニングツリーの設定

##### [ 設定のポイント ]

スパニングツリーの動作モードをマルチプルスパニングツリーに設定すると、PVST+、シングルスパニングツリーはすべて停止し、マルチプルスパニングツリーの動作を開始します。

##### [ コマンドによる設定 ]

##### 1. (config)# spanning-tree mode mst

マルチプルスパニングツリーを使用するように設定し、CIST が動作を開始します。

##### [ 注意事項 ]

no spanning-tree mode コマンドでマルチプルスパニングツリーの動作モード設定を削除すると、デ

フォルトの動作モードである pvst になります。その際、ポート VLAN で自動的に PVST+ が動作を開始します。

## (2) リージョン、インスタンスの設定

### [ 設定のポイント ]

MST リージョンは、同じリージョンに所属させたい装置はリージョン名、リビジョン番号、MST インスタンスのすべてを同じ設定にする必要があります。

MST インスタンスは、インスタンス番号と所属する VLAN を同時に設定します。リージョンを一致させるために、本装置に未設定の VLAN ID もインスタンスに所属させることができます。インスタンスに所属することを指定しない VLAN は自動的に CIST (インスタンス 0) に所属します。

MST インスタンスは、CIST (インスタンス 0) を含め 16 個まで設定できます。

### [ コマンドによる設定 ]

#### 1. (config)# spanning-tree mst configuration

```
(config-mst)# name "REGION TOKYO"
```

```
(config-mst)# revision 1
```

マルチプルスパニングツリーコンフィギュレーションモードに移り、name (リージョン名)、revision (リビジョン番号) の設定を行います。

#### 2. (config-mst)# instance 10 vlans 100-150

```
(config-mst)# instance 20 vlans 200-250
```

```
(config-mst)# instance 30 vlans 300-350
```

インスタンス 10、20、30 を設定し、各インスタンスに所属する VLAN を設定します。インスタンス 10 に VLAN 100 ~ 150、インスタンス 20 に VLAN 200 ~ 250、インスタンス 30 に VLAN 300 ~ 350 を設定します。指定していないそのほかの VLAN は CIST (インスタンス 0) に所属します。

## 21.10.3 マルチプルスパニングツリーのトポロジー設定

### (1) インスタンスごとのブリッジ優先度の設定

ブリッジ優先度は、ルートブリッジを決定するためのパラメータです。トポロジーを設計する際に、ルートブリッジにしたい装置を最高の優先度に設定し、ルートブリッジに障害が発生したときのために、次にルートブリッジにしたい装置を 2 番目の優先度に設定します。

### [ 設定のポイント ]

ブリッジ優先度は値が小さいほど高い優先度になり、最も小さい値を設定した装置がルートブリッジになります。ルートブリッジはブリッジ優先度と装置の MAC アドレスから成るブリッジ識別子で決定するため、本パラメータを設定しない場合は装置の MAC アドレスが最も小さい装置がルートブリッジになります。

マルチプルスパニングツリーのブリッジ優先度はインスタンスごとに設定します。インスタンスごとに値を変えた場合、インスタンスごとのロードバランシング (異なるトポロジーの構築) ができます。

### [ コマンドによる設定 ]

#### 1. (config)# spanning-tree mst 0 root priority 4096

```
(config)# spanning-tree mst 20 root priority 61440
```

CIST (インスタンス 0) のブリッジ優先度を 4096 に、インスタンス 20 のブリッジ優先度を 61440 に設定します。

## (2) インスタンスごとのパスコストの設定

パスコストは通信経路を決定するためのパラメータです。スパニングツリーのトポロジー設計において、ブリッジ優先度決定後に、指定ブリッジのルートポート（指定ブリッジからルートブリッジへの通信経路）を本パラメータで設計します。

### [ 設定のポイント ]

パスコスト値は指定ブリッジの各ポートに設定します。小さい値で設定することによってルートポートに選択されやすくなります。設定しない場合、ポートの速度ごとに異なるデフォルト値になり、高速なポートほどルートポートに選択されやすくなります。

パスコストは、速度の遅いポートを速いポートより優先して経路として使用したい場合に設定します。速いポートを優先したトポロジーとする場合は設定する必要はありません。パスコストのデフォルト値を次の表に示します。

表 21-18 パスコストのデフォルト値

| ポートの速度    | パスコストのデフォルト値 |
|-----------|--------------|
| 10Mbit/s  | 2000000      |
| 100Mbit/s | 200000       |
| 1Gbit/s   | 20000        |
| 10Gbit/s  | 2000         |

### [ コマンドによる設定 ]

#### 1. (config)# spanning-tree mst configuration

```
(config-mst)# instance 10 vlans 100-150
(config-mst)# instance 20 vlans 200-250
(config-mst)# instance 30 vlans 300-350
(config-mst)# exit
```

```
(config)# interface gigabitethernet 1/1
(config-if)# spanning-tree cost 2000
```

MST インスタンス 10, 20, 30 を設定し、ポート 1/1 のパスコストを 2000 に設定します。CIST (インスタンス 0), MST インスタンス 10, 20, 30 のポート 1/1 のパスコストは 2000 になります。

#### 2. (config-if)# spanning-tree mst 20 cost 500

MST インスタンス 20 のポート 1/1 のパスコストを 500 に変更します。インスタンス 20 以外は 2000 で動作します。

### [ 注意事項 ]

リンクアグリゲーションを使用する場合、チャンネルグループのパスコストのデフォルト値は、チャンネルグループ内の全ポートの合計ではなく、一つのポートの速度の値となります。リンクアグリゲーションの異速度混在モードを使用している場合は、最も遅いポートの速度の値となります。

## (3) インスタンスごとのポート優先度の設定

ポート優先度は 2 台の装置間での接続をスパニングツリーで冗長化し、パスコストも同じ値とする場合に、どちらのポートを使用するかを決定するために設定します。

2 台の装置間の接続を冗長化する機能にはリンクアグリゲーションがあり、通常はリンクアグリゲーション

ンを使用することをお勧めします。接続する対向の装置がリンクアグリゲーションをサポートしていなく  
スパニングツリーで冗長化する必要がある場合に本機能を使用してください。

[ 設定のポイント ]

ポート優先度は値が小さいほど高い優先度となります。2 台の装置間で冗長化している場合に、ルー  
トブリッジに近い側の装置でポート優先度の高いポートが通信経路として使われます。本パラメータ  
を設定しない場合はポート番号の小さいポートが優先されます。

[ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/1  
(config-if)# spanning-tree port-priority 64  
(config-if)# exit  
ポート 1/1 のポート優先度を 64 に設定します。
  
2. (config)# interface gigabitethernet 1/1  
(config-if)# spanning-tree mst 20 port-priority 144  
インスタンス 20 のポート 1/1 にポート優先度 144 を設定します。ポート 1/1 ではインスタンス 20 だ  
けポート優先度 144 となり、そのほかのインスタンスは 64 で動作します。

## 21.10.4 マルチプルスパニングツリーのパラメータ設定

各パラメータは「 $2 \times (\text{forward-time} - 1) \text{ max-age} \ 2 \times (\text{hello-time} + 1)$ 」という関係が成立するよ  
うに設定する必要があります。パラメータを変える場合はトポロジー全体でパラメータを合わせる必要が  
あります。

### (1) BPDU の送信間隔の設定

BPDU の送信間隔は、短くした場合はトポロジー変更を検知しやすくなります。長くした場合はトポロ  
ジー変更の検知までに時間が掛かるようになる一方で、BPDU トラフィックや本装置のスパニングツリー  
プログラムの負荷を軽減できます。

[ 設定のポイント ]

設定しない場合、2 秒間隔で BPDU を送信します。通常は設定する必要はありません。

[ コマンドによる設定 ]

1. (config)# spanning-tree mst hello-time 3  
マルチプルスパニングツリーの BPDU 送信間隔を 3 秒に設定します。

[ 注意事項 ]

BPDU の送信間隔を短くすると、トポロジー変更を検知しやすくなる一方で BPDU トラフィックが  
増加することによりスパニングツリープログラムの負荷が増加します。本パラメータをデフォルト値  
(2 秒) より短くすることによってタイムアウトのメッセージ出力やトポロジー変更が頻発する場合  
は、デフォルト値に戻して使用してください。

### (2) 送信する最大 BPDU 数の設定

スパニングツリーでは、CPU 負荷の増大を抑えるために、hello-time (BPDU 送信間隔) 当たりに送信す  
る最大 BPDU 数を決めることができます。トポロジー変更が連続的に発生すると、トポロジー変更を通

知、収束するために大量の BPDU が送信され、BPDU トラフィックの増加、CPU 負荷の増大につながります。送信する BPDU の最大数を制限することによりこれらを抑えます。

[ 設定のポイント ]

設定しない場合、hello-time (BPDU 送信間隔) 当たりの最大 BPDU 数は 3 で動作します。通常は設定する必要はありません。

[ コマンドによる設定 ]

1. (config)# spanning-tree mst transmission-limit 5

マルチプルスパニングツリーの hello-time 当たりの最大送信 BPDU 数を 5 に設定します。

### (3) 最大ホップ数の設定

ルートブリッジから送信する BPDU の最大ホップ数を設定します。BPDU のカウンタは装置を経由するたびに増加し、最大ホップ数を超えた BPDU は無効な BPDU となって無視されます。

シングルスパニングツリーの装置と接続しているポートは、最大ホップ数 (max-hops) ではなく最大有効時間 (max-age) のパラメータを使用します。ホップ数のカウントはマルチプルスパニングツリーの装置間で有効なパラメータです。

[ 設定のポイント ]

最大ホップ数を大きく設定することによって、多くの装置に BPDU が届くようになります。設定しない場合、最大ホップ数は 20 で動作します。

[ コマンドによる設定 ]

1. (config)# spanning-tree mst max-hops 10

マルチプルスパニングツリーの BPDU の最大ホップ数を 10 に設定します。

### (4) BPDU の最大有効時間の設定

マルチプルスパニングツリーでは、最大有効時間 (max-age) はシングルスパニングツリーの装置と接続しているポートでだけ有効なパラメータです。トポロジー全体をマルチプルスパニングツリーが動作している装置で構成する場合は設定する必要はありません。

最大有効時間は、ルートブリッジから送信する BPDU の最大有効時間を設定します。BPDU のカウンタは装置を経由するたびに増加して、最大有効時間を超えた BPDU は無効な BPDU となって無視されます。

[ 設定のポイント ]

最大有効時間を大きく設定することで、多くの装置に BPDU が届くようになります。設定しない場合、最大有効時間は 20 で動作します。

[ コマンドによる設定 ]

1. (config)# spanning-tree mst max-age 25

マルチプルスパニングツリーの BPDU の最大有効時間を 25 に設定します。

### (5) 状態遷移時間の設定

タイマによる動作となる場合、ポートの状態が Discarding から Learning, Forwarding へ一定時間ごとに遷移します。この状態遷移に必要な時間を設定できます。小さい値を設定すると、より早く

Forwarding 状態に遷移できます。

[ 設定のポイント ]

設定しない場合、状態遷移時間は 15 秒で動作します。本パラメータを短い時間に変更する場合、BPDU の最大有効時間 ( max-age )、送信間隔 ( hello-time ) との関係が「 $2 \times (\text{forward-time} - 1) \times \text{max-age} \geq 2 \times (\text{hello-time} + 1)$ 」を満たすように設定してください。

[ コマンドによる設定 ]

1. (config)# **spanning-tree mst forward-time 10**

マルチプルスパニングツリーの BPDU の最大有効時間を 10 に設定します。

## 21.11 マルチプルスパニングツリーのオペレーション

### 21.11.1 運用コマンド一覧

マルチプルスパニングツリーの運用コマンド一覧を次の表に示します。

表 21-19 運用コマンド一覧

| コマンド名                                 | 説明                                                 |
|---------------------------------------|----------------------------------------------------|
| show spanning-tree                    | スパニングツリー情報を表示します。                                  |
| show spanning-tree statistics         | スパニングツリーの統計情報を表示します。                               |
| clear spanning-tree statistics        | スパニングツリーの統計情報をクリアします。                              |
| clear spanning-tree detected-protocol | スパニングツリーの STP 互換モードを強制回復します。                       |
| show spanning-tree port-count         | スパニングツリーの収容数を表示します。                                |
| restart spanning-tree                 | スパニングツリープログラムを再起動します。                              |
| dump protocols spanning-tree          | スパニングツリーで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。 |

### 21.11.2 マルチプルスパニングツリーの状態の確認

マルチプルスパニングツリーの情報は show spanning-tree コマンドで確認してください。トポロジーが正しく構築されていることを確認するためには、次の項目を確認してください。

- リージョンの設定 ( Revision Level , Configuration Name , MST Instance の VLAN Mapped ) が正しいこと
- Regional Root の内容が正しいこと
- Port Information の Status , Role が正しいこと

show spanning-tree コマンドの実行結果を次の図に示します。

図 21-15 show spanning-tree コマンドの実行結果

```
> show spanning-tree mst instance 10
Date 2006/03/04 11:41:03 UTC
Multiple Spanning Tree: Enabled
Revision Level: 65535 Configuration Name: MSTP001
MST Instance 10
VLAN Mapped: 100-150
Regional Root Priority: 32778 MAC : 0012.e207.7200
Internal Root Cost : 2000 Root Port: 1/1
Bridge ID Priority: 32778 MAC : 0012.e205.0900
Regional Bridge Status : Designated
Port Information
 1/1 Up Status:Forwarding Role:Root
 1/2 Up Status:Discarding Role:Backup
 1/3 Up Status:Discarding Role:Alternate
 1/4 Up Status:Forwarding Role:Designated
>
```

## 21.12 スパニングツリー共通機能解説

---

### 21.12.1 PortFast

#### (1) 概要

PortFast は、端末が接続されループが発生しないことがあらかじめわかっているポートのための機能です。PortFast はスパニングツリーのトポロジー計算対象外となり、リンクアップ後すぐに通信できる状態になります。

#### (2) PortFast 適用時の BPDU 受信

PortFast を設定したポートは BPDU を受信しないことを想定したポートですが、もし、PortFast を設定したポートで BPDU を受信した場合は、その先にスイッチが存在しループの可能性があることとなります。そのため、PortFast 機能を停止し、トポロジー計算や BPDU の送受信など、通常のスパニングツリー対象のポートとしての動作を開始します。

いったんスパニングツリー対象のポートとして動作を開始した後、リンクのダウン/アップによって再び PortFast 機能が有効になります。

なお、BPDU を受信したときに PortFast 機能を停止しないようにする場合は、BPDU フィルタ機能を併用してください。

#### (3) PortFast 適用時の BPDU 送信

PortFast を設定したポートではスパニングツリーを動作させないため、BPDU の送信は行いません。

ただし、PortFast を設定したポート同士を誤って接続した状態を検出するために、PortFast 機能によって即時に通信可状態になった時点から 10 フレームだけ BPDU の送信を行います。

#### (4) BPDU ガード

PortFast に適用する機能として、BPDU ガード機能があります。BPDU ガード機能を適用したポートでは、BPDU 受信時に、スパニングツリー対象のポートとして動作するのではなくポートを inactive 状態にします。

inactive 状態にしたポートを activate コマンドで解放することによって、再び BPDU ガード機能を適用した PortFast としてリンクアップして通信を開始します。

### 21.12.2 BPDU フィルタ

#### (1) 概要

BPDU フィルタ機能を適用したポートでは、BPDU の送受信を停止します。BPDU フィルタ機能は、端末が接続されループが発生しないことがあらかじめわかっている、PortFast を設定したポートに適用します。

#### (2) BPDU フィルタに関する注意事項

PortFast を適用したポート以外に BPDU フィルタ機能を設定した場合、BPDU の送受信を停止するため、タイムによるポートの状態遷移が終了するまで通信断になります。

### 21.12.3 ループガード

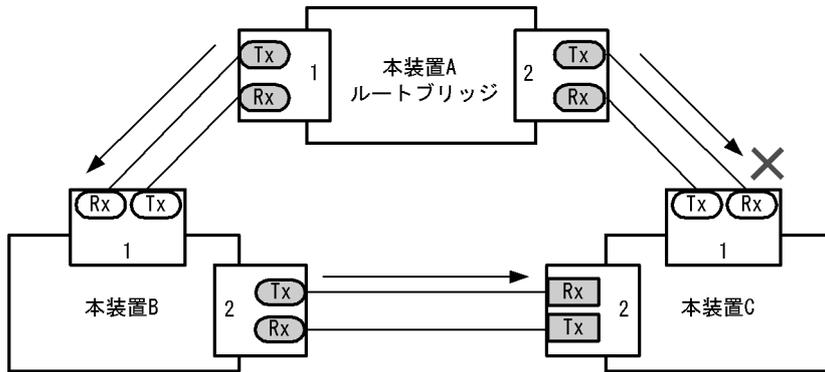
#### (1) 概要

片線切れなどの単一方向のリンク障害が発生し、BPDU の受信が途絶えた場合、ループが発生することがあります。ループガード機能は、このような場合にループの発生を防止する機能です。

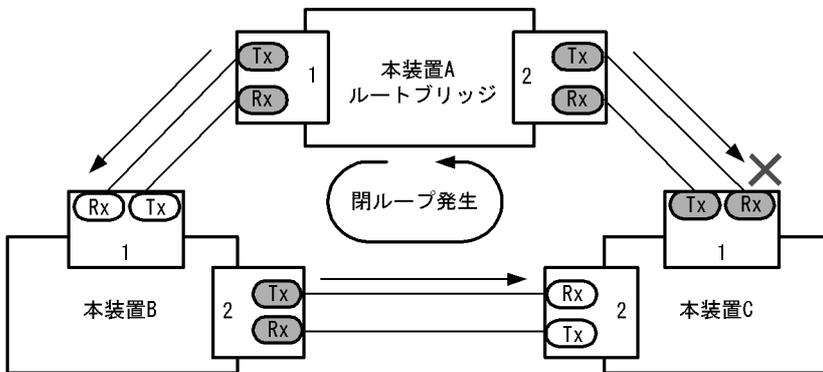
次の図に単一方向のリンク障害時の問題点を示します。

図 21-16 単一方向のリンク障害時の問題点

- (1) 本装置Cのポート1の片リンク故障で、BPDUの受信が途絶えるとルートポートがポート2に切り替わります。



- (2) 本装置Cのポート1は指定ポートとなっており、通信可状態を維持するため閉ループが発生します。



(凡例) ○ : ルートポート   ● : 指定ポート   ■ : 非指定ポート

ループガード機能とは BPDU の受信が途絶えたポートの状態を、再度 BPDU を受信するまで転送不可状態に移転させる機能です。BPDU 受信を開始した場合は通常のスパニングツリー対象のポートとしての動作を開始します。

ループガード機能は、端末を接続するポートを指定する機能である PortFast を設定したポート、またはループガード機能を設定したポートには設定できません。

#### (2) ループガードに関する注意事項

ループガードはマルチプルスパニングツリーでは使用できません。

ループガード機能を設定したあと、次に示すイベントが発生すると、ループガードが動作してポートをブロックします。その後、BPDUを受信するまで、ループガードは解除されません。

- 装置起動
- 系切替
- ポートのアップ（リンクアグリゲーションのアップも含む）
- スパニングツリープログラムの再起動
- スパニングツリープロトコルの種別変更（STP/高速STP、PVST+/高速PVST+）

なお、ループガード機能は、指定ポートだけでなく対向装置にも設定してください。指定ポートだけに設定すると、上記のイベントが発生しても、指定ポートはBPDUを受信しないことがあります。このような場合、ループガードの解除に時間が掛かります。ループガードを解除するには、対向装置のポートでBPDU受信タイムアウトを検出したあとのBPDUの送信を待つ必要があるためです。

また、両ポートにループガードを設定した場合でも、指定ポートでBPDUを一度も受信せずに、ループガードの解除に時間が掛かることがあります。具体的には、対向ポートが指定ポートとなるようにブリッジやポートの優先度、パスコストを変更した場合です。対向ポートでBPDUタイムアウトを検出し、ループガードが動作します。このポートが指定ポートになった場合、BPDUを受信しないことがあり、ループガードの解除に時間が掛かることがあります。

運用中にループガード機能を設定した場合、その時点では、ループガードは動作しません。運用中に設定したループガードは、BPDUの受信タイムアウトが発生した時に動作します。

本装置と対向装置のポート間にBPDUを中継しない装置が存在し、かつポートの両端にループガード機能を設定した状態でポートがリンクアップした場合、両端のポートはループガードが動作したままになります。復旧するには、ポート間に存在する装置のBPDU中継機能を有効にし、再度ポートをリンクアップさせる必要があります。

## 21.12.4 ルートガード

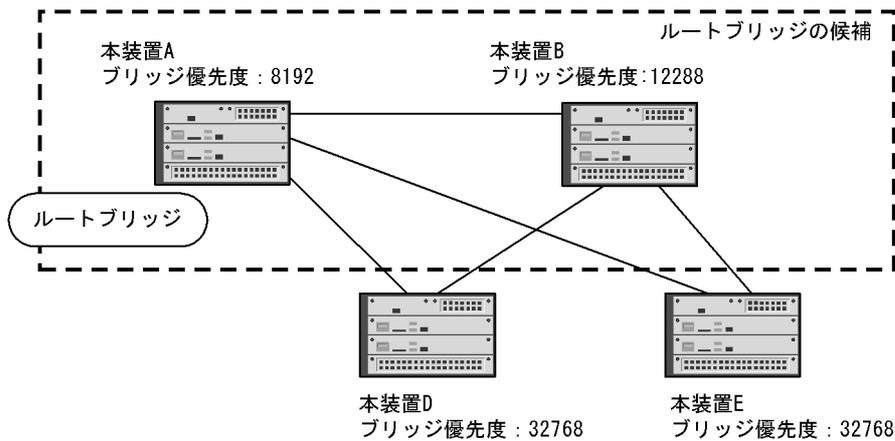
### (1) 概要

ネットワークの管理の届かない個所で誤って装置が接続された場合や設定が変更された場合、意図しないトポロジーになることがあります。意図しないトポロジーのルートブリッジの性能が低い場合、トラフィックが集中するとネットワーク障害のおそれがあります。ルートガード機能は、このようなときのためにルートブリッジの候補を特定しておくことによって、ネットワーク障害を回避する機能です。

誤って装置が接続されたときの問題点を次の図に示します。

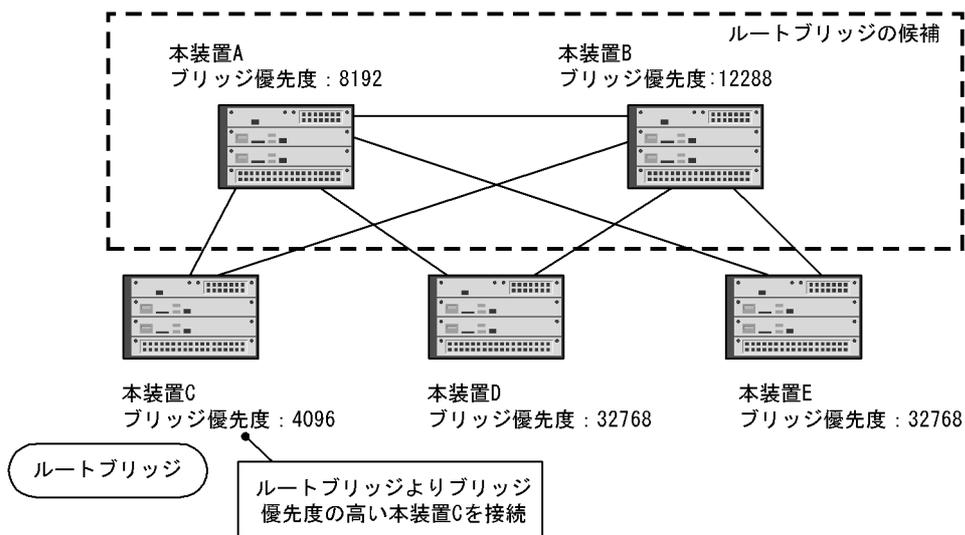
本装置 A、本装置 B をルートブリッジの候補として運用

図 21-17 本装置 A, 本装置 B をルートブリッジの候補として運用



本装置 A, 本装置 B よりブリッジ優先度の高い本装置 C を接続すると, 本装置 C がルートブリッジになり, 本装置 C にトラフィックが集中するようになる

図 21-18 本装置 A, 本装置 B よりブリッジ優先度の高い本装置 C を接続



ルートガード機能は, 現在のルートブリッジよりも優先度の高いブリッジを検出し, BPDU を廃棄することによってトポロジを保護します。また, 該当するポートをブロック状態に設定することでループを回避します。ルートガード機能は, ループガード機能を設定したポートには設定できません。

## 21.13 スパニングツリー共通機能のコンフィグレーション

### 21.13.1 コンフィグレーションコマンド一覧

スパニングツリー共通機能のコンフィグレーションコマンド一覧を次の表に示します。

表 21-20 コンフィグレーションコマンド一覧

| コマンド名                                    | 説明                              |
|------------------------------------------|---------------------------------|
| spanning-tree bpdufilter                 | ポートごとに BPDU フィルタ機能を設定します。       |
| spanning-tree bpduguard                  | ポートごとに BPDU ガード機能を設定します。        |
| spanning-tree guard                      | ポートごとにループガード機能, ルートガード機能を設定します。 |
| spanning-tree link-type                  | ポートのリンクタイプを設定します。               |
| spanning-tree loopguard default          | ループガード機能をデフォルトで使用するように設定します。    |
| spanning-tree portfast                   | ポートごとに PortFast 機能を設定します。       |
| spanning-tree portfast bpduguard default | BPDU ガード機能をデフォルトで使用するように設定します。  |
| spanning-tree portfast default           | PortFast 機能をデフォルトで使用するように設定します。 |

### 21.13.2 PortFast の設定

#### (1) PortFast の設定

PortFast は、端末を接続するポートなど、ループが発生しないことがあらかじめわかっているポートを直ちに通信できる状態にしたい場合に適用します。

##### [ 設定のポイント ]

spanning-tree portfast default コマンドを設定すると、アクセスポート、プロトコルポート、MAC ポートにデフォルトで PortFast 機能を適用します。デフォルトで適用してポートごとに無効にした場合は、spanning-tree portfast disable コマンドを設定します。  
トランクポートでは、ポートごとの指定で適用できます。

##### [ コマンドによる設定 ]

1. (config)# spanning-tree portfast default  
すべてのアクセスポート、プロトコルポート、MAC ポートに対して PortFast 機能を適用するように設定します。
2. (config)# interface gigabitethernet 1/1  
(config-if)# switchport mode access  
(config-if)# spanning-tree portfast disable  
(config-if)# exit  
ポート 1/1 (アクセスポート) で PortFast 機能を使用しないように設定します。
3. (config)# interface gigabitethernet 1/3  
(config-if)# switchport mode trunk  
(config-if)# spanning-tree portfast trunk

ポート 1/3 をトランクポートに指定し、PortFast 機能を適用します。トランクポートはデフォルトでは適用されません。ポートごとに指定するためには trunk パラメータを指定する必要があります。

## (2) BPDU ガードの設定

BPDU ガード機能は、PortFast を適用したポートで BPDU を受信した場合にそのポートを inactive 状態にします。通常、PortFast 機能は冗長経路ではないポートを指定し、ポートの先にはスパニングツリー装置がないことを前提とします。BPDU を受信したことによる意図しないトポロジー変更を回避したい場合に設定します。

### [ 設定のポイント ]

BPDU ガード機能を設定するためには、PortFast 機能を同時に設定する必要があります。

spanning-tree portfast bpduguard default コマンドは PortFast 機能を適用しているすべてのポートにデフォルトで BPDU ガードを適用します。デフォルトで適用するときに BPDU ガード機能を無効にしたい場合は、spanning-tree bpduguard disable コマンドを設定します。

### [ コマンドによる設定 ]

#### 1. (config)# spanning-tree portfast default

```
(config)# spanning-tree portfast bpduguard default
```

すべてのアクセスポート、プロトコルポート、MAC ポートに対して PortFast 機能を設定します。また、PortFast 機能を適用したすべてのポートに対し BPDU ガード機能を設定します。

#### 2. (config)# interface gigabitethernet 1/1

```
(config-if)# spanning-tree bpduguard disable
```

```
(config-if)# exit
```

ポート 1/1 (アクセスポート) で BPDU ガード機能を使用しないように設定します。ポート 1/1 は通常の PortFast 機能を適用します。

#### 3. (config)# interface gigabitethernet 1/2

```
(config-if)# switchport mode trunk
```

```
(config-if)# spanning-tree portfast trunk
```

ポート 1/2 (トランクポート) に PortFast 機能を設定します。また、BPDU ガード機能を設定します。トランクポートはデフォルトでは PortFast 機能を適用しないためポートごとに設定します。デフォルトで BPDU ガード機能を設定している場合は、PortFast 機能を設定すると自動的に BPDU ガードも適用します。デフォルトで設定していない場合は、spanning-tree bpduguard enable コマンドで設定します。

## 21.13.3 BPDU フィルタの設定

BPDU フィルタ機能は、BPDU を受信した場合にその BPDU を廃棄します。また、BPDU を一切送信しなくなります。通常は冗長経路ではないポートを指定することを前提とします。

### [ 設定のポイント ]

インタフェース単位に BPDU フィルタ機能を設定できます。

### [ コマンドによる設定 ]

#### 1. (config)# interface gigabitethernet 1/1

```
(config-if)# spanning-tree bpdudfilter enable
```

ポート 1/1 で BPDU フィルタ機能を設定します。

### 21.13.4 ループガードの設定

片線切れなどの単一方向のリンク障害が発生し、BPDU の受信が途絶えた場合、ループが発生することがあります。ループガードは、このようにループの発生を防止したい場合に設定します。

#### [ 設定のポイント ]

ループガードは、PortFast 機能を設定していないポートで動作します。

spanning-tree loopguard default コマンドを設定すると、PortFast を設定したポート以外のすべてのポートにループガードを適用します。デフォルトで適用する場合に、ループガードを無効にしたい場合は spanning-tree guard none コマンドを設定します。

#### [ コマンドによる設定 ]

##### 1. (config)# spanning-tree loopguard default

PortFast を設定したポート以外のすべてのポートに対してループガード機能を適用するように設定します。

##### 2. (config)# interface gigabitethernet 1/1

```
(config-if)# spanning-tree guard none
```

```
(config-if)# exit
```

デフォルトでループガードを適用するように設定した状態で、ポート 1/1 はループガードを無効にするように設定します。

##### 3. (config)# no spanning-tree loopguard default

```
(config)# interface gigabitethernet 1/2
```

```
(config-if)# spanning-tree guard loop
```

デフォルトでループガードを適用する設定を削除します。また、ポート 1/2 に対してポートごとの設定でループガードを適用します。

### 21.13.5 ルートガードの設定

ネットワークに誤って装置が接続された場合や設定が変更された場合、ルートブリッジが替わり、意図しないトポロジになることがあります。ルートガードは、このような意図しないトポロジ変更を防止したい場合に設定します。

#### [ 設定のポイント ]

ルートガードは指定ポートに対して設定します。ルートブリッジの候補となる装置以外の装置と接続する箇所すべてに適用します。

ルートガード動作時、PVST+ が動作している場合は、該当する VLAN のポートだけブロック状態に設定します。マルチプルスパニングツリーが動作している場合、該当するインスタンスのポートだけブロック状態に設定しますが、該当するポートが境界ポートの場合は、全インスタンスのポートをブロック状態に設定します。

#### [ コマンドによる設定 ]

##### 1. (config)# interface gigabitethernet 1/1

```
(config-if)# spanning-tree guard root
```

ポート 1/1 でルートガード機能を設定します。

### 21.13.6 リンクタイプの設定

リンクタイプはポートの接続状態を表します。Rapid PVST+、シングルスパニングツリーの Rapid STP、マルチプルスパニングツリーで高速な状態遷移を行うためには、スイッチ間の接続が point-to-point である必要があります。shared の場合は高速な状態遷移はしないで、PVST+、シングルスパニングツリーの STP と同様にタイマによる状態遷移となります。

#### [ 設定のポイント ]

ポートごとに接続状態を設定できます。設定しない場合、ポートが全二重の接続のときは point-to-point、半二重の接続の場合は shared となります。

#### [ コマンドによる設定 ]

```
1. (config)# interface gigabitethernet 1/1
 (config-if)# spanning-tree link-type point-to-point
```

ポート 1/1 を point-to-point 接続とみなして動作させます。

#### [ 注意事項 ]

実際のネットワークの接続形態が 1 対 1 接続ではない構成では、本コマンドで point-to-point を指定しないでください。1 対 1 接続ではない構成とは、一つのポートに隣接するスパニングツリー装置が 2 台以上存在する構成です。

## 21.14 スパニングツリー共通機能のオペレーション

### 21.14.1 運用コマンド一覧

スパニングツリー共通機能の運用コマンド一覧を次の表に示します。

表 21-21 運用コマンド一覧

| コマンド名              | 説明                |
|--------------------|-------------------|
| show spanning-tree | スパニングツリー情報を表示します。 |

### 21.14.2 スパニングツリー共通機能の状態の確認

スパニングツリー情報は show spanning-tree detail コマンドで確認してください。VLAN 10 の PVST+ の例を次の図に示します。

PortFast はポート 1/3, 1/4, 1/5 に設定していることを PortFast の項目で確認できます。ポート 1/3 は PortFast を設定していて、ポート 1/4 は PortFast に加えて BPDU ガードを設定しています。どちらのポートも意図しない BPDU を受信しないで正常に動作していることを示しています。ポート 1/5 は BPDU フィルタを設定しています。

ループガードはポート 1/2 に設定していることを Loop Guard の項目で確認できます。ルートガードはポート 1/6 に設定していることを Root Guard の項目で確認できます。リンクタイプは各ポートの Link Type の項目で確認できます。すべてのポートが point-to-point で動作しています。

図 21-19 スパニングツリーの情報

```

> show spanning-tree vlan 10 detail
Date 2006/03/21 18:13:59 UTC
VLAN 10 PVST+ Spanning Tree:Enabled Mode:Rapid PVST+
 Bridge ID
 Priority:32778 MAC Address:0012.e210.3004
 Bridge Status:Designated Path Cost Method:Short
 Max Age:20 Hello Time:2
 Forward Delay:15
 Root Bridge ID
 Priority:32778 MAC Address:0012.e210.1004
 Root Cost:4
 Root Port:1/1
 Max Age:20 Hello Time:2
 Forward Delay:15
 Port Information
 Port:1/1 Up
 Status:Forwarding Role:Root
 Priority:128 Cost:4
 Link Type:point-to-point Compatible Mode:-
 Loop Guard:OFF PortFast:OFF
 BpduFilter:OFF Root Guard:OFF
 BPDU Parameters(2006/03/21 18:13:59):
 Designated Root
 Priority:32778 MAC address:0012.e210.1004
 Designated Bridge
 Priority:32778 MAC address:0012.e210.1004
 Root Path Cost:0
 Port ID
 Priority:128 Number:1
 Message Age Time:0(3)/20
 Port:1/2 Up
 Status:Discarding Role:Alternate
 Priority:128 Cost:4
 Link Type:point-to-point Compatible Mode:-
 Loop Guard:ON PortFast:OFF
 BpduFilter:OFF Root Guard:OFF
 BPDU Parameters(2006/03/21 18:13:58):
 Designated Root
 Priority:32778 MAC address:0012.e210.1004
 Designated Bridge
 Priority:32778 MAC address:0012.e210.2004
 Root Path Cost:4
 Port ID
 Priority:128 Number:1
 Message Age Time:1(3)/20
 Port:1/3 Up
 Status:Forwarding Role:Designated
 Priority:128 Cost:4
 Link Type:point-to-point Compatible Mode:-
 Loop Guard:OFF PortFast:ON (BPDU not received)
 BpduFilter:OFF Root Guard:OFF
 Port:1/4 Up
 Status:Forwarding Role:Designated
 Priority:128 Cost:4
 Link Type:point-to-point Compatible Mode:-
 Loop Guard:OFF PortFast:BPDU Guard(BPDU not received)
 BpduFilter:OFF Root Guard:OFF
 Port:1/5 Up
 Status:Forwarding Role:Designated
 Priority:128 Cost:4
 Link Type:point-to-point Compatible Mode:-
 Loop Guard:ON PortFast:ON(BPDU not received)
 BpduFilter:OFF Root Guard:OFF
 Port:1/6 Up

```

|                          |                   |
|--------------------------|-------------------|
| Status:Forwarding        | Role:Designated   |
| Priority:128             | Cost:4            |
| Link Type:point-to-point | Compatible Mode:- |
| Loop Guard:OFF           | PortFast:OFF      |
| BpduFilter:OFF           | Root Guard:ON     |



# 22 Ring Protocol の解説

この章は，Autonomous Extensible Ring Protocol について説明します。Autonomous Extensible Ring Protocol は，リングトポロジーでのレイヤ 2 ネットワークの冗長化プロトコルで，以降，Ring Protocol と呼びます。

---

22.1 Ring Protocol の概要

---

22.2 Ring Protocol の基本原理

---

22.3 シングルリングの動作概要

---

22.4 マルチリングの動作概要

---

22.5 Ring Protocol のネットワーク設計

---

22.6 Ring Protocol 使用時の注意事項

---

## 22.1 Ring Protocol の概要

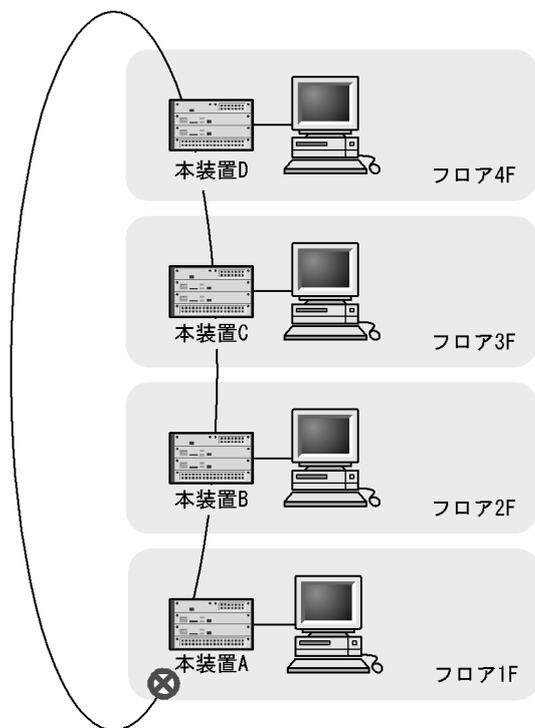
### 22.1.1 概要

Ring Protocol とは、スイッチをリング状に接続したネットワークでの障害の検出と、それに伴う経路切り替えを高速に行うレイヤ 2 ネットワークの冗長化プロトコルです。

レイヤ 2 ネットワークの冗長化プロトコルとして、スパンニングツリーが利用されますが、障害発生に伴う切り替えの収束時間が遅いなどの欠点があります。Ring Protocol を使用すると、障害発生に伴う経路切り替えを高速にできるようになります。また、リングトポロジーを利用することで、メッシュトポロジーよりも伝送路やインタフェースの必要量が少なくて済むという利点もあります。

Ring Protocol の適用例を次の図に示します。

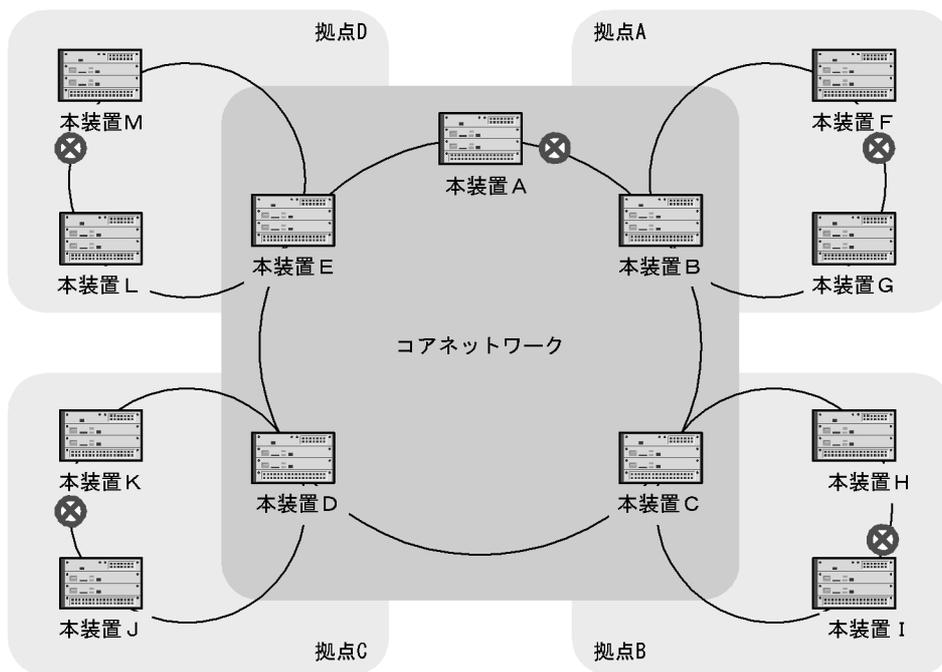
図 22-1 Ring Protocol の適用例（その 1）



(凡例)

⊗ : ブロッキング

図 22-2 Ring Protocol の適用例 (その2)

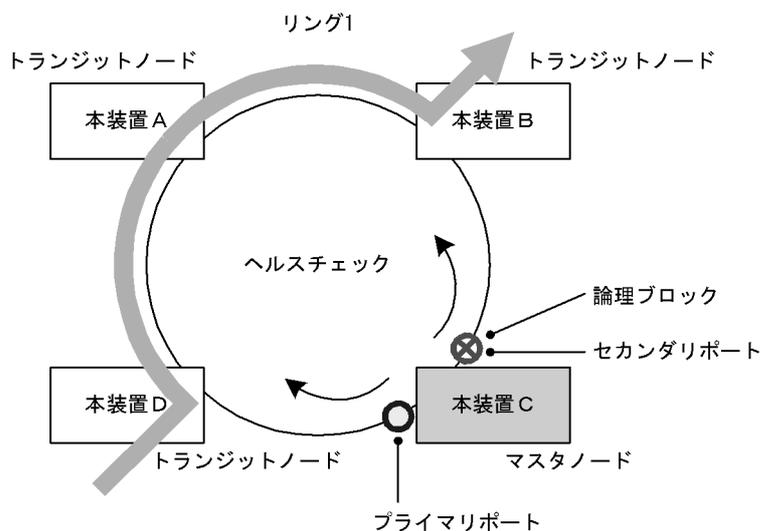


(凡例)

⊗ : ブロッキング

Ring Protocol によるリングネットワークの概要を次の図に示します。

図 22-3 Ring Protocol の概要



(凡例)

○ : フォワーディング

⊗ : ブロッキング

➡ : データの流れ

リングを構成するノードのうち一つをマスターノードとして、ほかのリング構成ノードをトランジットノード

ドとします。各ノード間を接続する二つのポートをリングポートと呼び、マスタノードのリングポートにはプライマリポートとセカンダリポートがあります。マスタノードはセカンダリポートを論理ブロックすることでリング構成を分断します。これによって、データフレームのループを防止しています。マスタノードはリング内の状態監視を目的とした制御フレーム（ヘルスチェックフレーム）を定期的に送信します。マスタノードは、巡回したヘルスチェックフレームの受信、未受信によって、リング内で障害が発生していないかどうかを判断します。障害または障害復旧を検出したマスタノードは、セカンダリポートの論理ブロックを設定または解除することで経路を切り替え、通信を復旧させます。

## 22.1.2 特長

### (1) イーサネットベースのリングネットワーク

Ring Protocol はイーサネットベースのネットワーク冗長化プロトコルです。従来のリングネットワークでは FDDI のように二重リンクの光ファイバを用いたネットワークが主流でしたが、Ring Protocol を用いることでイーサネットを用いたリングネットワークが構築できます。

### (2) シンプルな動作方式

Ring Protocol を使用したネットワークは、マスタノード 1 台とそのほかのトランジットノードで構成したシンプルな構成となります。リング状態（障害や障害復旧）の監視や経路の切り替え動作は、主にマスタノードが行い、そのほかのトランジットノードはマスタノードからの指示によって経路の切り替え動作を行います。

### (3) 制御フレーム

Ring Protocol では、本プロトコル独自の制御フレームを使用します。制御フレームは、マスタノードによるリング状態の監視やマスタノードからトランジットノードへの経路の切り替え指示に使われます。制御フレームの送受信は、専用の VLAN 上で行われるため、通常のスパンニングツリーのようにデータフレームと制御フレームが同じ VLAN 内に流れることはありません。

### (4) 負荷分散方式

リング内で使用する複数の VLAN を論理的なグループ単位にまとめ、マスタノードを基点としてデータの流れを右回りと左回りに分散させる設定ができます。負荷分散や VLAN ごとに経路を分けたい場合に有効です。

## 22.1.3 サポート仕様

Ring Protocol でサポートする項目と仕様を次の表に示します。

表 22-1 Ring Protocol でサポートする項目・仕様

| 項目                         |                        | 内容                      |
|----------------------------|------------------------|-------------------------|
| 適用レイヤ                      | レイヤ 2                  |                         |
|                            | レイヤ 3                  | ×                       |
| リング構成                      | シングルリング                |                         |
|                            | マルチリング                 | (共有リンクありマルチリング構成含む)     |
| 装置当たりのリング ID 最大数           |                        | 16 <sup>1</sup>         |
| リングポート (1 リング ID 当たりのポート数) |                        | 2 (物理ポートまたはリンクアグリゲーション) |
| VLAN 数                     | 1 リング ID 当たりの制御 VLAN 数 | 1 (デフォルト VLAN の設定は不可)   |

| 項目              |                                      | 内容                            |
|-----------------|--------------------------------------|-------------------------------|
|                 | 1 リング ID 当たりのデータ転送用 VLAN グループ最大数     | 2                             |
|                 | 1 データ転送用 VLAN グループ当たりの VLAN マッピング最大数 | 128 <sup>2</sup>              |
|                 | 1VLAN マッピング当たりの VLAN 最大数             | 4094                          |
| ヘルスチェックフレーム送信間隔 |                                      | 10 ~ 10000 ミリ秒の範囲で 1 ミリ秒単位    |
| 障害監視時間          |                                      | 32 ~ 12288 ミリ秒の範囲で 1 ミリ秒単位    |
| 負荷分散方式          |                                      | 二つのデータ転送用 VLAN グループを使用することで可能 |

(凡例)    : サポート    x : 未サポート

注 1

リングネットワークの構成によっては、最大 16 個まで設定できない場合があります。

注 2

Ring Protocol と VRF 機能を併用する ( コンフィグレーションコマンド `vrf mode` の `axrp-enable` パラメータ, または `axrp-enable-ipv4-ipv6` パラメータを設定している ) 場合, VLAN マッピングの最大数は 64 となります。

**【OP-NPAR】**

## 22.2 Ring Protocol の基本原理

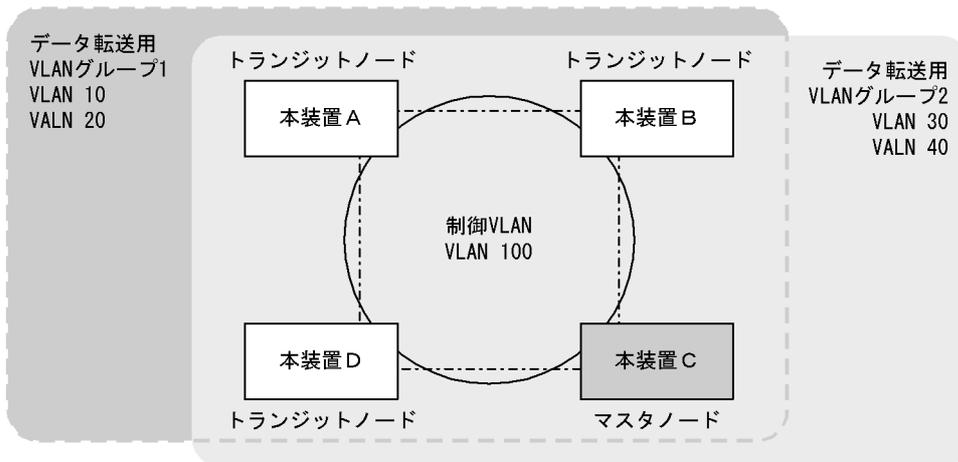
### 22.2.1 ネットワーク構成

Ring Protocol を使用する場合の基本的なネットワーク構成を次に示します。

#### (1) シングルリング構成

シングルリング構成について、次の図に示します。

図 22-4 シングルリング構成

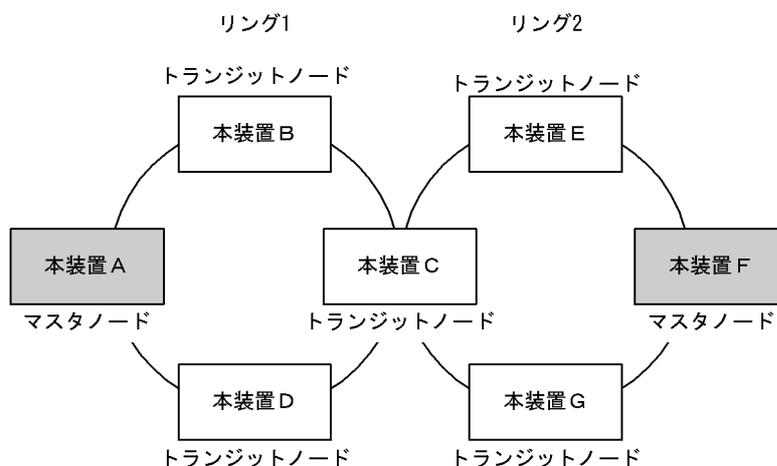


マスタノード 1 台とトランジットノード数台から成る一つのリング構成をシングルリング構成と呼びます。リングを構成するノード間は、リングポートとして、物理ポートまたはリンクアグリゲーションで接続されます。また、リングを構成するすべてのノードに、制御 VLAN として同一の VLAN、およびデータフレームの転送用として共通の VLAN を使用する必要があります。マスタノードから送信した制御フレームは、制御 VLAN 内を巡回します。データフレームの送受信に使用する VLAN は、VLAN グループと呼ばれる一つの論理的なグループに束ねて使用します。VLAN グループは複数の VLAN をまとめることができ、一つのリングにマスタノードを基点とした右回り用と左回り用の最大 2 グループを設定できます。

#### (2) マルチリング構成

マルチリング構成のうち、隣接するリングの接点となるノードが一つの場合の構成について次の図に示します。

図 22-5 マルチリング構成

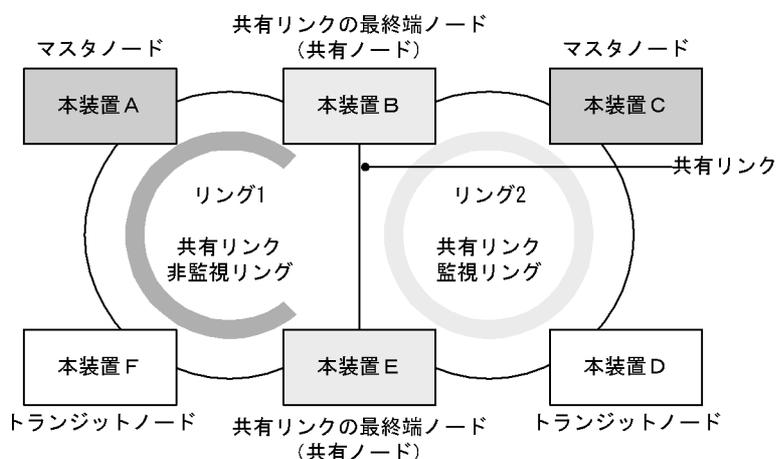


それぞれのリングを構成しているノードは独立したシングルリングとして動作します。このため、リング障害の検出および復旧の検出はそれぞれのリングで独立して行われます。

### (3) 共有リンクありのマルチリング構成

マルチリング構成のうち、隣接するリングの接点となるノードが二つ以上の場合の構成について次の図に示します。

図 22-6 共有リンクありのマルチリング構成



(凡例) ■: リング1の監視経路 □: リング2の監視経路

複数のシングルリングが、二つ以上のノードで接続されている場合、複数のリングでリンクを共有することになります。このリンクを共有リンクと呼び、共有リンクのあるマルチリング構成を、共有リンクありのマルチリング構成と呼びます。これに対し、(2)のように、複数のシングルリングが一つのノードで接続されている場合には、共有リンクがありませんので、共有リンクなしのマルチリング構成と呼びます。

共有リンクありのマルチリング構成では、隣接するリングで共通の VLAN をデータ転送用の VLAN グループとして使用した場合に、共有リンクで障害が発生すると隣接するリングそれぞれのマスタノードが障害を検出し、複数のリングをまたいだループ（いわゆるスーパーループ）が発生します。このため、本構成ではシングルリング構成とは異なる障害検出、および切り替え動作を行う必要があります。

Ring Protocol では、共有リンクをリングの一部とする複数のリングのうち、一つを共有リンクの障害および復旧を監視するリング（共有リンク監視リング）とし、それ以外のリングを、共有リンクの障害および復旧を監視しないリング（共有リンク非監視リング）とします。また、共有リンクの両端に位置するノードを共有リンク非監視リングの最終端ノード（または、共有ノード）と呼びます。このように、各リングのマスタノードで監視対象リングを重複させないことによって、共有リンク間の障害によるループの発生を防止します。

## 22.2.2 制御 VLAN

Ring Protocol を利用するネットワークでは、制御フレームの送信範囲を限定するために、制御フレームの送受信に専用の VLAN を使用します。この VLAN を制御 VLAN と呼び、リングを構成するすべてのノードで同一の VLAN を使用します。制御 VLAN は、リングごとに共通な一つの VLAN を使用しますので、マルチリング構成時には、隣接するリングで異なる VLAN を使用する必要があります。

## 22.2.3 障害監視方法

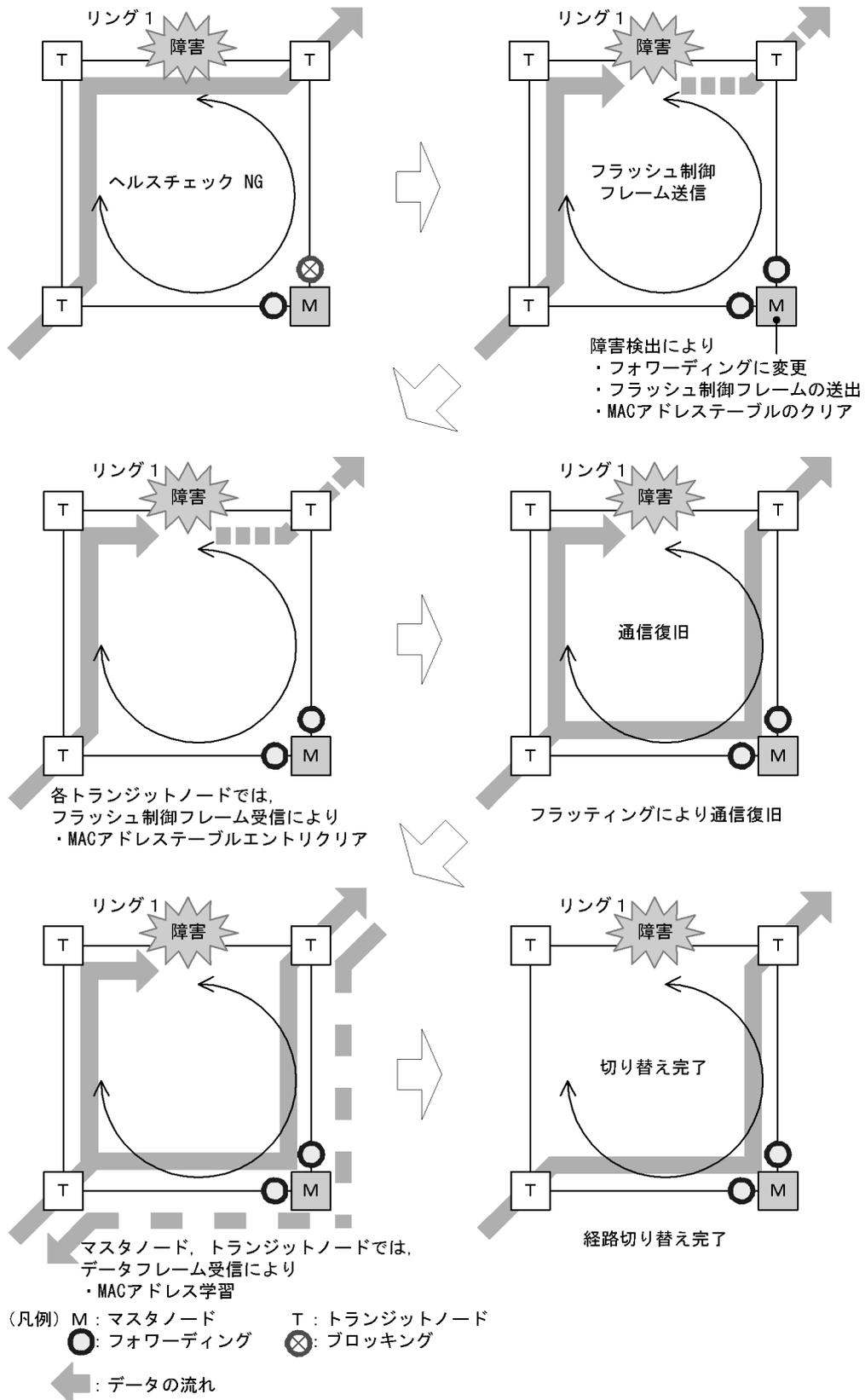
Ring Protocol のリング障害の監視は、マスタノードがヘルスチェックフレームと呼ぶ制御フレームを定期的を送信し、マスタノードがこのヘルスチェックフレームの受信可否を監視することで実現します。マスタノードでは、ヘルスチェックフレームが一定時間到達しないとリング障害が発生したと判断し、障害動作を行います。また、リング障害中に再度ヘルスチェックフレームを受信すると、リング障害が復旧したと判断し、復旧動作を行います。

## 22.2.4 通信経路の切り替え

マスタノードは、リング障害の検出による迂回経路への切り替えのために、セカンダリポートをブロッキングからフォワーディングに変更します。また、リング障害の復旧検出による経路の切り戻しのために、セカンダリポートをフォワーディングからブロッキングに変更します。これに併せて、早急な通信の復旧を行うために、リング内のすべてのノードで、MAC アドレステーブルエントリのクリアが必要です。MAC アドレステーブルエントリのクリアが実施されないと、切り替え（または切り戻し）前の情報に従ってデータフレームの転送が行われるため、正しくデータが届かないおそれがあります。したがって、通信を復旧させるために、リングを構成するすべてのノードで MAC アドレステーブルエントリのクリアを実施します。

マスタノードおよびトランジットノードそれぞれの場合の切り替え動作について次に説明します。

図 22-7 Ring Protocol の経路切り替え動作概要



### (1) マスタノードの経路切り替え

マスタノードでは、リング障害を検出するとセカンダリポートのブロッキングを解除します。また、リングポートで MAC アドレステーブルエントリのクリアを行います。これによって、MAC アドレスの学習が行われるまでフラッディングを行います。セカンダリポートを経由したフレームの送受信によって MAC アドレス学習を行い、新しい経路への切り替えが完了します。

### (2) トランジットノードの経路切り替え

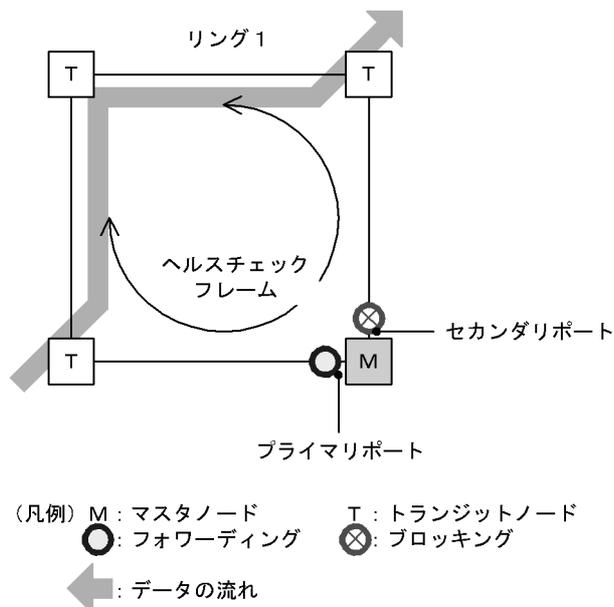
マスタノードがリングの障害を検出すると、同一の制御 VLAN を持つリング内の、そのほかのトランジットノードに対して MAC アドレステーブルエントリのクリアを要求するために、フラッシュ制御フレームと呼ぶ制御フレームを送信します。トランジットノードでは、このフラッシュ制御フレームを受信すると、リングポートでの MAC アドレステーブルエントリのクリアを行います。これによって、MAC アドレスの学習が行われるまでフラッディングを行います。新しい経路でのフレームの送受信によって MAC アドレス学習が行われ、通信経路の切り替えが完了します。

## 22.3 シングルリングの動作概要

### 22.3.1 リング正常時の動作

シングルリングでのリング正常時の動作について次の図に示します。

図 22-8 リング正常時の動作



#### (1) マスタノード動作

片方向リンク障害による障害誤検出を防止するために、二つのリングポートからヘルスチェックフレームを送信します。あらかじめ設定された時間内に、両方向のヘルスチェックフレームを受信するか監視します。データフレームの転送は、プライマリポートで行います。セカンダリポートは論理ブロックされているため、データフレームの転送および MAC アドレス学習は行いません。

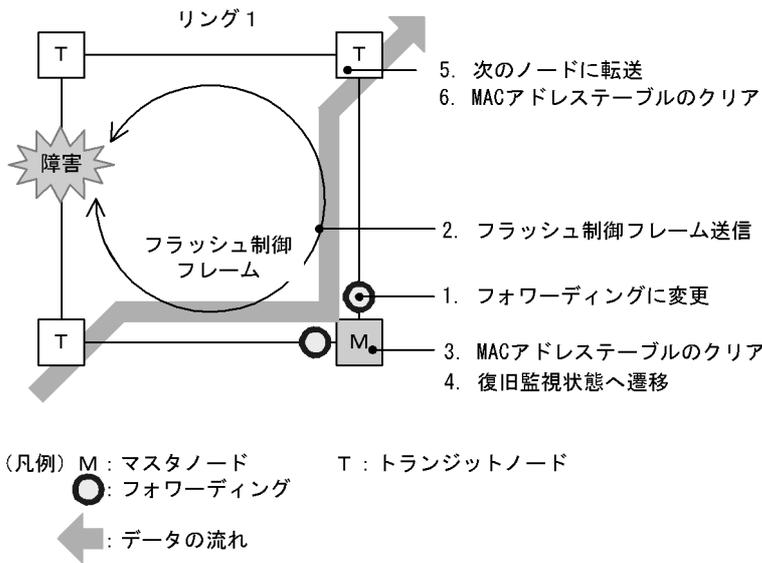
#### (2) トランジットノード動作

トランジットノードでは、マスタノードが送信するヘルスチェックフレームの監視は行いません。ヘルスチェックフレームを受信すると、リング内の次ノードに転送します。データフレームの転送は、両リングポートで行います。

### 22.3.2 障害検出時の動作

シングルリングでのリング障害検出時の動作について次の図に示します。

図 22-9 リング障害時の動作



(1) マスタノード動作

あらかじめ設定された時間内に、両方向のヘルスチェックフレームを受信しなければ障害と判断します。障害を検出したマスタノードは、次に示す手順で切り替え動作を行います。

1. データ転送用リング VLAN 状態の変更  
 セカンダリポートのリング VLAN 状態をブロッキングからフォワーディングに変更します。障害検出時のリング VLAN 状態は次の表のように変更します。

表 22-2 障害検出時のデータ転送用リング VLAN 状態

| リングポート   | 変更前（正常時） | 変更後（障害時） |
|----------|----------|----------|
| プライマリポート | フォワーディング | フォワーディング |
| セカンダリポート | ブロッキング   | フォワーディング |

2. フラッシュ制御フレームの送信  
 マスタノードのプライマリポートおよびセカンダリポートからフラッシュ制御フレームを送信します。
3. MAC アドレステーブルのクリア  
 リングポートに関する MAC アドレステーブルエントリのクリアを行います。MAC アドレステーブルエントリをクリアすることで、迂回経路へ切り替えられます。
4. 監視状態の変更  
 リング障害を検出すると、マスタノードは障害監視状態から復旧監視状態に遷移します。

(2) トランジットノード動作

障害を検出したマスタノードから送信されるフラッシュ制御フレームを受信すると、トランジットノードでは次に示す動作を行います。

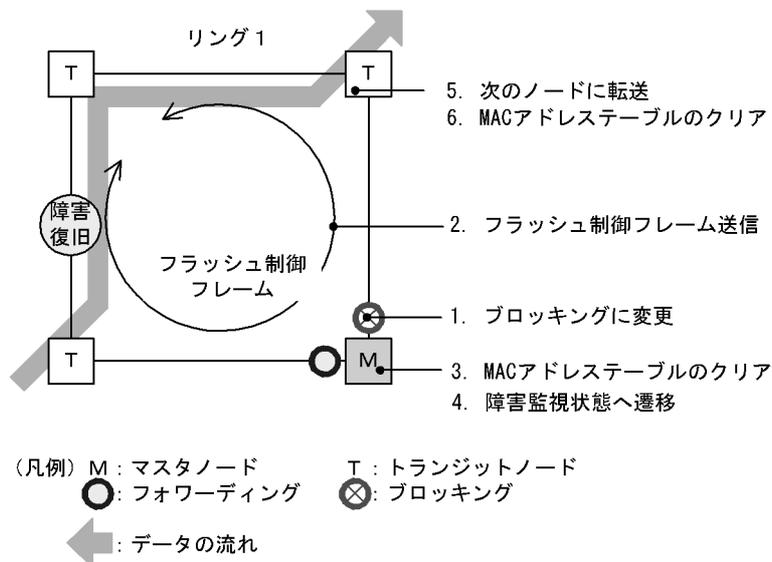
5. フラッシュ制御フレームの転送  
 受信したフラッシュ制御フレームを次のノードに転送します。
6. MAC アドレステーブルのクリア

リングポートに関する MAC アドレステーブルエントリのクリアを行います。MAC アドレステーブルエントリをクリアすることで、迂回経路へ切り替えられます。

### 22.3.3 復旧検出時の動作

シングルリングでのリング障害復旧時の動作について次の図に示します。

図 22-10 障害復旧時の動作



#### (1) マスタノード動作

リング障害を検出している状態で、自身が送出したヘルスチェックフレームを受信すると、リング障害が復旧したと判断し、次に示す復旧動作を行います。

##### 1. データ転送用リング VLAN 状態の変更

セカンダリポートのリング VLAN 状態をフォワーディングからブロッキングに変更します。復旧検出時のリング VLAN 状態は次の表のように変更します。

表 22-3 復旧検出時のデータ転送用リング VLAN 状態

| リングポート   | 変更前 (障害時) | 変更後 (復旧時) |
|----------|-----------|-----------|
| プライマリポート | フォワーディング  | フォワーディング  |
| セカンダリポート | フォワーディング  | ブロッキング    |

##### 2. フラッシュ制御フレームの送信

マスタノードのプライマリポートおよびセカンダリポートからフラッシュ制御フレームを送信します。なお、リング障害復旧時は、各トランジットノードが転送したフラッシュ制御フレームがマスタノードへ戻ってきますが、マスタノードでは受信しても廃棄します。

##### 3. MAC アドレステーブルのクリア

リングポートに関する MAC アドレステーブルエントリのクリアを行います。

##### 4. 監視状態の変更

リング障害の復旧を検出すると、マスタノードは復旧監視状態から障害監視状態に遷移します。

## (2) トランジットノード動作

マスタノードから送信されるフラッシュ制御フレームを受信すると、次に示す動作を行います。

### 5. フラッシュ制御フレームの転送

受信したフラッシュ制御フレームを次のノードに転送します。

### 6. MAC アドレステーブルクリア

リングポートに関する MAC アドレステーブルエントリのクリアを行います。

また、リンク障害が発生したトランジットノードでは、リンク障害が復旧した際のループの発生を防ぐため、リングポートのリング VLAN 状態はブロッキング状態となります。ブロッキング状態を解除する契機は、マスタノードが送信するフラッシュ制御フレームを受信したとき、またはトランジットノードでリングポートのフラッシュ制御フレーム受信待ち保護時間 (forwarding-shift-time) がタイムアウトしたときとなります。フラッシュ制御フレーム受信待ち保護時間 (forwarding-shift-time) は、リングポートのリンク障害復旧時に設定されます。

## 22.3.4 経路切り戻し抑止および解除時の動作

経路切り戻し抑止機能を適用すると、マスタノードでリングの障害復旧を検出した場合に、マスタノードは復旧抑止状態になり、すぐには復旧動作を行いません。本機能を有効にするには、コンフィグレーションコマンド preempt-delay の設定が必要です。

なお、経路切り戻し抑止状態は、次の契機で解除します。

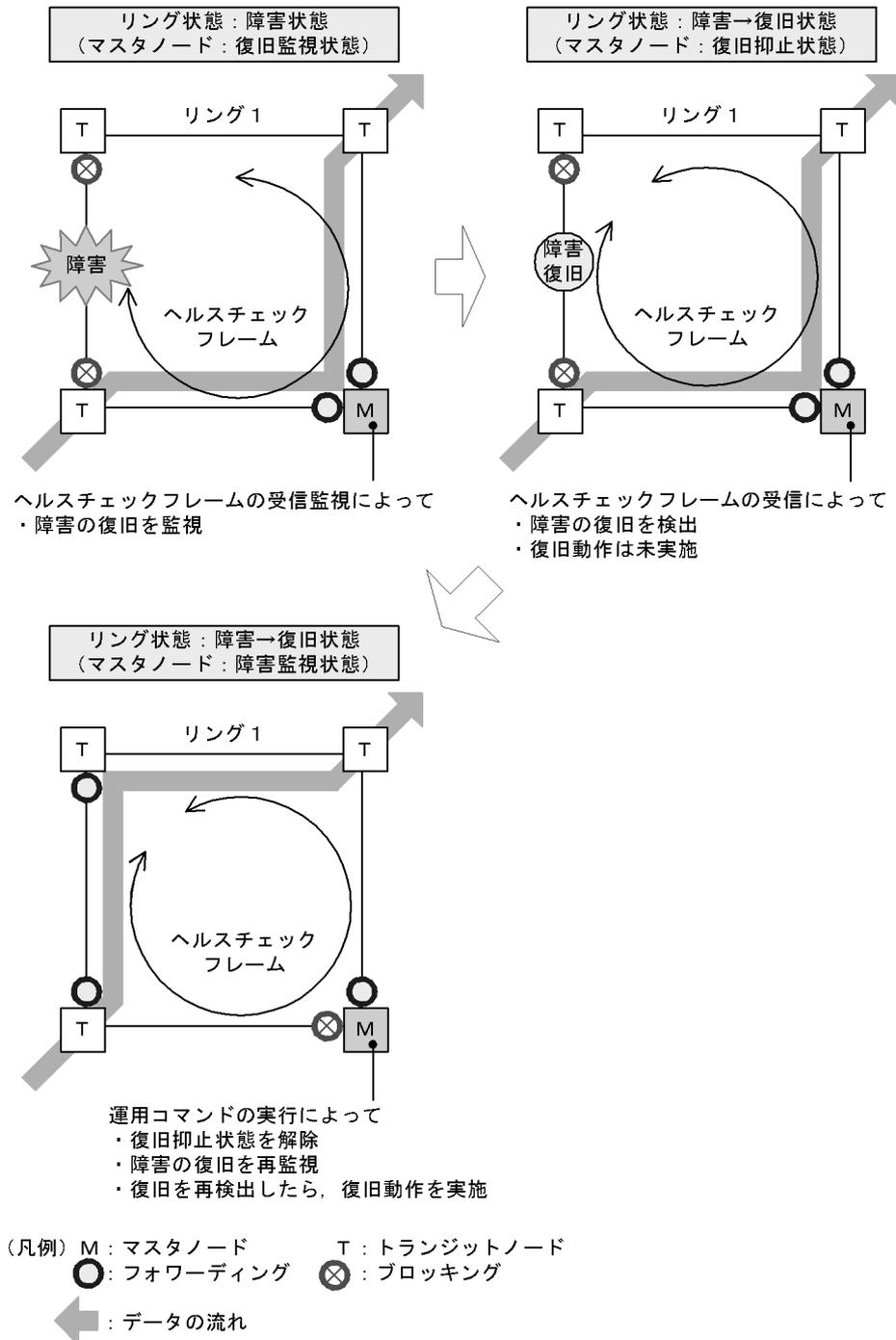
- 運用コマンド clear axrp preempt-delay の実行によって、経路切り戻し抑止が解除された場合
- コンフィグレーションコマンド preempt-delay で指定した、経路切り戻し抑止時間が経過した場合
- 経路切り戻し抑止機能を有効にするコンフィグレーションコマンド preempt-delay を削除した場合

復旧抑止状態が解除されると、マスタノードは再度、復旧監視状態に遷移します。その後リング障害の復旧を再検出すると、復旧動作を行います。復旧が完了すると、マスタノードは障害監視状態に遷移します。

また、経路切り戻し抑止状態でリングの障害が発生しても、マスタノードは復旧抑止状態を維持します。運用コマンド clear axrp preempt-delay の実行によって経路切り戻し抑止状態が解除されると、マスタノードは再度、復旧監視状態に遷移します。このとき、リング障害の復旧は検出しないため、復旧動作は行いません。その後、リングネットワーク上のすべての障害が復旧すると、マスタノードは障害の復旧を検出して、すぐに復旧動作を行います。

運用コマンド clear axrp preempt-delay の実行によって経路切り戻し抑止を解除した場合の動作を次の図に示します。その他の契機で解除した場合も、同様の動作となります。

図 22-11 運用コマンドの実行によって経路切り戻し抑止を解除した場合の動作



また、次に示すイベントが発生した場合は経路の切り戻し抑止状態を解除して、マスタノードが障害監視状態に遷移します。

- ・ 装置起動 (運用コマンド reload および ppupdate の実行を含む)
- ・ コンフィグレーションファイルの運用への反映 (運用コマンド copy の実行)
- ・ BCU, CSU または MSU の系切替 (運用コマンド redundancy force-switchover の実行を含む)
- ・ 全 BSU 障害から一部 BSU の障害復旧 (運用コマンド activate bsu の実行を含む) 【AX6700S】
- ・ Ring Protocol プログラムの再起動 (運用コマンド restart axrp の実行を含む)

- VLAN プログラムの再起動 (運用コマンド `restart vlan` の実行を含む)

## 22.4 マルチリングの動作概要

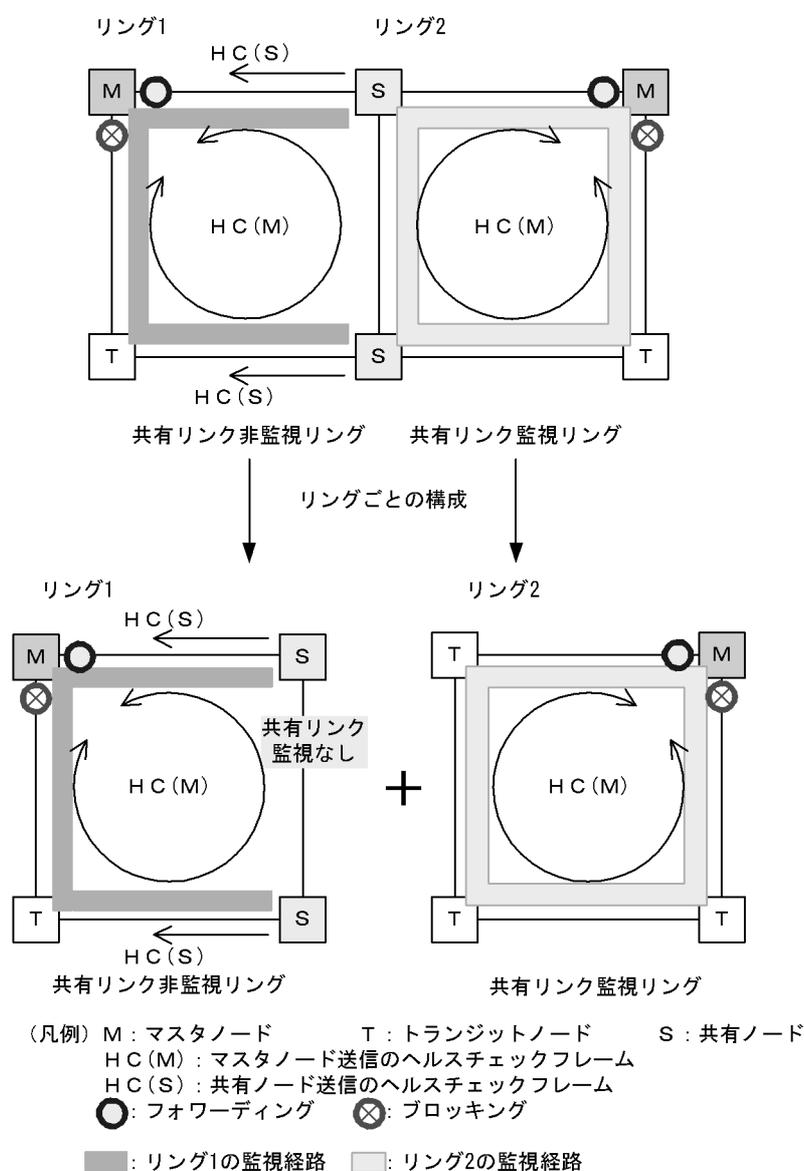
マルチリング構成のうち、共有リンクありのマルチリング構成について説明します。共有リンクなしのマルチリング構成については、シングルリング時の動作と同様ですので、「22.3 シングルリングの動作概要」を参照してください。

なお、この節では、HC はヘルスチェックフレームを意味し、HC(M) はマスターノードが送信するヘルスチェックフレーム、HC(S) は共有ノードが送信するヘルスチェックフレームを表します。

### 22.4.1 リング正常時の動作

共有リンクありのマルチリング構成でのリング正常時の状態について次の図に示します。

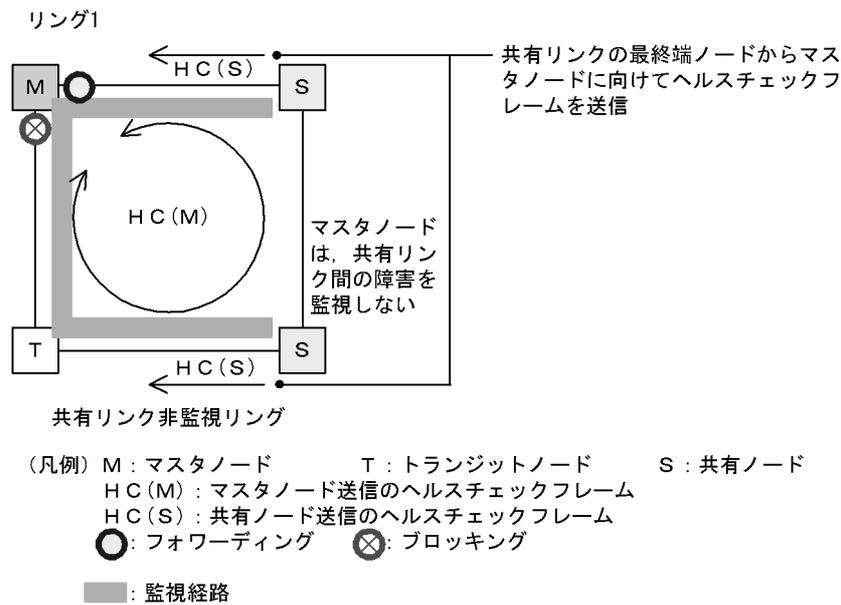
図 22-12 リング正常時の状態



## (1) 共有リンク非監視リング

共有リンク非監視リングは、マスタノード 1 台とトランジットノード数台で構成します。しかし、共有リンクの障害を監視しないため、補助的な役割として、共有リンクの両端に位置する共有リンク非監視リングの最終端ノード（共有ノード）から、ヘルスチェックフレームをマスタノードに向けて送信します。このヘルスチェックフレームは、二つのリングポートのうち、共有リンクではない方のリングポートから送信します。これによって、共有リンク非監視リングのマスタノードは、共有リンクで障害が発生した場合に、自身が送信したヘルスチェックフレームが受信できなくなっても、共有リンク非監視リングの最終端ノード（共有ノード）からのヘルスチェックフレームが受信できている間は障害を検出しないようになります。

図 22-13 共有リンク非監視リングでの正常時の動作



## (a) マスタノード動作

片方向リンク障害による障害誤検出を防止するために、二つのリングポートからヘルスチェックフレーム（HC(M)）を送信します。あらかじめ設定した時間内に、両方向の HC(M) を受信するか監視します。マスタノードが送信した HC(M) とは別に、共有リンクの両端に位置する共有リンク非監視リングの最終端ノード（共有ノード）から送信したヘルスチェックフレーム（HC(S)）についても合わせて受信を監視します。データフレームの転送は、プライマリポートで行います。セカンダリポートは論理ブロックされているため、データフレームの転送および MAC アドレス学習は行いません。

## (b) トランジットノード動作

トランジットノードの動作は、シングルリング時と同様です。トランジットノードは、HC(M) および HC(S) を監視しません。HC(M) や HC(S) を受信すると、リング内の次ノードに転送します。データフレームの転送は、両リングポートで行います。

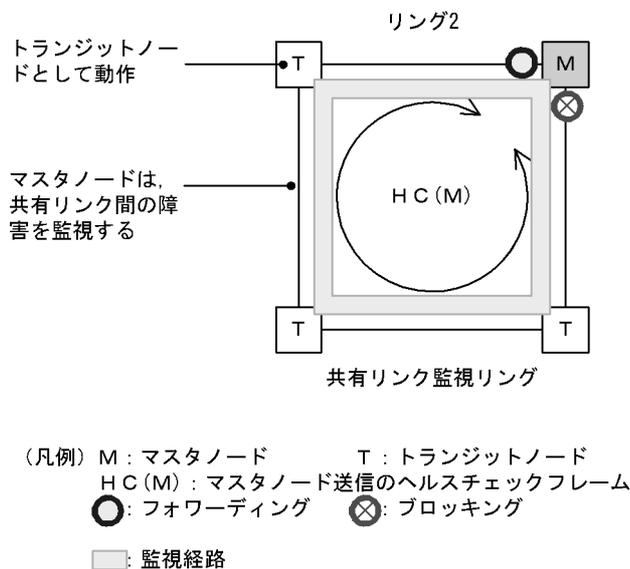
## (c) 共有リンク非監視リングの最終端ノード動作

共有リンク非監視リングの最終端ノード（共有ノード）は、共有リンク非監視リングのマスタノードに向けて HC(S) の送信を行います。HC(S) の送信は、二つのリングポートのうち、共有リンクではない方のリングポートから送信します。マスタノードが送信する HC(M) や、データフレームの転送については、トランジットノードの場合と同様となります。

## (2) 共有リンク監視リング

共有リンク監視リングは、シングルリング時と同様に、マスターノード 1 台と、そのほか数台のトランジットノードとの構成となります。共有リンクの両端に位置するノードは、シングルリング時と同様にマスターノードまたはトランジットノードとして動作します。

図 22-14 共有リンク監視リングでの正常時の動作



### (a) マスタノード動作

片方向リンク障害による障害誤検出を防止するために、二つのリングポートからヘルスチェックフレーム (HC(M)) を送信します。あらかじめ設定された時間内に、両方向の HC(M) を受信するかを監視します。データフレームの転送は、プライマリポートで行います。セカンダリポートは論理ブロックされているため、データフレームの転送および MAC アドレス学習は行いません。

### (b) トランジットノード動作

トランジットノードの動作は、シングルリング時と同様です。トランジットノードは、マスターノードが送信した HC(M) を監視しません。HC(M) を受信すると、リング内の次ノードに転送します。データフレームの転送は、両リングポートで行います。

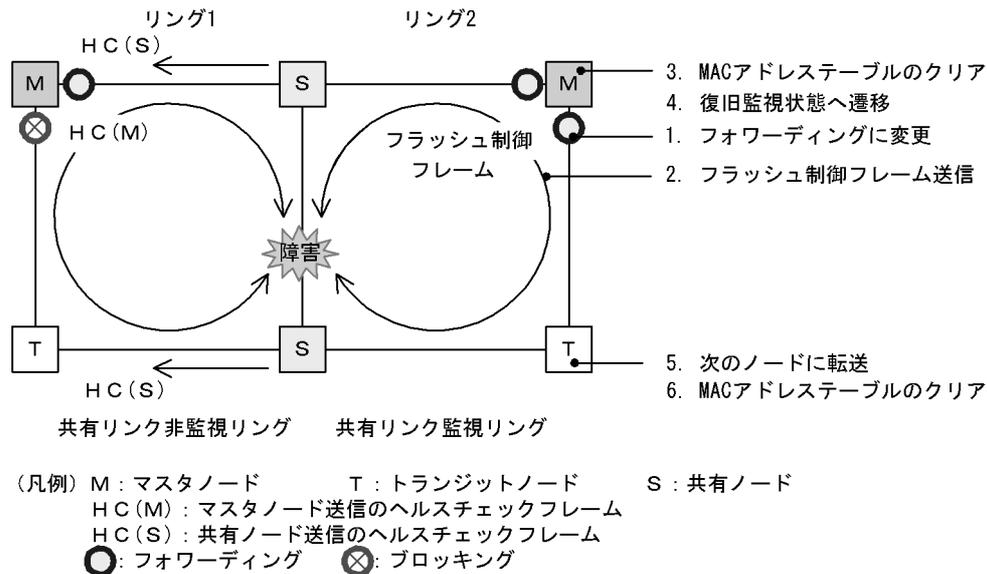
## 22.4.2 共有リンク障害・復旧時の動作

共有リンクありのマルチリング構成時に、共有リンク間で障害が発生した際の障害および復旧動作について説明します。

### (1) 障害検出時の動作

共有リンクの障害を検出した際の動作について次の図に示します。

図 22-15 共有リンク障害時の動作



(a) 共有リンク監視リングのマスタノード動作

共有リンクで障害が発生すると、マスタノードは両方向の HC(M) を受信できなくなり、リング障害を検出します。障害を検出したマスタノードはシングルリング時と同様に、次に示す手順で障害動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b) 共有リンク監視リングのトランジットノード動作

シングルリング時と同様に、マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

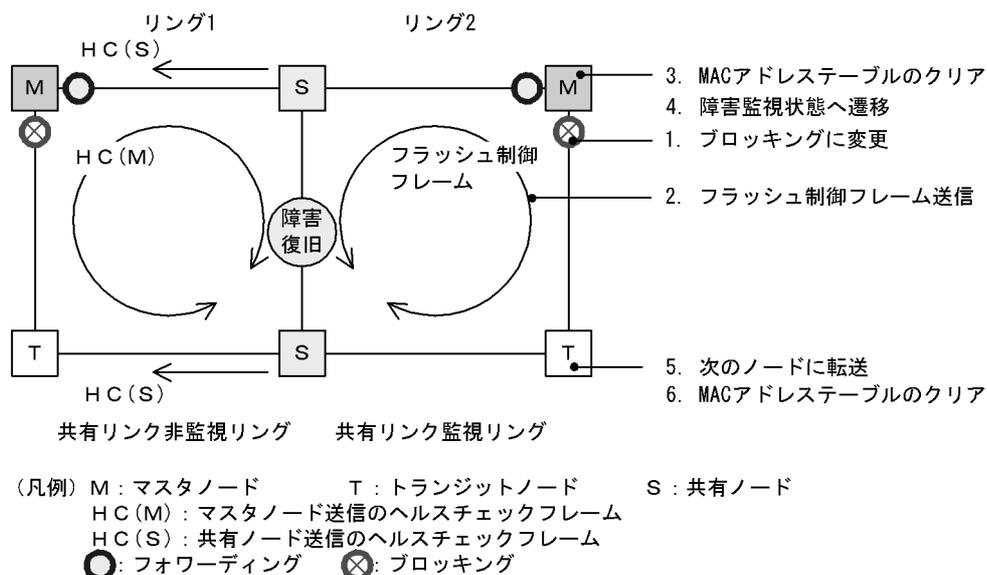
(c) 共有リンク非監視リングのマスタノードおよびトランジットノード動作

共有リンク非監視リングのマスタノードは、共有リンクでのリング障害を検出しないため、障害動作は行いません。このため、トランジットノードについても経路の切り替えは発生しません。

(2) 復旧検出時の動作

共有リンクの障害復旧を検出した際の動作について次の図に示します。

図 22-16 共有リンク復旧時の動作



## (a) 共有リンク監視リングのマスタノード動作

リング障害を検出している状態で、自身が送信した HC(M) を受信すると、リング障害が復旧したと判断し、シングルリング時と同様に、次に示す手順で復旧動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

## (b) 共有リンク監視リングのトランジットノード動作

シングルリング時と同様に、マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

## (c) 共有リンク非監視リングのマスタノードおよびトランジットノード動作

共有リンク非監視リングのマスタノードは、リング障害を検出していないため、トランジットノードを含め、復旧動作は行いません。

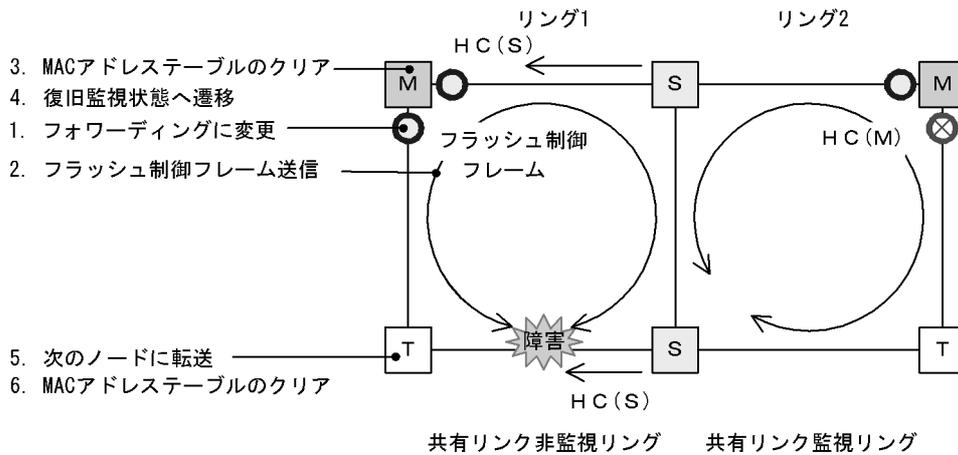
### 22.4.3 共有リンク非監視リングでの共有リンク以外の障害・復旧時の動作

共有リンク非監視リングでの、共有リンク以外のリング障害および復旧時の動作について説明します。

## (1) 障害検出時の動作

共有リンク非監視リングでの共有リンク以外の障害を検出した際の動作について次の図に示します。

図 22-17 共有リンク非監視リングにおける共有リンク以外のリング障害時の動作



(凡例) M : マスタノード      T : トランジットノード      S : 共有ノード  
 H C (M) : マスタノード送信のヘルスチェックフレーム  
 H C (S) : 共有ノード送信のヘルスチェックフレーム  
 ○ : フォワーディング      ⊗ : ブロッキング

(a) 共有リンク非監視リングのマスタノード動作

共有リンク非監視リングのマスタノードは、自身が送信した両方向の HC(M) と共有ノードが送信した HC(S) が共に未受信となりリング障害を検出します。障害を検出したマスタノードの動作はシングルリング時と同様に、次に示す手順で障害動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b) 共有リンク非監視リングのトランジットノードおよび共有ノード動作

シングルリング時と同様に、マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

(c) 共有リンク監視リングのマスタノードおよびトランジットノード動作

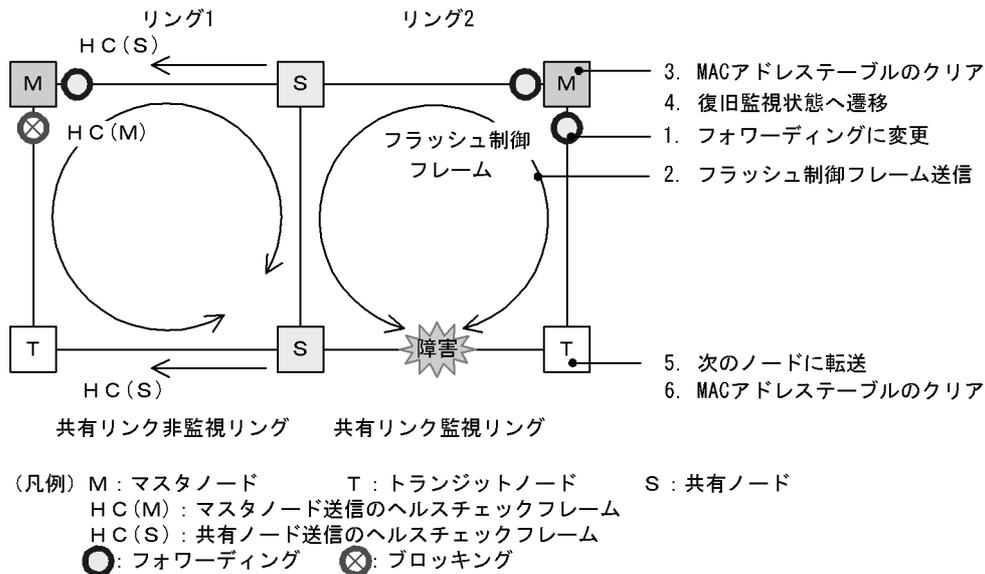
共有リンク監視リング内では障害が発生していないため、障害動作は行いません。

(2) 復旧検出時の動作

共有リンク非監視リングでの共有リンク以外の障害が復旧した際の動作について次の図に示します。



図 22-19 共有リンク監視リングでの共有リンク以外のリング障害時の動作



## (a) 共有リンク監視リングのマスタノード動作

共有リンク監視リング内で障害が発生すると、マスタノードは両方向の HC(M) を受信できなくなり、リング障害を検出します。障害を検出したマスタノードはシングルリング時と同様に、次に示す手順で障害動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

## (b) 共有リンク監視リングのトランジットノード動作

シングルリング時と同様に、マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

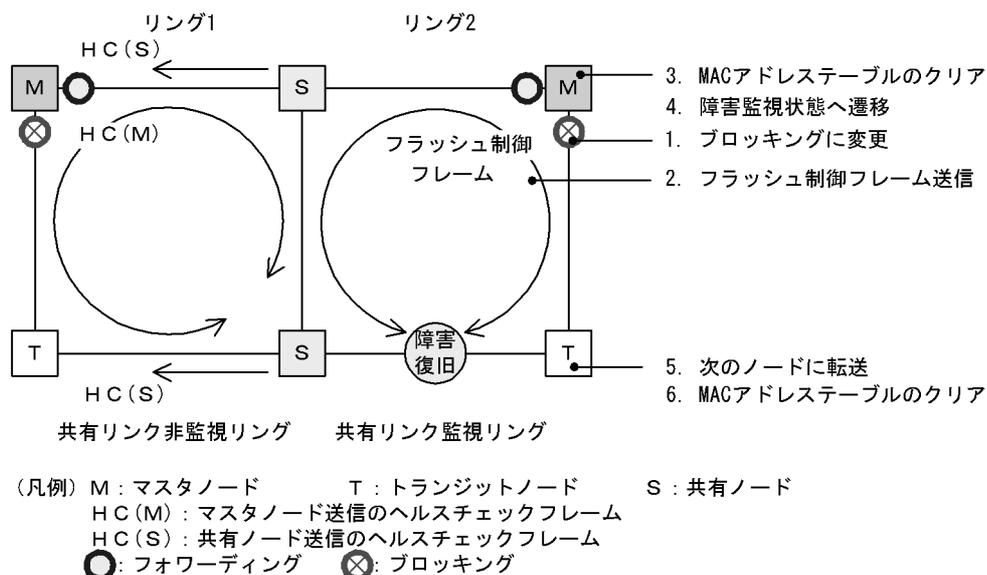
## (c) 共有リンク非監視リングのマスタノードおよびトランジットノード（共有ノード）動作

共有リンク非監視リング内では障害が発生していないため、障害動作は行いません。

## (2) 復旧検出時の動作

共有リンク監視リングでの共有リンク以外の障害が復旧した際の動作について次の図に示します。

図 22-20 共有リンク監視リングでの共有リンク以外のリング障害復旧時の動作



## (a) 共有リンク監視リングのマスタノード動作

リング障害を検出している状態で、自身が送信した HC(M) を受信すると、リング障害が復旧したと判断し、シングルリング時と同様に、次に示す手順で復旧動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

## (b) 共有リンク監視リングのトランジットノード動作

シングルリング時と同様に、マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

## (c) 共有リンク非監視リングのマスタノードおよびトランジットノード（共有ノード）動作

共有リンク非監視リング内では障害が発生していないため、復旧動作は行いません。

## 22.4.5 経路切り戻し抑止および解除時の動作

マルチリング構成での経路切り戻し抑止および解除時の動作については、シングルリング時の動作と同様ですので、「22.3 シングルリングの動作概要」を参照してください。

## 22.5 Ring Protocol のネットワーク設計

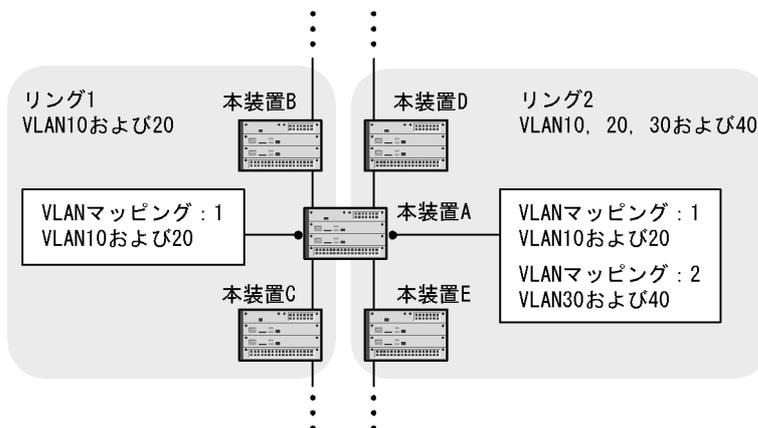
### 22.5.1 VLAN マッピングの使用方法

#### (1) VLAN マッピングとデータ転送用 VLAN

マルチリング構成などで、一つの装置に複数のリング ID を設定するような場合、それぞれのリング ID に複数の同一 VLAN を設定する必要があります。このとき、データ転送用 VLAN として使用する VLAN のリスト（これを VLAN マッピングと呼びます）をあらかじめ設定しておくことで、マルチリング構成時のデータ転送用 VLAN の設定を簡略できたり、コンフィギュレーションの設定誤りによるループなどを防止できたりします。

VLAN マッピングは、データ転送用に使用する VLAN を VLAN マッピング ID に割り当てて使用します。この VLAN マッピング ID を VLAN グループに設定して、データ転送用 VLAN として管理します。

図 22-21 リングごとの VLAN マッピングの割り当て例



#### (2) PVST+ と併用する場合の VLAN マッピング

Ring Protocol と PVST+ を併用する場合は、PVST+ に使用する VLAN を VLAN マッピングにも設定します。このとき、VLAN マッピングに割り当てる VLAN は一つだけにしてください。PVST+ と併用する VLAN 以外のデータ転送用 VLAN は、別の VLAN マッピングに設定して、PVST+ と併用する VLAN マッピングと合わせて VLAN グループに設定します。

### 22.5.2 制御 VLAN の forwarding-delay-time の使用方法

トランジットノードの装置起動やプログラム再起動 (restart axrp コマンド) など、Ring Protocol が初期状態から動作する場合、データ転送用 VLAN は論理ブロックされています。トランジットノードは、マスタノードが送信するフラッシュ制御フレームを受信することでこの論理ブロックを解除します。しかし、プログラム再起動時や系切替時などは、マスタノードの障害監視時間 (health-check holdtime) が長いと、リングネットワークの状態変化を認識できないおそれがあります。この場合、フラッシュ制御フレーム受信待ち保護時間 (forwarding-shift-time) がタイムアウトするまで論理ブロックは解除されないため、トランジットノードのデータ VLAN は通信できない状態になります。制御 VLAN のフォワーディング遷移時間 (forwarding-delay-time) を設定すると次に示す手順で動作するため、このようなケースを回避できます。

1. トランジットノードは、装置起動やプログラム再起動直後に、制御 VLAN をいったん論理ブロックします。
2. トランジットノードの制御 VLAN が論理ブロックされたので、マスタノードで障害を検出します（ただし、装置起動時はこれ以前に障害を検出しています）。このため、通信は迂回経路に切り替わります。
3. トランジットノードは、制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）のタイムアウトによって制御 VLAN のブロッキングを解除します。
4. マスタノードはヘルスチェックフレームを受信することで復旧を検出し、フラッシュ制御フレームを送信します。
5. トランジットノードは、このフラッシュ制御フレームを受信することでデータ転送用 VLAN の論理ブロックを解除します。これによってデータ転送用 VLAN での通信が再開され、リングネットワーク全体でも通常の通信経路に復旧します。

### (1) 制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）と障害監視時間（health-check holdtime）の関係について

制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）は、障害監視時間（health-check holdtime）より大きな値を設定してください。制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）は、障害監視時間（health-check holdtime）の 2 倍程度を目安として設定することを推奨します。障害監視時間（health-check holdtime）より小さな値を設定した場合、マスタノードで障害を検出できません。したがって、迂回経路への切り替えが行われなため、通信断の時間が長くなるおそれがあります。

## 22.5.3 プライマリポートの自動決定

マスタノードのプライマリポートは、ユーザが設定した二つのリングポートの情報に従って、自動で決定します。次の表に示すように、優先度の高い方がプライマリポートとして動作します。また、VLAN グループごとに優先度を逆にすることで、ユーザが特に意識することなく、経路の振り分けができるようになります。

表 22-4 プライマリポートの選択方式（VLAN グループ # 1）

| リングポート # 1 | リングポート # 2 | 優先ポート                                                                                                                           |
|------------|------------|---------------------------------------------------------------------------------------------------------------------------------|
| 物理ポート      | 物理ポート      | <ul style="list-style-type: none"> <li>• NIF 番号の小さい方がプライマリポートとして動作</li> <li>• NIF 番号が同一の場合は、ポート番号の小さい方がプライマリポートとして動作</li> </ul> |
| 物理ポート      | チャンネルグループ  | 物理ポート側がプライマリポートとして動作                                                                                                            |
| チャンネルグループ  | 物理ポート      | 物理ポート側がプライマリポートとして動作                                                                                                            |
| チャンネルグループ  | チャンネルグループ  | チャンネルグループ番号の小さい方がプライマリポートとして動作                                                                                                  |

表 22-5 プライマリポートの選択方式（VLAN グループ # 2）

| リングポート # 1 | リングポート # 2 | 優先ポート                                                                                                                           |
|------------|------------|---------------------------------------------------------------------------------------------------------------------------------|
| 物理ポート      | 物理ポート      | <ul style="list-style-type: none"> <li>• NIF 番号が大きい方がプライマリポートとして動作</li> <li>• NIF 番号が同一の場合は、ポート番号の大きい方がプライマリポートとして動作</li> </ul> |
| 物理ポート      | チャンネルグループ  | チャンネルグループ側がプライマリポートとして動作                                                                                                        |
| チャンネルグループ  | 物理ポート      | チャンネルグループ側がプライマリポートとして動作                                                                                                        |
| チャンネルグループ  | チャンネルグループ  | チャンネルグループ番号の大きい方がプライマリポートとして動作                                                                                                  |

また、上記の決定方式以外に、コンフィグレーションコマンド `axrp-primary-port` を使って、ユーザが VLAN グループごとにプライマリポートを設定することもできます。

## 22.5.4 同一装置内でのノード種別混在構成

### (1) ノード種別の混在設定

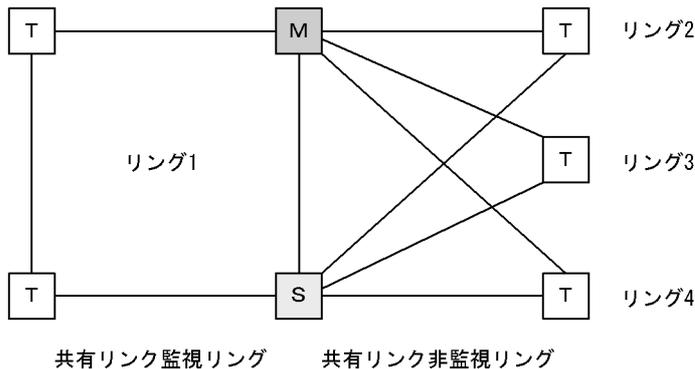
本装置が、二つの異なるリングに属している場合に、一方のリングではマスタノードとして動作し、もう一方のリングではトランジットノードとして動作させることができます。

### (2) 最大マルチリング数

本装置を共有リンク非監視リングのマスタノードとしてマルチリング構成にする場合、マルチリング数は 16 より少なくなります。例えば、同一装置で共有リンク非監視リングのマスタノードだけで構成した場合のマルチリング数は、最大 8 になります。

例を次の図に示します。この図では、リング 1 が共有リンク監視リングに、リング 2、リング 3 およびリング 4 は共有リンク非監視リングになっています。また、すべてのリングで、同一装置がマスタノードになっています。この場合、この装置での設定可能な残りリング数は 9 リングになります。

図 22-22 共有リンク非監視リングでのマスタノード設定

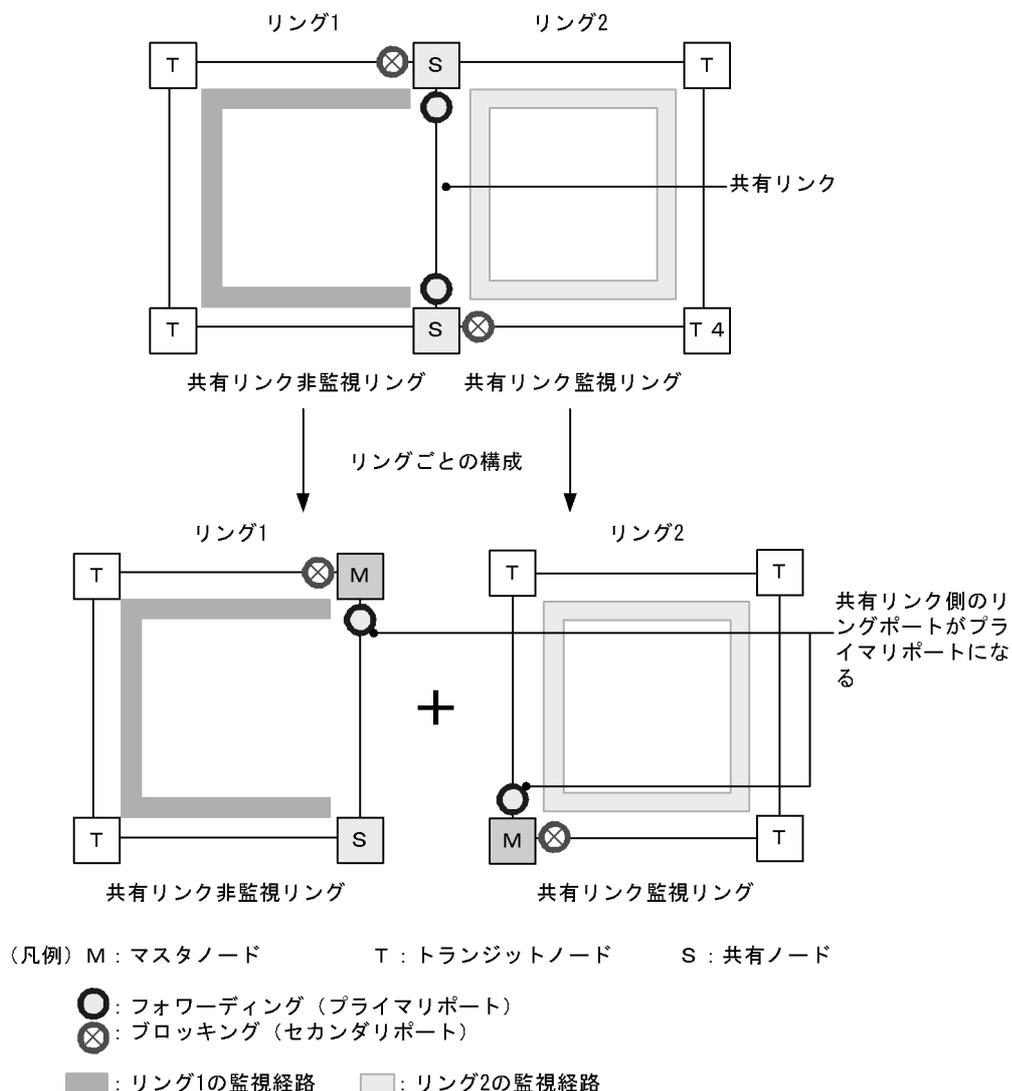


(凡例) M : マスタノード      T : トランジットノード      S : 共有ノード

## 22.5.5 共有ノードでのノード種別混在構成

共有リンクありのマルチリング構成で、共有リンクの両端に位置するノードをマスタノードとして動作させることができます。この場合、マスタノードのプライマリポートは、データ転送用の VLAN グループによらず、必ず共有リンク側のリングポートになります。このため、本構成では、データ転送用の VLAN グループを二つ設定したことによる負荷分散は実現できません。

図 22-23 共有ノードをマスタノードとした場合のポート状態



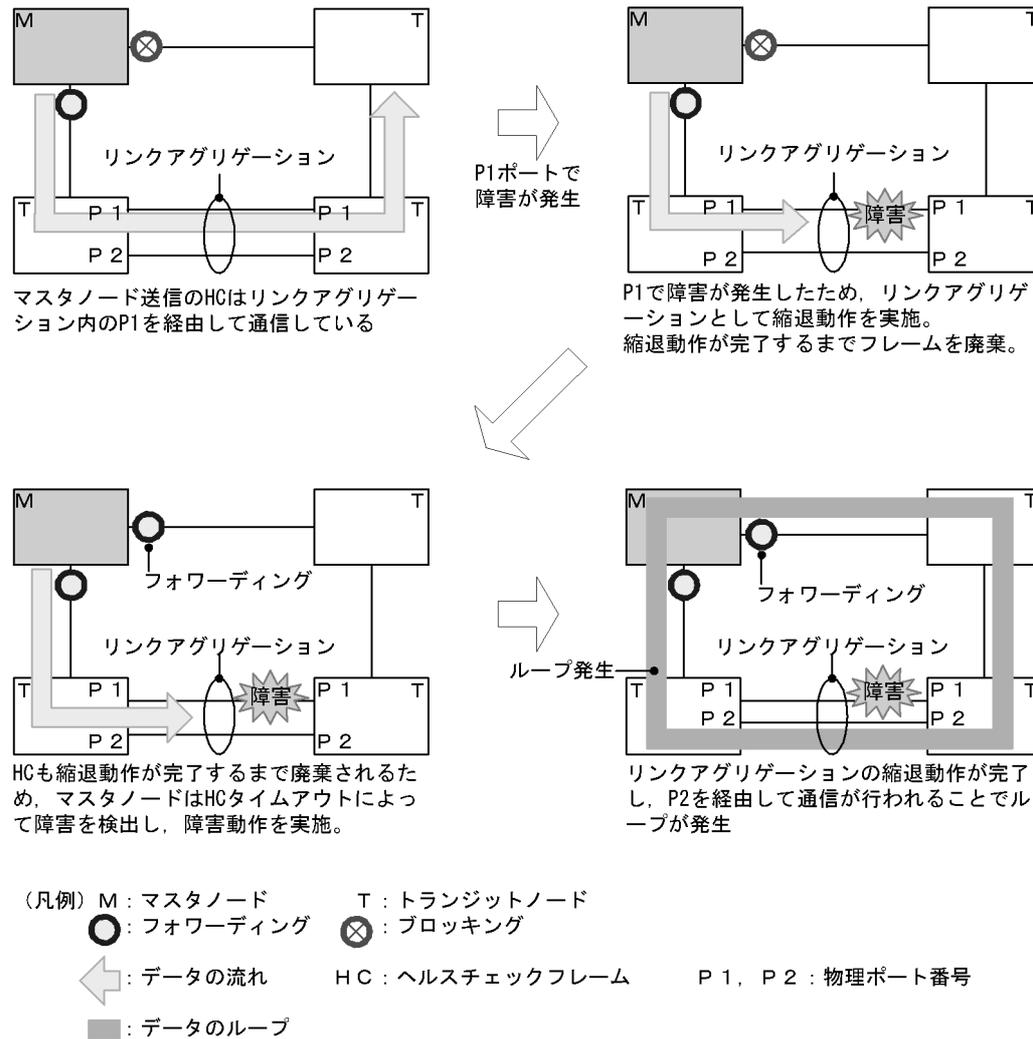
## 22.5.6 リンクアグリゲーションを用いた場合の障害監視時間の設定

リングポートをリンクアグリゲーションで構成した場合に、ヘルスチェックフレームが転送されているリンクアグリゲーション内のポートに障害が発生すると、リンクアグリゲーションの切り替えまたは縮退動作が完了するまでの間、制御フレームが廃棄されてしまいます。このため、マスタノードの障害監視時間 (health-check holdtime) がリンクアグリゲーションの切り替えまたは縮退動作が完了する時間よりも短いと、マスタノードがリングの障害を誤検出し、経路の切り替えを行います。この結果、ループが発生するおそれがあります。

リングポートをリンクアグリゲーションで構成した場合は、マスタノードの障害監視時間をリンクアグリゲーションによる切り替えまたは縮退動作が完了する時間よりも大きくする必要があります。

なお、LACP によるリンクアグリゲーションを使用する場合は、LACPDU の送信間隔の初期値が long (30 秒) となっていますので、初期値を変更しないまま運用すると、ループが発生するおそれがあります。LACP によるリンクアグリゲーションを使用する際は、LACPDU の送信間隔を short (1 秒) に設定してください。

図 22-24 リンクアグリゲーション使用時の障害検出



### 22.5.7 IEEE802.3ah/UDLD 機能との併用

本プロトコルでは、片方向リンク障害での障害の検出および切り替え動作は実施しません。片方向リンク障害発生時にも切り替え動作を実施したい場合は、IEEE802.3ah/UDLD 機能を併用してください。リング内のノード間を接続するリングポートに対して IEEE802.3ah/UDLD 機能の設定を行います。IEEE802.3ah/UDLD 機能によって、片方向リンク障害が検出されると、該当ポートを閉塞します。これによって、該当リングを監視するマスターノードはリング障害を検出し、切り替え動作を行います。

### 22.5.8 リンクダウン検出タイマおよびリンクアップ検出タイマとの併用

リングポートに使用しているポート（物理ポートまたはリンクアグリゲーションに属する物理ポート）のリンク状態が不安定な場合、マスターノードがリング障害やリング障害復旧を連続で検出してリングネットワークが不安定な状態になり、ループや長時間の通信断が発生するおそれがあります。このような状態を防ぐには、リングポートに使用しているポートに対して、リンクダウン検出タイマおよびリンクアップ検出タイマを設定します。リンクダウン検出タイマおよびリンクアップ検出タイマの設定については、「15.2.5 リンクダウン検出タイマの設定」および「15.2.6 リンクアップ検出タイマの設定」を参照して

ください。

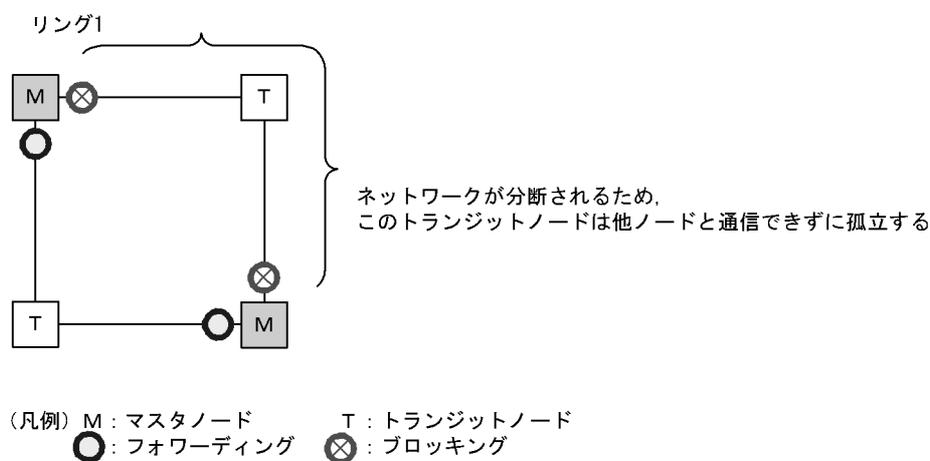
## 22.5.9 Ring Protocol の禁止構成

Ring Protocol を使用したネットワークでの禁止構成を次の図に示します。

### (1) 同一リング内に複数のマスタノードを設定

同一のリング内に 2 台以上のマスタノードを設定しないでください。同一リング内に複数のマスタノードがあると、セカンダリポートが論理ブロックされるためにネットワークが分断されてしまい、適切な通信ができなくなります。

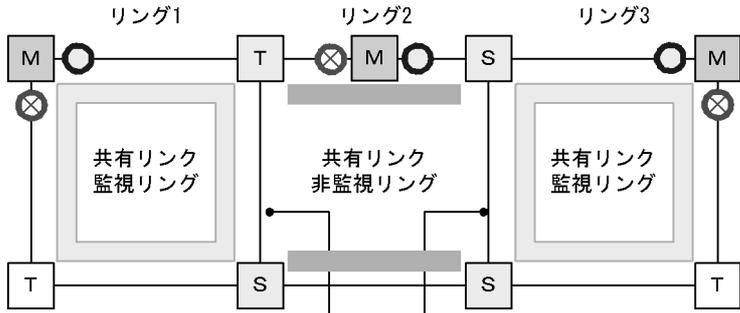
図 22-25 同一リング内に複数のマスタノードを設定



### (2) 共有リンク監視リングが複数ある構成

共有リンクありのマルチリング構成では、共有リンク監視リングはネットワーク内で必ず一つとなるように構成してください。共有リンク監視リングが複数あると、共有リンク非監視リングでの障害監視が分断されるため、正しい障害監視ができなくなります。

図 22-26 共有リンク監視リングが複数ある構成



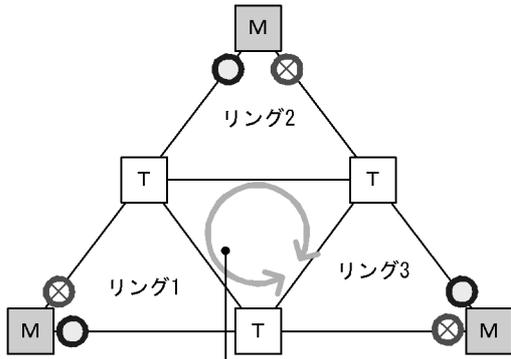
2箇所で分断されるため、共有リンク非監視リングの  
 マスタノードは正しく障害監視ができない。

(凡例) M : マスタノード      T : トランジットノード      S : 共有ノード  
 ○ : フォワーディング      ⊗ : ブロッキング  
 □ : リング1, 3の監視経路      ■ : リング2の監視経路

(3) ループになるマルチリング構成例

次に示す図のようなマルチリング構成を組むとトランジットノード間でループ構成となります。

図 22-27 ループになるマルチリング構成



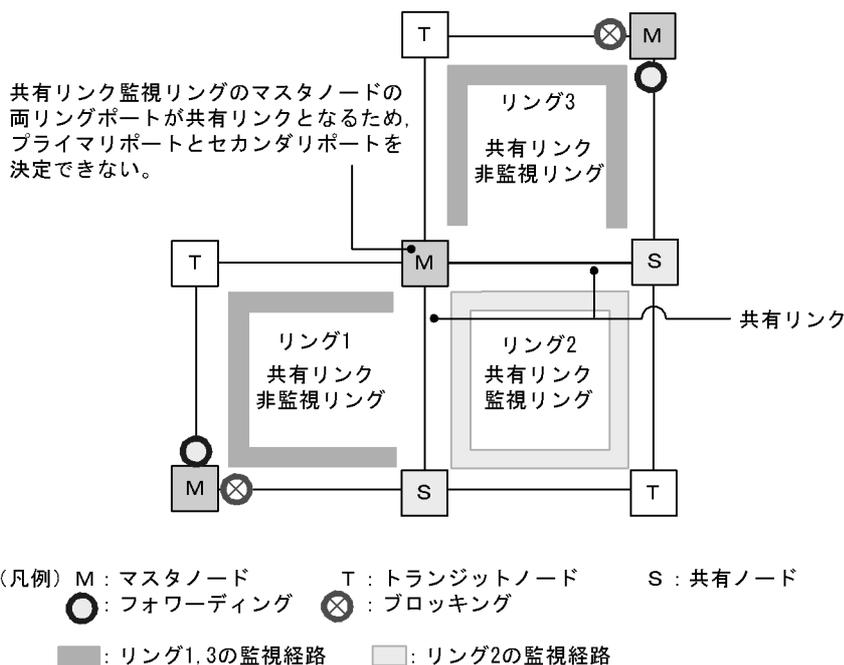
各リングのトランジットノード間でループになる

(凡例) M : マスタノード      T : トランジットノード  
 ○ : フォワーディング      ⊗ : ブロッキング

(4) マスタノードのプライマリポートが決定できない構成

次の図のように、二つの共有リンク非監視リングの最終端に位置するノードにマスタノードを設定しないでください。このような構成の場合、マスタノードの両リングポートが共有リンクとなるため、プライマリポートを正しく決定できません。

図 22-28 マスタノードのプライマリポートが決定できない構成



## 22.5.10 リングポートにリンクアグリゲーションを使用する場合について

リングポートにリンクアグリゲーションを使用する場合、リンクアグリゲーションを使用できるリングポートの最大数はチャンネルグループに集約されるポートの数によって決定します。

リンクアグリゲーションを使用できるリングポートの数は、次の式から算出できます。算出結果が 81 以上の場合は、リンクアグリゲーションを使用できるリングポート数を超過しています。

$$A \times 18 + B \times 8 + C \times 6 + D \times 4 + E \times 2 + F \times 1 < 81$$

A : 集約されるポート数が 11 ~ 16 のリンクアグリゲーションを使用したリングポート数

B : 集約されるポート数が 9 ~ 10 のリンクアグリゲーションを使用したリングポート数

C : 集約されるポート数が 7 ~ 8 のリンクアグリゲーションを使用したリングポート数

D : 集約されるポート数が 5 ~ 6 のリンクアグリゲーションを使用したリングポート数

E : 集約されるポート数が 3 ~ 4 のリンクアグリゲーションを使用したリングポート数

F : 集約されるポート数が 1 ~ 2 のリンクアグリゲーションを使用したリングポート数

次に算出例を示します。

### (1) リンクアグリゲーションをリングポートに使用する適切な例

- 集約されるポート数が 4 個のリンクアグリゲーションを 32 個のリングポートに使用した場合

$$\text{算出結果} : 32 \times 2 = 64$$

- 集約されるポート数が 8 個のリンクアグリゲーションを 12 個のリングポートに、集約されるポート数が 4 個のリンクアグリゲーションを 4 個のリングポートに使用した場合

$$\text{算出結果} : 12 \times 6 + 4 \times 2 = 80$$

### (2) リンクアグリゲーションをリングポートに使用する不適切な例

- 集約されるポート数が 16 個のリンクアグリゲーションを 6 個のリングポートに使用した場合

算出結果： $6 \times 18 = 108$

- 集約されるポート数が 8 個のリンクアグリゲーションを 8 個のリングポートに、集約されるポート数が 4 個のリンクアグリゲーションを 24 個のリングポートに使用した場合

算出結果： $8 \times 6 + 24 \times 2 = 96$

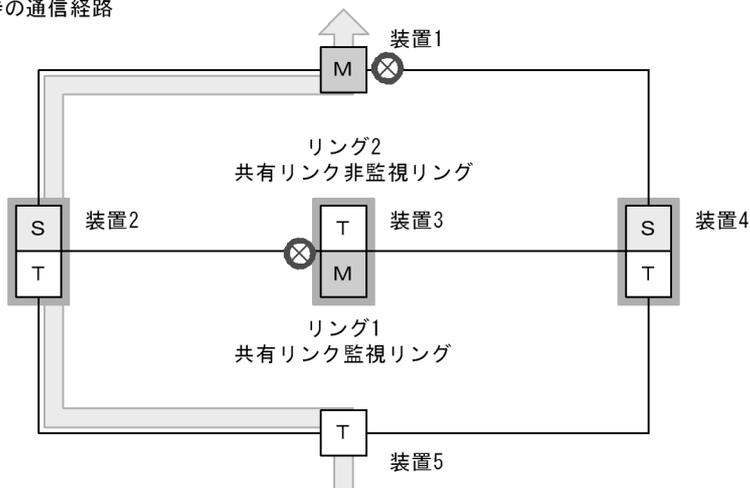
### 22.5.11 マスタノードの両リングポートが共有リンクとなる構成

次の図のように両リングポートが共有リンクとなるマスタノード（リング 1 の装置 3）が存在する共有リンクありのマルチリング構成では、共有リンク非監視リングのマスタノード（リング 2 の装置 1）に、コンフィグレーションコマンド `flush-request-transmit vlan` で隣接リング用フラッシュ制御フレームを送信する設定をしてください。

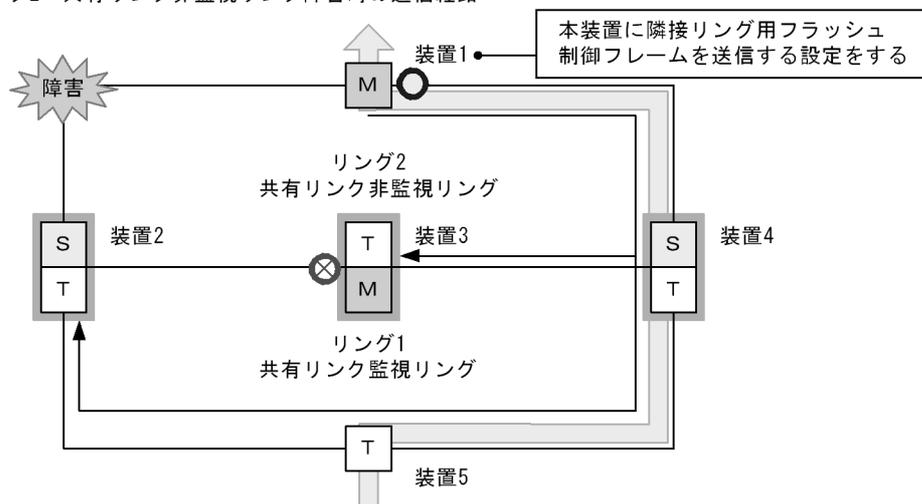
この設定によって、共有リンク非監視リングでリング障害が発生するとマスタノードは隣接するリングを構成する装置（以降、隣接リング構成装置）に隣接リング用フラッシュ制御フレームを送信するため、すぐに新しい通信経路に切り替えられます。なお、共有リンク非監視リングのリング障害が復旧した場合も同様になります。

図 22-29 マスタノードの両リングポートが共有リンクとなる構成例

## ● 正常時の通信経路



## ● リング2 共有リンク非監視リング障害時の通信経路



(凡例) M : マスタノード      T : トランジットノード  
 S : 共有リンクの最終端ノード (トランジットノード)      □ : 共有ノード  
 ○ : フォワーディング      ⊗ : ブロッキング      ← : 隣接リング用フラッシュ制御フレーム  
 ← : データの流れ

このような構成で隣接リング用フラッシュ制御フレームを送信する設定をしない場合、共有リンク非監視リングでリング障害が発生すると、共有リンク非監視リングでは経路の切り替えが実施されますが、隣接する共有リンク監視リングでは実施されません。この結果、共有リンク監視リングを構成する装置では古いMACアドレス学習の情報が残るため、すぐに新しい通信経路に切り替わらないおそれがあります。また、共有リンク非監視リングのリング障害が復旧した場合も同様になります。

## 22.6 Ring Protocol 使用時の注意事項

### (1) 運用中のコンフィグレーション変更について

運用中に、Ring Protocol の次に示すコンフィグレーションを変更する場合は、ループ構成にならないように注意が必要です。

- Ring Protocol 機能の停止 (disable コマンド)
- 動作モード (mode コマンド) の変更および属性 (ring-attribute パラメータ) の変更
- 制御 VLAN (control-vlan コマンド) の変更および制御 VLAN に使用している VLAN ID (vlan コマンド, switchport trunk コマンド, state コマンド) の変更
- データ転送用 VLAN (axrp vlan-mapping コマンド, vlan-group コマンド) の変更
- プライマリポート (axrp-primary-port コマンド) の変更
- 共有リンク監視リングのマスタノードが動作している装置に、共有リンク非監視リングの最終端ノードを追加 (動作モードの属性に rift-ring-edge パラメータ指定のあるリングを追加)

これらのコンフィグレーションは、次の手順で変更することを推奨します。

1. コンフィグレーションを変更する装置のリングポート、またはマスタノードのセカンダリポートを shutdown コマンドなどでダウン状態にします。
2. コンフィグレーションを変更する装置の Ring Protocol 機能を停止 (disable コマンド) します。
3. コンフィグレーションを変更します。
4. Ring Protocol 機能の停止を解除 (no disable コマンド) します。
5. 事前にダウン状態としたリングポートをアップ (shutdown コマンドなどの解除) します。

### (2) 他機能との共存

「17.3 レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

### (3) 制御 VLAN に使用する VLAN について

- Ring Protocol の制御フレームは Tagged フレームになります。このため、制御 VLAN に使用する VLAN は、トランクポートの allowed vlan (ネイティブ VLAN は不可) に設定してください。
- Tag 変換によって、制御 VLAN に使用する VLAN を異なる VLAN ID に変換すると、正常に障害・復旧検出ができなくなります。制御 VLAN に対して、Tag 変換は設定しないでください。

### (4) トランジットノードのリング VLAN 状態について

トランジットノードでは、装置またはリングポートが障害となり、その障害が復旧した際、ループの発生を防ぐために、リングポートのリング VLAN 状態はブロッキング状態となります。このブロッキング状態解除の契機の一つとして、フラッシュ制御フレーム受信待ち保護時間 (forwarding-shift-time) のタイムアウトがあります。このとき、フラッシュ制御フレーム受信待ち保護時間 (forwarding-shift-time) がマスタノードのヘルスチェック送信間隔 (health-check interval) よりも短い場合、マスタノードがリング障害の復旧を検出して、セカンダリポートをブロッキング状態に変更するよりも先に、トランジットノードのリングポートがフォワーディング状態となることがあり、ループが発生するおそれがあります。したがって、フラッシュ制御フレーム受信待ち保護時間 (forwarding-shift-time) はヘルスチェック送信間隔 (health-check interval) より大きい値を設定してください。

### (5) 共有リンクありのマルチリングでの VLAN 構成について

複数のリングで共通に使用する共有リンクでは、それぞれのリングで同じ VLAN を使用する必要があります。共有リンク間での VLAN のポートのフォワーディング/ブロッキング制御は共有リンク監視リングで

行います。このため、共有リンク監視/非監視リングで異なる VLAN を使用すると、共有リンク非監視リングで使用している VLAN はブロッキングのままとなり、通信ができなくなります。

## (6) Ring Protocol 使用時のネットワーク構築について

### (a) リングネットワークを構築してから、Ring Protocol を動作させる場合

Ring Protocol を利用するネットワークはループ構成となります。ネットワークの構築時は、次に示すような対応を行いループを防止してください。

- 事前に、リング構成ノードのリングポート（物理ポートまたはチャネルグループ）を shutdown コマンドなどでダウン状態にしてください。
- Ring Protocol のコンフィグレーション設定、または Ring Protocol の設定を含むコンフィグレーションファイルのコピー（copy コマンド）をして、Ring Protocol を有効にしてください。
- ネットワーク内のすべての装置に Ring Protocol の設定が完了した時点でリングポートをアップ（shutdown コマンドなどの解除）してください。

### (b) Ring Protocol が動作している装置を順次接続して、リングネットワークを構築する場合

リングネットワークの構築が完了していない状態でマスタノードのセカンダリポートを他装置と接続した場合、セカンダリポートがリンクアップしてもブロッキング状態を維持するため、該当ポートを使用した通信はできません。このため、次に示すどれかの方法でリングネットワークを構築してください。

- リングネットワークを構成するすべてのトランジットノードの接続が完了したあと、マスタノードを接続してください。
- リングネットワークを構築するときに、最初にマスタノードを接続する場合は、プライマリポート側からトランジットノードを接続してください。そして、すべてのトランジットノードの接続が完了したあと、マスタノードのセカンダリポートを接続してください。
- フォワーディング状態に遷移するまでの保護時間として、コンフィグレーションコマンド forwarding-shift-time で「infinity」以外の値をマスタノードに設定してください。また、リングネットワークの構築が完了したあと、この保護時間（forwarding-shift-time コマンドでの設定値）は、マスタノードでのヘルスチェックフレームの送信間隔（health-check interval コマンドでの設定値）よりも大きい値を設定してください。小さい場合、一時的にループの発生するおそれがあるため、設定値は十分に考慮してください。
- リングネットワークを構築するときに、最初にマスタノードを接続し、セカンダリポート側からトランジットノードを接続する場合は、次の手順で実施してください。
  1. マスタノードのプライマリポートでは、接続時にダウン状態となるように、shutdown コマンドを実行します。
  2. マスタノードの Ring Protocol 機能を停止（disable コマンド）します。
  3. すべてのトランジットノードを接続します。
  4. マスタノードの Ring Protocol 機能の停止を解除（no disable コマンド）します。
  5. ダウン状態としていたマスタノードのプライマリポートをアップ（no shutdown コマンド）します。

## (7) ヘルスチェックフレームの送信間隔と障害監視時間について

障害監視時間（health-check holdtime）は送信間隔（health-check interval）より大きな値を設定してください。送信間隔よりも小さな値を設定すると、受信タイムアウトとなり障害を誤検出します。また、障害監視時間と送信間隔はネットワーク構成などを十分に考慮した値を設定してください。障害監視時間は送信間隔の2倍以上を目安として設定することを推奨します。2倍未満に設定すると、ヘルスチェックフレームの受信が1回失敗した状態で障害を検出することがあるため、ネットワークの負荷などによって遅延が発生した場合に障害を誤検出するおそれがあります。

## (8) 相互運用

Ring Protocol は、本装置独自仕様の機能です。他社スイッチとは相互運用できません。

## (9) リングを構成する装置について

Ring Protocol を用いたネットワーク内で、本装置間に Ring Protocol をサポートしていない他社スイッチや伝送装置などを設置した場合、本装置のマスタノードが送信するフラッシュ制御フレームを解釈できないため、即時に MAC アドレステーブルエントリがクリアされません。その結果、通信経路の切り替え（もしくは切り戻し）前の情報に従ってデータフレームの転送が行われるため、正しくデータが届かないおそれがあります。

## (10) マスタノード障害時について

マスタノードが装置障害などによって通信できない状態になると、リングネットワークの障害監視が行われなくなります。このため、迂回経路への切り替えは行われず、マスタノード以外のトランジットノード間の通信はそのまま継続されます。また、マスタノードが装置障害から復旧する際には、フラッシュ制御フレームをリング内のトランジットノードに向けて送信します。このため、一時的に通信が停止するおそれがあります。

## (11) ネットワーク内の多重障害時について

同一リング内の異なるノード間で 2 箇所以上の障害が起きた場合（多重障害）、マスタノードは既に 1 箇所目の障害で障害検出を行っているため、2 箇所目以降の障害を検出しません。また、多重障害での復旧検出についても、最後の障害が復旧するまでマスタノードが送信しているヘルスチェックフレームを受信できないため、復旧を検出できません。その結果、多重障害のうち、一部の障害が復旧した（リングとして障害が残っている状態）ときには一時的に通信できないことがあります。

## (12) リングポートに指定したリンクアグリゲーションのダウンについて

リングネットワークを構成するノード間をリンクアグリゲーション（スタティックモードまたは LACP モード）で接続していた場合、リンクアグリゲーションの該当チャンネルグループを shutdown コマンドでダウン状態にするときは、あらかじめチャンネルグループに属するすべての物理ポートを shutdown コマンドでダウン状態に設定してください。

なお、該当チャンネルグループを no shutdown コマンドでアップ状態にするときは、あらかじめチャンネルグループに属するすべての物理ポートを shutdown コマンドでダウン状態に設定してください。

## (13) VLAN のダウンを伴う障害発生時の経路の切り替えについて

マスタノードのプライマリポートでリンクダウンなどの障害が発生すると、データ転送用の VLAN グループに設定されている VLAN が一時的にダウンする場合があります。このような場合、経路の切り替えによる通信の復旧に時間がかかることがあります。

なお、VLAN debounce 機能を使用することで VLAN のダウンを回避できる場合があります。VLAN debounce 機能の詳細については、「20.7 VLAN debounce 機能の解説」を参照してください。

## (14) ネットワーク負荷の高い環境での運用について

トランジットノードで、定常的またはバースト的に、リングポートに高負荷のトラフィックが流れると、Ring Protocol の制御フレームの破棄または遅延が発生し、マスタノードで障害を誤検出するおそれがあります。上記の環境に当てはまる場合には、次の対応を行ってください。

- Ring Protocol のパラメータ値の調整による対応の場合

ヘルスチェックフレームの送信間隔 (health-check interval), および障害監視時間 (health-check holdtime) を環境に合わせて調整して運用してください。

- フロー制御の設定による対応の場合  
次のどれかを条件とした MAC QoS フローリストを用いて, Ring Protocol の制御フレームに対する優先制御を設定し運用してください。詳細については, 「コンフィグレーションガイド Vol.2 5.10 優先度決定の解説」を参照してください。
- Ring Protocol の制御フレームに使用している宛先 MAC アドレス (0112.E2E0.0F00 ~ 0112.E2E0.0F0F) を条件とする。
- Ring Protocol の制御フレームに使用している EtherType 値 (0x88f3), または EtherType 名称 (axp) を条件とする。
- Ring Protocol の制御 VLAN に使用している VLAN ID を条件とする。

### (15) リングポートに対する回線テストの実行について

リングポートに対して回線テスト (運用コマンド test interfaces) を実行する場合は, 次の手順で実施してください。この手順で実施しない場合, 回線テスト終了後に一時的にループが発生するおそれがあります。

1. 運用コマンド deactivate でテスト対象のリングポートを inactive 状態にします。  
マスタノードはリング障害を検出し, 通信経路を切り替えます。
2. 該当ポートに対して, 回線テストを実行します。
3. 回線テスト終了後, 運用コマンド activate でリングポートを復旧させます。  
マスタノードはリング障害の復旧を検出し, 通信経路を切り戻します。

### (16) VLAN のダウンを伴うコンフィグレーションコマンドの設定について

Ring Protocol に関するコンフィグレーションコマンドが設定されていない状態で, 一つ目の Ring Protocol に関するコンフィグレーションコマンド (次に示すどれかのコマンド) を設定した場合に, すべての VLAN が一時的にダウンします。そのため, Ring Protocol を用いたリングネットワークを構築する場合には, あらかじめ次に示すコンフィグレーションコマンドを設定しておくことを推奨します。

- axrp
- axrp vlan-mapping
- axrp-ring-port
- axrp-primary-port
- axrp virtual-link

なお, VLAN マッピング (axrp vlan-mapping コマンド) については, 新たに追加設定した場合でも, その VLAN マッピングに関連づけられる VLAN が一時的にダウンします。すでに設定されている VLAN マッピング, およびその VLAN マッピングに関連づけられているその他の VLAN には影響ありません。

### (17) マスタノードの装置起動時のフラッシュ制御フレーム送受信について

マスタノードの装置起動時に, トランジットノードがマスタノードと接続されているリングポートのリンクアップをマスタノードよりも遅く検出すると, マスタノードが初期動作時に送信するフラッシュ制御フレームを受信できない場合があります。このとき, フラッシュ制御フレームを受信できなかったトランジットノードのリングポートはブロッキング状態となります。該当するリングポートはフラッシュ制御フレーム受信待ち保護時間 (forwarding-shift-time) が経過するとフォワーディング状態となり, 通信が復旧します。

隣接するトランジットノードでフラッシュ制御フレームを受信できない場合には, マスタノードのフラッ

シユ制御フレームの送信回数を調節すると、受信できることがあります。また、フラッシュ制御フレーム未受信による通信断の時間を短縮したい場合は、トランジットノードのフラッシュ制御フレーム受信待ち保護時間（初期値：10 秒）を短くしてください。

なお、次の場合も同様です。

- VLAN プログラムの再起動（運用コマンド restart vlan の実行）
- コンフィグレーションファイルの運用への反映（運用コマンド copy の実行）
- 1 枚目の BSU アップ（運用コマンド activate bsu の実行）【AX6700S】

#### (18) 経路切り戻し抑止機能適用時のフラッシュ制御フレーム受信待ち保護時間の設定について

経路切り戻し抑止機能を動作させる場合、トランジットノードでのフラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）には infinity を指定するか、または経路切り戻し抑止時間（preempt-delay）よりも大きな値を指定してください。経路切り戻し抑止中、トランジットノードでのフラッシュ制御フレーム受信待ち保護時間がタイムアウトして該当リングポートの論理ブロックを解除してしまうと、マスタノードはセカンダリポートの論理ブロック状態を解除しているため、ループが発生するおそれがあります。

#### (19) Ring Protocol と VRF 機能の併用について【OP-NPAR】

Ring Protocol と VRF 機能を併用する（コンフィグレーションコマンド vrf mode の axrp-enable パラメータ、または axrp-enable-ipv4-ipv6 パラメータを設定している）場合、次の点に注意してください。

- Ring Protocol の制御 VLAN を IP インタフェースとして使用しないでください。IP インタフェースとして使用した場合、リング状態を正常に監視できません。
- Ring Protocol のデータ転送用 VLAN を設定できる VLAN マッピング ID の範囲は 1 ~ 64 となります。グローバルネットワークの IP インタフェースとして使用する VLAN は、VLAN マッピング ID 1 に設定してください。

また、VRF の IP インタフェースとして使用する VLAN は、VLAN マッピング ID 2 ~ 64 に設定し、VRF ID と VLAN マッピング ID を一致させてください。

なお、この条件に一致していない場合、該当 VLAN で通信ができません。

# 23 Ring Protocol の設定と運用

この章では , Ring Protocol の設定例について説明します。

---

23.1 コンフィグレーション

---

23.2 オペレーション

---

## 23.1 コンフィグレーション

Ring Protocol 機能が動作するためには、axrp、axrp vlan-mapping、mode、control-vlan、vlan-group、axrp-ring-port の設定が必要です。すべてのノードについて、構成に即したコンフィグレーションを設定してください。

### 23.1.1 コンフィグレーションコマンド一覧

Ring Protocol のコンフィグレーションコマンド一覧を次の表に示します。

表 23-1 コンフィグレーションコマンド一覧

| コマンド名                       | 説明                                                        |
|-----------------------------|-----------------------------------------------------------|
| axrp                        | リング ID を設定します。                                            |
| axrp vlan-mapping           | VLAN マッピング、およびそのマッピングに参加する VLAN を設定します。                   |
| axrp-primary-port           | プライマリポートを設定します。                                           |
| axrp-ring-port              | リングポートを設定します。                                             |
| control-vlan                | 制御 VLAN として使用する VLAN を設定します。                              |
| disable                     | Ring Protocol 機能を無効にします。                                  |
| flush-request-count         | フラッシュ制御フレームを送信する回数を設定します。                                 |
| flush-request-transmit vlan | 隣接するリング構成の装置に対して、隣接リング用フラッシュ制御フレームを送信する VLAN を設定します。      |
| forwarding-shift-time       | フラッシュ制御フレームの受信待ちを行う保護時間を設定します。                            |
| health-check holdtime       | ヘルスチェックフレームの保護時間を設定します。                                   |
| health-check interval       | ヘルスチェックフレームの送信間隔を設定します。                                   |
| mode                        | リングでの動作モードを設定します。                                         |
| name                        | リングを識別するための名称を設定します。                                      |
| preempt-delay               | 経路切り戻し抑止機能を有効にして抑止時間を設定します。                               |
| vlan-group                  | Ring Protocol 機能で運用する VLAN グループ、および VLAN マッピング ID を設定します。 |

### 23.1.2 Ring Protocol 設定の流れ

Ring Protocol 機能を正常に動作させるには、構成に合った設定が必要です。設定の流れを次に示します。

#### (1) スパニングツリーの停止

Ring Protocol を使用する場合には、事前にスパニングツリーを停止することを推奨します。ただし、本装置で Ring Protocol とスパニングツリーを併用するときは、停止する必要はありません。スパニングツリーの停止については、「21 スパニングツリー」を参照してください。

#### (2) Ring Protocol 共通の設定

リングの構成、またはリングでの本装置の位置づけに依存しない共通の設定を行います。

- リング ID
- 制御 VLAN
- VLAN マッピング

- VLAN グループ

### (3) モードとポートの設定

リングの構成，またはリングでの本装置の位置づけに応じた設定を行います。設定の組み合わせに矛盾がある場合，Ring Protocol 機能は正常に動作しません。

- モード
- リングポート

### (4) 各種パラメータ設定

Ring Protocol 機能は，次に示すコンフィギュレーションの設定がない場合，初期値で動作します。値を変更したい場合はコマンドで設定してください。

- 機能の無効化
- ヘルスチェックフレーム送信間隔
- ヘルスチェックフレーム受信待ち保護時間
- フラッシュ制御フレーム受信待ち保護時間
- フラッシュ制御フレーム送信回数
- プライマリポート
- 経路切り戻し抑止機能の有効化および抑止時間

## 23.1.3 リング ID の設定

#### [ 設定のポイント ]

リング ID を設定します。同じリングに属する装置にはすべて同じリング ID を設定する必要があります。

#### [ コマンドによる設定 ]

1. (config)# axrp 1  
リング ID 1 を設定します。

## 23.1.4 制御 VLAN の設定

### (1) 制御 VLAN の設定

#### [ 設定のポイント ]

制御 VLAN として使用する VLAN を指定します。データ転送用 VLAN に使われている VLAN は使用できません。また，異なるリングで使われている VLAN ID と同じ値の VLAN ID は使用できません。

#### [ コマンドによる設定 ]

1. (config)# axrp 1  
リング ID 1 の axrp コンフィギュレーションモードに移行します。
2. (config-axrp)# control-vlan 2  
制御 VLAN として VLAN2 を指定します。

## (2) 制御 VLAN のフォワーディング遷移時間の設定

### [ 設定のポイント ]

Ring Protocol が初期状態の場合に、トランジットノードでの制御 VLAN のフォワーディング遷移時間を設定します。それ以外のノードでは、本設定を実施しても無効となります。トランジットノードでの制御 VLAN のフォワーディング遷移時間 ( forwarding-delay-time パラメータでの設定値 ) は、マスタノードでのヘルスチェックフレームの保護時間 ( health-check holdtime コマンドでの設定値 ) よりも大きな値を設定してください。

### [ コマンドによる設定 ]

1. (config)# axrp 1  
(config-axrp)# control-vlan 2 forwarding-delay-time 10  
制御 VLAN のフォワーディング遷移時間を 10 秒に設定します。

## 23.1.5 VLAN マッピングの設定

### (1) VLAN 新規設定

#### [ 設定のポイント ]

データ転送用に使用する VLAN を VLAN マッピングに括り付けます。一つの VLAN マッピングを共通定義として複数のリングで使用できます。設定できる VLAN マッピングの最大数は 128 個です。VLAN マッピングに設定する VLAN はリストで複数指定できます。リングネットワーク内で使用するデータ転送用 VLAN は、すべてのノードで同じにする必要があります。ただし、VLAN グループに指定した VLAN マッピングの VLAN が一致していればよいので、リングネットワーク内のすべてのノードで VLAN マッピング ID を一致させる必要はありません。

#### [ コマンドによる設定 ]

1. (config)# axrp vlan-mapping 1 vlan 5-7  
VLAN マッピング ID 1 に、VLAN ID 5, 6, 7 を設定します。

### (2) VLAN 追加

#### [ 設定のポイント ]

設定済みの VLAN マッピングに対して、VLAN ID を追加します。追加した VLAN マッピングを適用したリングが動作中の場合には、すぐに反映されます。また、複数のリングで適用されている場合には、同時に反映されます。リング運用中に VLAN マッピングを変更すると、ループが発生することがあります。

#### [ コマンドによる設定 ]

1. (config)# axrp vlan-mapping 1 vlan add 8-10  
VLAN マッピング ID 1 に VLAN ID 8, 9, 10 を追加します。

### (3) VLAN 削除

#### [ 設定のポイント ]

設定済みの VLAN マッピングから、VLAN ID を削除します。削除した VLAN マッピングを適用した

リングが動作中の場合には、すぐに反映されます。また、複数のリングで適用されている場合には、同時に反映されます。リング運用中に VLAN マッピングを変更すると、ループが発生することがあります。

[ コマンドによる設定 ]

1. (config)# axrp vlan-mapping 1 vlan remove 8-9  
VLAN マッピング ID 1 から VLAN ID 8, 9 を削除します。

## 23.1.6 VLAN グループの設定

[ 設定のポイント ]

VLAN グループに VLAN マッピングを割り当てることによって、VLAN ID を Ring Protocol で使用する VLAN グループに所属させます。VLAN グループは一つのリングに最大二つ設定できます。VLAN グループには、リスト指定によって最大 128 個の VLAN マッピング ID を設定できます。

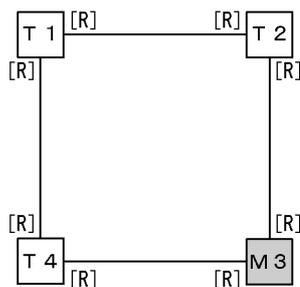
[ コマンドによる設定 ]

1. (config)# axrp 1  
(config-axrp)# vlan-group 1 vlan-mapping 1  
VLAN グループ 1 に、VLAN マッピング ID 1 を設定します。

## 23.1.7 モードとリングポートに関する設定 (シングルリングと共有リンクなしマルチリング構成)

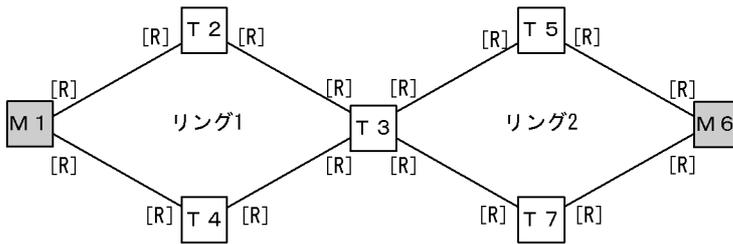
シングルリング構成を「図 23-1 シングルリング構成」に、共有リンクなしマルチリング構成を「図 23-2 共有リンクなしマルチリング構成」に示します。

図 23-1 シングルリング構成



(凡例) M : マスタノード      T : トランジットノード  
[R] : リングポート

図 23-2 共有リンクなしマルチリング構成



(凡例) M : マスタノード  
T : トランジットノード  
[R] : リングポート

シングルリング構成と共有リンクなしマルチリング構成での、マスタノード、およびトランジットノードに関するモードとリングポートの設定は同様になります。

### (1) マスタノード

#### [ 設定のポイント ]

リングでの本装置の動作モードをマスタモードに設定します。イーサネットインタフェースまたはポートチャンネルインタフェースをリングポートとして指定します。リングポートは一つのリングに対して二つ設定してください。「図 23-1 シングルリング構成」では M3 ノード、「図 23-2 共有リンクなしマルチリング構成」では M1 および M6 ノードがこれに該当します。

#### [ コマンドによる設定 ]

##### 1. (config)# axrp 2

```
(config-axrp)# mode master
```

リング ID 2 の動作モードをマスタモードに設定します。

##### 2. (config)# interface gigabitethernet 1/1

```
(config-if)# axrp-ring-port 2
```

```
(config-if)# interface gigabitethernet 1/2
```

```
(config-if)# axrp-ring-port 2
```

ポート 1/1 および 1/2 のインタフェースモードに移行し、該当するインタフェースをリング ID 2 のリングポートとして設定します。

### (2) トランジットノード

#### [ 設定のポイント ]

リングでの本装置の動作モードをトランジットモードに設定します。イーサネットインタフェースまたはポートチャンネルインタフェースをリングポートとして指定します。リングポートは一つのリングに対して二つ設定してください。「図 23-1 シングルリング構成」では T1, T2 および T4 ノード、「図 23-2 共有リンクなしマルチリング構成」では T2, T3, T4, T5 および T7 ノードがこれに該当します。

#### [ コマンドによる設定 ]

##### 1. (config)# axrp 2

```
(config-axrp)# mode transit
```

リング ID 2 の動作モードをトランジットモードに設定します。

```
2. (config)# interface gigabitethernet 1/1
 (config-if)# axrp-ring-port 2
 (config-if)# interface gigabitethernet 1/2
 (config-if)# axrp-ring-port 2
```

ポート 1/1 および 1/2 のインタフェースモードに移行し、該当するインタフェースをリング ID 2 のリングポートとして設定します。

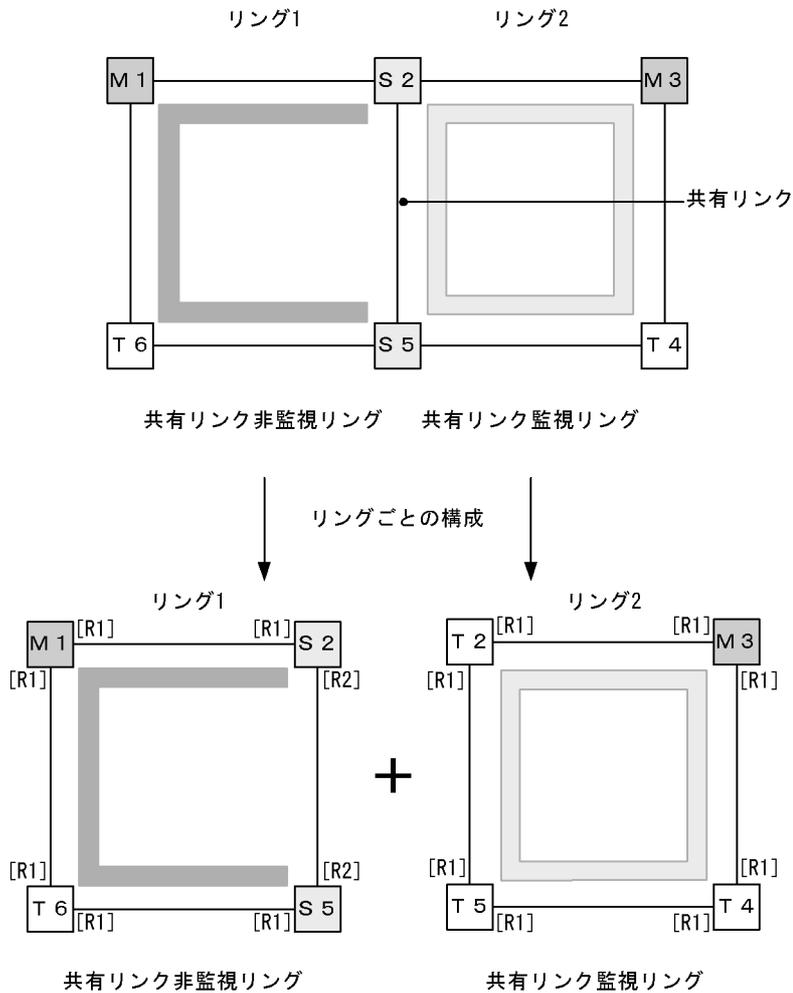
### 23.1.8 モードとリングポートに関する設定（共有リンクありマルチリング構成）

共有リンクありマルチリング構成について、モードとリングポートのパラメータ設定パターンを示します。

#### （1）共有リンクありマルチリング構成（基本構成）

共有リンクありマルチリング構成（基本構成）を次の図に示します。

図 23-3 共有リンクありマルチリング構成（基本構成）



(凡例) M : マスタノード                      T : トランジットノード                      S : 共有ノード  
 [R1] : リングポート  
 [R2] : リングポート (共有リンク非監視リング最終端ノードの共有リンク側ポート)  
 ■ : リング1の監視経路                      □ : リング2の監視経路

(a) 共有リンク監視リングのマスタノード

シングルリングのマスタノード設定と同様です。「23.1.7 モードとリングポートに関する設定 (シングルリングと共有リンクなしマルチリング構成) (1) マスタノード」を参照してください。「図 23-3 共有リンクありマルチリング構成 (基本構成)」では M3 ノードがこれに該当します。

(b) 共有リンク監視リングのトランジットノード

シングルリングのトランジットノード設定と同様です。「23.1.7 モードとリングポートに関する設定 (シングルリングと共有リンクなしマルチリング構成) (2) トランジットノード」を参照してください。「図 23-3 共有リンクありマルチリング構成 (基本構成)」では T2, T4 および T5 ノードがこれに該当します。

(c) 共有リンク非監視リングのマスタノード

[ 設定のポイント ]

リングでの本装置の動作モードをマスタモードに設定します。また、本装置が構成しているリングの属性、およびそのリングでの本装置の位置づけを共有リンク非監視リングに設定します。イーサネットインタフェースまたはポートチャネルインタフェースをリングポートとして指定します。リングポートは一つのリングに対して二つ設定してください。「図 23-3 共有リンクありマルチリング構成 (基本構成)」では M1 ノードがこれに該当します。

[ コマンドによる設定 ]

1. (config)# axrp 1

```
(config-axrp)# mode master ring-attribute rift-ring
```

リング ID 1 の動作モードをマスタモード、リング属性を共有リンク非監視リングに設定します。

2. (config)# interface gigabitethernet 1/1

```
(config-if)# axrp-ring-port 1
```

```
(config-if)# interface gigabitethernet 1/2
```

```
(config-if)# axrp-ring-port 1
```

ポート 1/1 および 1/2 のインタフェースモードに移行し、該当するインタフェースをリング ID 1 のリングポートとして設定します。

(d) 共有リンク非監視リングのトランジットノード

シングルリングのトランジットノード設定と同様です。「23.1.7 モードとリングポートに関する設定 (シングルリングと共有リンクなしマルチリング構成) (2) トランジットノード」を参照してください。「図 23-3 共有リンクありマルチリング構成 (基本構成)」では T6 ノードがこれに該当します。

(e) 共有リンク非監視リングの最終端ノード (トランジット)

[ 設定のポイント ]

リングでの本装置の動作モードをトランジットモードに設定します。また、本装置が構成しているリングの属性、およびそのリングでの本装置の位置づけを共有リンク非監視リングの最終端ノードに設定します。構成上二つ存在する共有リンク非監視リングの最終端ノードの区別にはエッジノード ID (1 または 2) を指定します。「図 23-3 共有リンクありマルチリング構成 (基本構成)」では S2 および S5 ノードがこれに該当します。リングポート設定は共有リンク側のポートにだけ shared-edge を指定します。「図 23-3 共有リンクありマルチリング構成 (基本構成)」では S2 および S5 ノードのリングポート [R2] がこれに該当します。

[ コマンドによる設定 ]

1. (config)# axrp 1

```
(config-axrp)# mode transit ring-attribute rift-ring-edge 1
```

リング ID 1 での動作モードをトランジットモード、リング属性を共有リンク非監視リングの最終端ノード、エッジノード ID を 1 に設定します。

2. (config)# interface gigabitethernet 1/1

```
(config-if)# axrp-ring-port 1
```

```
(config-if)# interface gigabitethernet 1/2
```

```
(config-if)# axrp-ring-port 1 shared-edge
```

ポート 1/1 および 1/2 のインタフェースモードに移行し、該当するインタフェースをリング ID 1 のリングポートとして設定します。このとき、ポート 1/2 を共有リンクとして shared-edge パラメータも設定します。

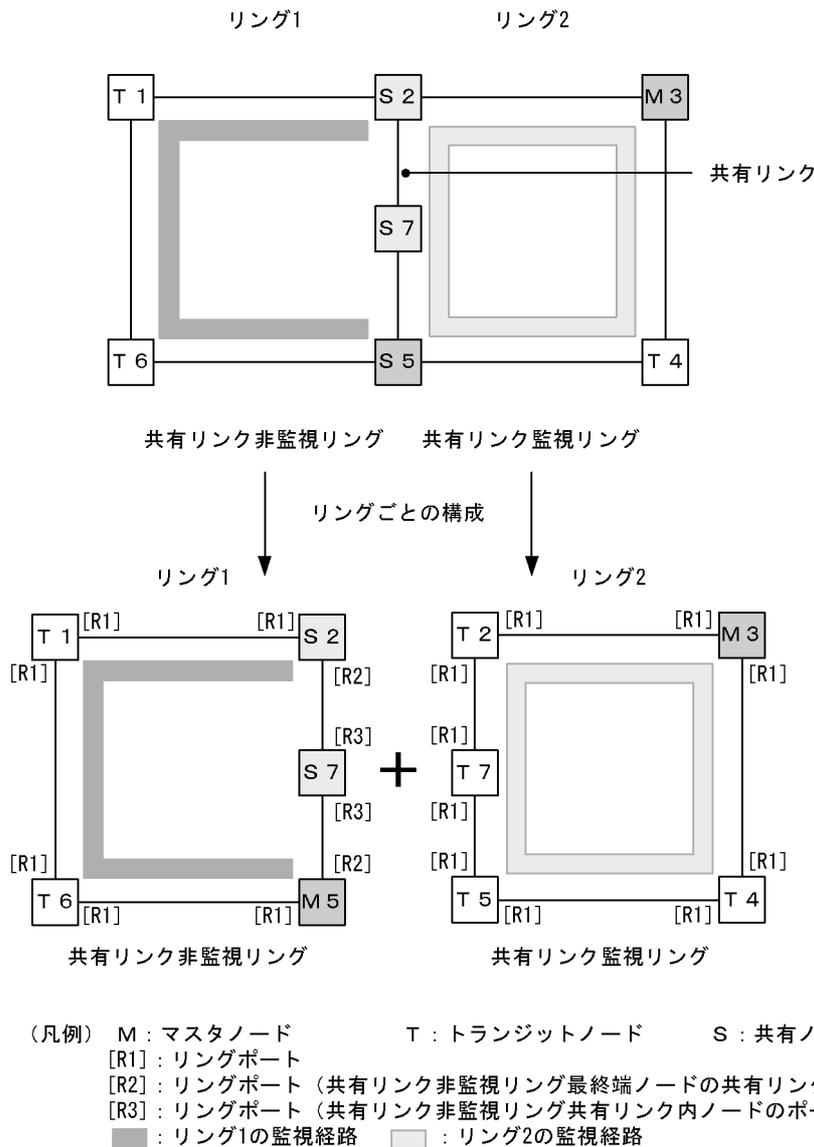
[ 注意事項 ]

エッジノード ID は、二つある共有リンク非監視リングの最終端ノードで他方と異なる ID を設定してください。

(2) 共有リンクありのマルチリング構成 ( 拡張構成 )

共有リンクありマルチリング構成 ( 拡張構成 ) を次の図に示します。共有リンク非監視リングの最終端ノード ( マスタノード ) および共有リンク非監視リングの共有リンク内ノード ( トランジット ) 以外の設定については、「(1) 共有リンクありマルチリング構成 ( 基本構成 )」を参照してください。

図 23-4 共有リンクありのマルチリング構成 ( 拡張構成 )



(a) 共有リンク非監視リングの最終端ノード ( マスタノード )

[ 設定のポイント ]

リングでの本装置の動作モードをマスタモードに設定します。また、本装置が構成しているリングの属性、およびそのリングでの本装置の位置づけを共有リンク非監視リングの最終端ノードに設定しま

す。構成上二つ存在する共有リンク非監視リングの最終端ノードの区別にはエッジノード ID (1 または 2) を指定します。「図 23-4 共有リンクありのマルチリング構成 (拡張構成)」では M5 ノードがこれに該当します。リングポート設定は共有リンク側のポートにだけ shared-edge を指定します。「図 23-4 共有リンクありのマルチリング構成 (拡張構成)」では M5 ノードのリングポート [R2] がこれに該当します。

[ コマンドによる設定 ]

1. (config)# axrp 1  
(config-axrp)# mode master ring-attribute rift-ring-edge 2  
リング ID 1 での動作モードをマスタモード、リング属性を共有リンク非監視リングの最終端ノード、エッジノード ID を 2 に設定します。
2. (config)# interface gigabitethernet 1/1  
(config-if)# axrp-ring-port 1  
(config-if)# interface gigabitethernet 1/2  
(config-if)# axrp-ring-port 1 shared-edge  
ポート 1/1 および 1/2 のインタフェースモードに移行し、該当するインタフェースをリング ID 1 のリングポートとして設定します。このとき、ポート 1/2 を共有リンクとして shared-edge パラメータも設定します。

[ 注意事項 ]

エッジノード ID は、二つある共有リンク非監視リングの最終端ノードで他方と異なる ID を設定してください。

(b) 共有リンク非監視リングの共有リンク内ノード (トランジット)

[ 設定のポイント ]

リングでの本装置の動作モードをトランジットモードに設定します。「図 23-4 共有リンクありのマルチリング構成 (拡張構成)」では S7 ノードがこれに該当します。リングポートは両ポート共に shared パラメータを指定し、共有ポートとして設定します。「図 23-4 共有リンクありのマルチリング構成 (拡張構成)」では S7 ノードのリングポート [R3] がこれに該当します。

[ コマンドによる設定 ]

1. (config)# axrp 1  
(config-axrp)# mode transit  
リング ID 1 の動作モードをトランジットモードに設定します。
2. (config)# interface gigabitethernet 1/1  
(config-if)# axrp-ring-port 1 shared  
(config-if)# interface gigabitethernet 1/2  
(config-if)# axrp-ring-port 1 shared  
ポート 1/1 および 1/2 のインタフェースモードに移行し、該当するインタフェースをリング ID 1 の共有リンクポートに設定します。

[ 注意事項 ]

1. 共有リンク監視リングの共有リンク内トランジットノードに shared 指定でポート設定をした場合、Ring Protocol 機能は正常に動作しません。

- 共有リンク非監視リングの共有リンク内で shared 指定したノードにマスタモードは指定できません。

## 23.1.9 各種パラメータの設定

### (1) Ring Protocol 機能の無効

[ 設定のポイント ]

コマンドを指定して Ring Protocol 機能を無効にします。ただし、運用中に Ring Protocol 機能を無効にすると、ネットワークの構成上、ループが発生するおそれがあります。このため、先に Ring Protocol 機能を動作させているインタフェースを shutdown コマンドなどで停止させてから、Ring Protocol 機能を無効にしてください。

[ コマンドによる設定 ]

1. (config)# axrp 1

```
(config-axrp)# disable
```

該当するリング ID 1 の axrp コンフィグレーションモードに移行します。disable コマンドを実行することで、Ring Protocol 機能が無効となります。

### (2) ヘルスチェックフレーム送信間隔

[ 設定のポイント ]

マスタノード、または共有リンク非監視リングの最終端ノードでのヘルスチェックフレームの送信間隔を設定します。それ以外のノードでは、本設定を実施しても、無効となります。

[ コマンドによる設定 ]

1. (config)# axrp 1

```
(config-axrp)# health-check interval 500
```

ヘルスチェックフレームの送信間隔を 500 ミリ秒に設定します。

[ 注意事項 ]

マルチリングの構成をとる場合、同一リング内のマスタノードと共有リンク非監視リングの最終端ノードでのヘルスチェックフレーム送信間隔は同じ値を設定してください。値が異なる場合、障害検出処理が正常に行われません。

### (3) ヘルスチェックフレーム受信待ち保護時間

[ 設定のポイント ]

マスタノードでのヘルスチェックフレームの受信待ち保護時間を設定します。それ以外のノードでは、本設定を実施しても、無効となります。受信待ち保護時間を変更することで、障害検出時間を調節できます。

受信待ち保護時間 (health-check holdtime コマンドでの設定値) は、送信間隔 (health-check interval コマンドでの設定値) よりも大きい値を設定してください。

[ コマンドによる設定 ]

1. (config)# axrp 1

```
(config-axrp)# health-check holdtime 1500
```

ヘルスチェックフレームの受信待ち保護時間を 1500 ミリ秒に設定します。

#### (4) フラッシュ制御フレーム受信待ち保護時間およびマスタノードのフォワーディング状態に遷移するまでの保護時間

##### [ 設定のポイント ]

トランジットノードの場合、フラッシュ制御フレームの受信待ち保護時間を設定します。この保護時間 (forwarding-shift-time コマンドでの設定値) は、マスタノードでのヘルスチェックフレームの送信間隔 (health-check interval コマンドでの設定値) よりも大きい値を設定してください。設定誤りからマスタノードが復旧を検出するよりも先にトランジットノードのリングポートがフォワーディング状態になってしまった場合、一時的にループが発生するおそれがあります。

マスタノードの場合、セカンダリポートのポートアップを検出したときにフォワーディング状態に遷移するまでの保護時間を設定します。この保護時間 (forwarding-shift-time コマンドでの設定値)

は、マスタノードでのヘルスチェックフレームの送信間隔 (health-check interval コマンドでの設定値) よりも大きい値を設定してください。設定誤りからマスタノードが復旧を検出するよりも先にマスタノードのセカンダリポートがフォワーディング状態になってしまった場合、一時的にループが発生するおそれがあります。

##### [ コマンドによる設定 ]

1. (config)# axrp 1  
(config-axrp)# mode transit  
(config-axrp)# forwarding-shift-time 100  
フラッシュ制御フレームの受信待ちの保護時間を 100 秒に設定します。

#### (5) プライマリポートの設定

##### [ 設定のポイント ]

マスタノードでプライマリポートを設定できます。マスタノードでリングポート (axrp-ring-port コマンド) 指定のあるインタフェースに設定してください。本装置が共有リンク非監視リングの最終端となっている場合は設定されても動作しません。通常、プライマリポートは自動で割り振られますので、axrp-primary-port コマンドの設定または変更によってプライマリポートを切り替える場合は、リング動作がいったん停止します。

##### [ コマンドによる設定 ]

1. (config)# interface port-channel 10  
(config-if)# axrp-primary-port 1 vlan-group 1  
ポートチャンネルインタフェースコンフィギュレーションモードに移行し、該当するインタフェースをリング ID 1, VLAN グループ ID 1 のプライマリポートに設定します。

#### (6) 経路切り戻し抑止機能の有効化および抑止時間の設定

##### [ 設定のポイント ]

マスタノードで障害復旧検出後、経路切り戻し動作を抑止する時間を設定します。なお、抑止時間として infinity を指定した場合、運用コマンド clear axrp preempt-delay が入力されるまで経路切り戻し動作を抑止します。

##### [ コマンドによる設定 ]

1. (config)# axrp 1

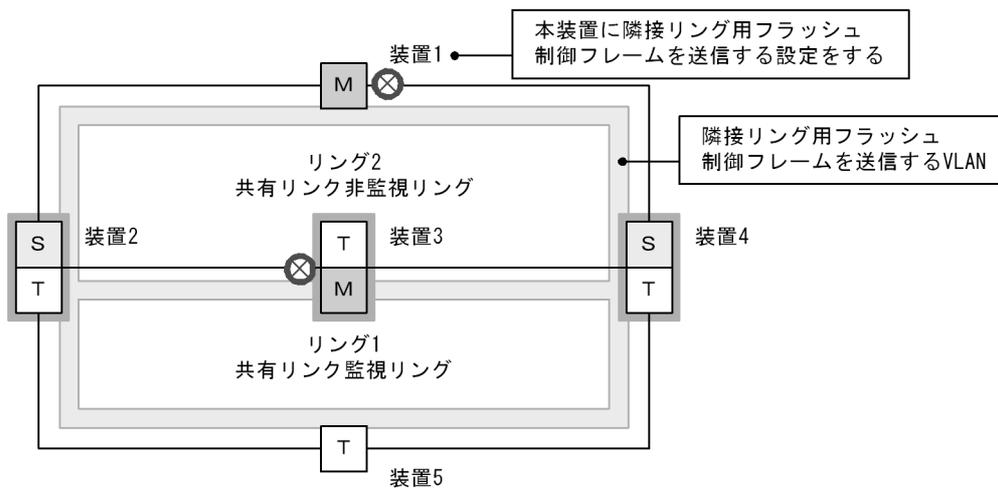
```
(config-axrp)# preempt-delay infinity
```

リング ID 1 のコンフィグレーションモードに移行し、経路切り戻し抑止時間を infinity に設定します。

### 23.1.10 隣接リング用フラッシュ制御フレームの送信設定

マスタノードの両リングポートが共有リンクとなる構成を次の図に示します。このような構成では、共有リンク非監視リングのマスタノードで隣接リング用フラッシュ制御フレームを送信する設定をしてください。

図 23-5 マスタノードの両リングポートが共有リンクとなる構成



(凡例) M : マスタノード      T : トランジットノード  
 S : 共有リンクの最終端ノード (トランジットノード)      □ : 共有ノード  
 ⊗ : ブロッキング

#### [ 設定のポイント ]

「図 23-5 マスタノードの両リングポートが共有リンクとなる構成」のように両リングポートが共有リンクとなるマスタノード (リング 1 の装置 3) が存在する共有リンクありのマルチリング構成では、共有リンク非監視リングのマスタノード (リング 2 の装置 1) で隣接リング用フラッシュ制御フレームを送信する設定をしてください。

このとき、隣接リング用フラッシュ制御フレームの送信に使用する VLAN として、この図にあるように送信対象となるリングの各ノードで VLAN マッピングに括り付けられた VLAN を設定してください。

また、この VLAN は隣接リング用フラッシュ制御フレームの送信専用として、データ転送に使用しないでください。

#### [ コマンドによる設定 ]

1. (config)# axrp 2

```
(config-axrp)# flush-request-transmit vlan 10
```

リング ID 2 (共有リンク非監視リングのマスタノード) のコンフィグレーションモードに移行して、リング ID 2 の障害発生 / 復旧時に VLAN ID 10 に対して隣接リング用フラッシュ制御フレームを送信する設定をします。

## 23.2 オペレーション

### 23.2.1 運用コマンド一覧

Ring Protocol の運用コマンド一覧を次の表に示します。

表 23-2 運用コマンド一覧

| コマンド名                    | 説明                                                            |
|--------------------------|---------------------------------------------------------------|
| show axrp                | Ring Protocol 情報を表示します。                                       |
| clear axrp               | Ring Protocol の統計情報をクリアします。                                   |
| clear axrp preempt-delay | リングの経路切り戻し抑止状態を解除します。                                         |
| restart axrp             | Ring Protocol プログラムを再起動します。                                   |
| dump protocols axrp      | Ring Protocol プログラムで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。 |
| show port <sup>1</sup>   | ポートの Ring Protocol 使用状態を表示します。                                |
| show vlan <sup>2</sup>   | VLAN の Ring Protocol 使用状態を表示します。                              |

注 1

「運用コマンドレファレンス Vol.1 17. イーサネット」を参照してください。

注 2

「運用コマンドレファレンス Vol.1 20. VLAN」を参照してください。

### 23.2.2 Ring Protocol の状態確認

#### (1) コンフィグレーション設定と運用の状態確認

show axrp コマンドで Ring Protocol の設定と運用状態を確認できます。コンフィグレーションコマンドで設定した Ring Protocol の設定内容が正しく反映されているかどうかを確認してください。リング単位の状態情報確認には show axrp <ring id list> コマンドを使用できます。

表示される情報は、項目 "Oper State" の内容により異なります。"Oper State" に "enable" が表示されている場合は Ring Protocol 機能が動作しています。このとき、表示内容は全項目について運用の状態を示しています。"Oper State" に "-" が表示されている場合は必須であるコンフィグレーションコマンドが揃っていない状態です。また、"Oper State" に "Not Operating" が表示されている場合、コンフィグレーションに矛盾があるなどの理由で、Ring Protocol 機能が動作できていない状態です。"Oper State" の表示状態が "-", または "Not Operating" 時には、コンフィグレーションを確認してください。

show axrp コマンド、show axrp detail コマンドの表示例を次に示します。

図 23-6 show axrp コマンドの実行結果

```

> show axrp
Date 2007/01/27 12:00:00 UTC

Total Ring Counts:4

Ring ID:1
Name:RING#1
Oper State:enable Mode:Master Attribute:-

VLAN Group ID Ring Port Role/State Ring Port Role/State
1 1/1 primary/forwarding 1/2 secondary/blocking
2 1/1 secondary/blocking 1/2 primary/forwarding

Ring ID:2
Name:RING#2
Oper State:enable Mode:Transit Attribute:-

VLAN Group ID Ring Port Role/State Ring Port Role/State
1 1 (ChGr) -/forwarding 2 (ChGr) -/forwarding
2 1 (ChGr) -/forwarding 2 (ChGr) -/forwarding

Ring ID:3
Name:
Oper State:disable Mode:- Attribute:-

VLAN Group ID Ring Port Role/State Ring Port Role/State
1 - -/- - -/-
2 - -/- - -/-

Ring ID:4
Name:RING#4
Oper State:enable Mode:Transit Attribute:rft-ring-edge(1)
Shared Edge Port:1/3

VLAN Group ID Ring Port Role/State Ring Port Role/State
1 1/3 -/- 1/4 -/forwarding
2 1/3 -/- 1/4 -/forwarding
>

```

show axrp detail コマンドを使用すると、統計情報やマスターノードのリング状態などについての詳細情報を確認できます。統計情報については、Ring Protocol 機能が有効 ("Oper State" が "enable") でない限り 0 を表示します。

図 23-7 show axrp detail のコマンド実行結果

```

> show axrp detail
Date 2007/01/27 12:00:00 UTC

Total Ring Counts:4

Ring ID:1
Name:RING#1
Oper State:enable Mode:Master Attribute:-
Control VLAN ID:5 Ring State:normal
Health Check Interval (msec):100
Health Check Hold Time (msec):256
Flush Request Counts:3

VLAN Group ID:1
VLAN ID:6-10,12
Ring Port:1/1 Role:primary State:forwarding
Ring Port:1/2 Role:secondary State:blocking

VLAN Group ID:2
VLAN ID:16-20,22
Ring Port:1/1 Role:secondary State:blocking
Ring Port:1/2 Role:primary State:forwarding

Last Transition Time:2007/01/24 10:00:00
Fault Counts Recovery Counts Total Flush Request Counts
1 1 12

Ring ID:2
Name:RING#2
Oper State:enable Mode : Transit Attribute : -
Control VLAN ID:15
Forwarding Shift Time (sec):10
Last Forwarding:flush request receive

VLAN Group ID:1
VLAN ID :26-30,32
Ring Port:1(ChGr) Role:- State:forwarding
Ring Port:2(ChGr) Role:- State:forwarding

VLAN Group ID:2
VLAN ID:36-40,42
Ring Port:1(ChGr) Role:- State:forwarding
Ring Port:2(ChGr) Role:- State:forwarding

Ring ID:3
Name:
Oper State:disable Mode:- Attribute:-
Control VLAN ID:-

VLAN Group ID:1
VLAN ID:-
Ring Port:- Role:- State:-
Ring Port:- Role:- State:-

VLAN Group ID:2
VLAN ID:-
Ring Port:- Role:- State:-
Ring Port:- Role:- State:-

Ring ID:4
Name:RING#4
Oper State:enable Mode:Transit Attribute:rift-ring-edge(1)
Shared Edge Port:1/3
Control VLAN ID:45
Health Check Interval (msec):1000
Forwarding Shift Time (sec):10
Last Forwarding:flush request receive

VLAN Group ID:1
VLAN ID:46-50,52
Ring Port:1/3 Role:- State:-
Ring Port:1/4 Role:- State:forwarding

```

## 23. Ring Protocol の設定と運用

```
VLAN Group ID:2
VLAN ID:56-60,62
Ring Port:1/3 Role:- State:-
Ring Port:1/4 Role:- State:forwarding
>
```

# 24 Ring Protocol とスパニングツリー / GSRP の併用

この章では、同一装置での Ring Protocol とスパニングツリーの併用、および同一装置での Ring Protocol と GSRP の併用について説明します。

---

24.1 Ring Protocol とスパニングツリーとの併用

---

24.2 Ring Protocol と GSRP との併用

---

24.3 仮想リンクのコンフィギュレーション

---

24.4 仮想リンクのオペレーション

---

## 24.1 Ring Protocol とスパニングツリーとの併用

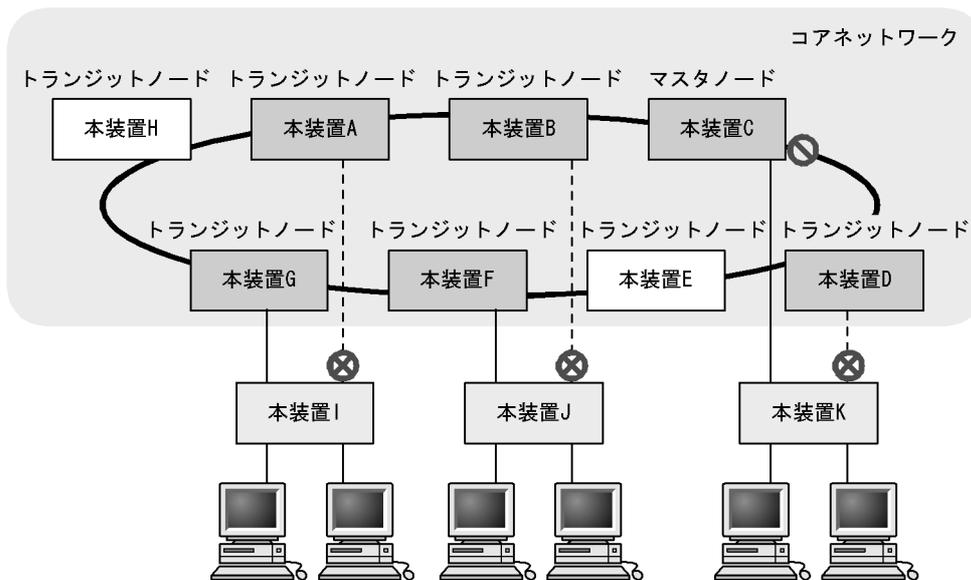
本装置では、Ring Protocol とスパニングツリーの併用ができます。Ring Protocol と併用可能なスパニングツリーのプロトコル種別については、「17.3 レイヤ2 スイッチ機能と他機能の共存について」、Ring Protocol の詳細については、「22 Ring Protocol の解説」を参照してください。

### 24.1.1 概要

同一装置で Ring Protocol とスパニングツリーを併用して、コアネットワークを Ring Protocol、アクセスネットワークをスパニングツリーとしたネットワークを構成できます。例えば、すべてをスパニングツリーで構成していたネットワークを、コアネットワークだけ Ring Protocol に変更することで、アクセスネットワークの既存設備の多くを変更することなく流用できます。なお、Ring Protocol は、シングルリングおよびマルチリング（共有リンクありのマルチリングを含む）のどちらの構成でも、スパニングツリーと併用できます。

シングルリング構成、またはマルチリング構成での Ring Protocol とスパニングツリーとの併用例を次の図に示します。本装置 A - G - I 間、B - F - J 間、C - D - K 間でそれぞれスパニングツリートポロジを構成しています。なお、本装置 A ~ D および F ~ G では、Ring Protocol とスパニングツリーが同時に動作しています。

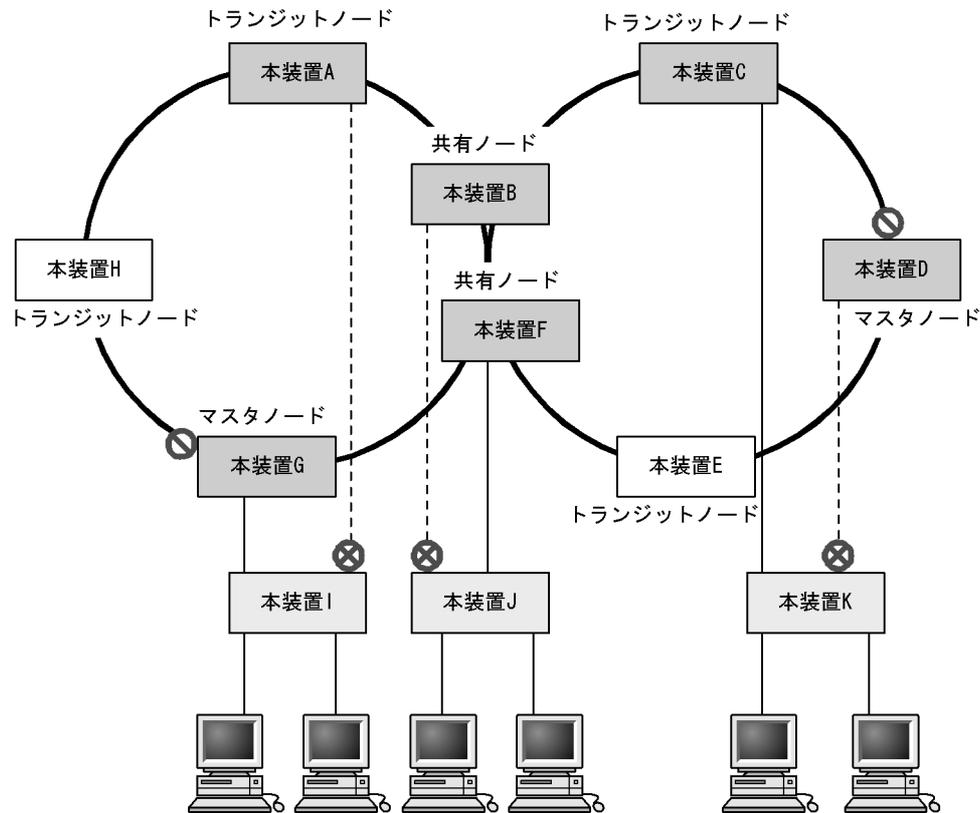
図 24-1 Ring Protocol とスパニングツリーの併用例（シングルリング構成）



(凡例)

- ⊗ : スパニングツリーによるブロッキング    ⊙ : Ring Protocolによるブロッキング
- : Ring Protocolとスパニングツリー併用の装置
- : スパニングツリーだけの装置    □ : Ring Protocolだけの装置

図 24-2 Ring Protocol とスパニングツリーの併用例 (マルチリング構成)



(凡例)

- ⊗ : スパニングツリーによるブロッキング
- ⊘ : Ring Protocolによるブロッキング
- : Ring Protocolとスパニングツリー併用の装置
- : スパニングツリーだけの装置
- : Ring Protocolだけの装置

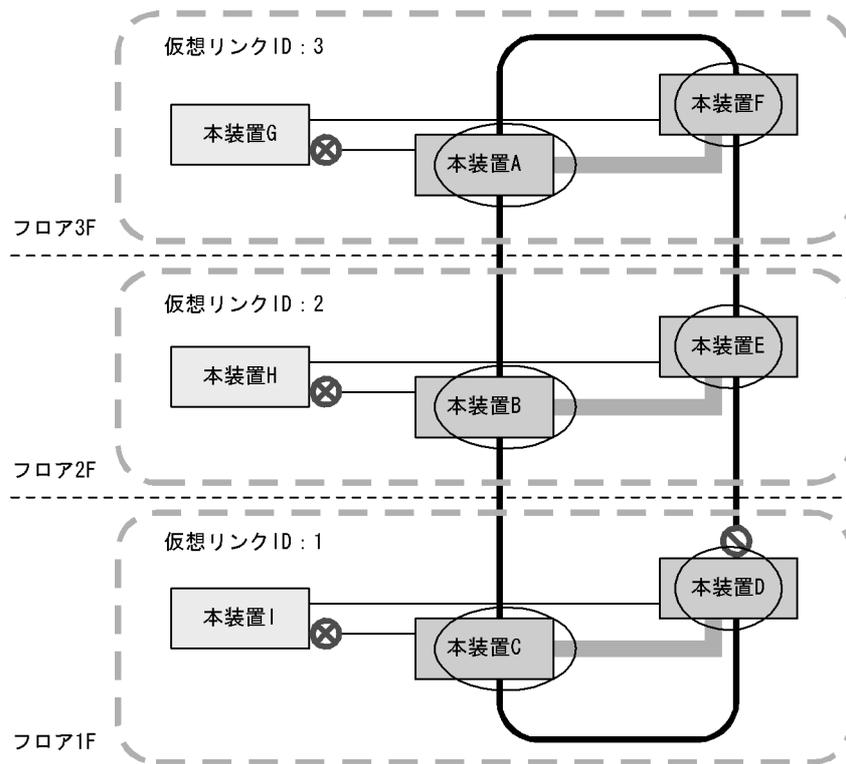
## 24.1.2 動作仕様

Ring Protocol とスパニングツリーを併用するには、二つの機能が共存している任意の 2 装置間を仮想的な回線で接続する必要があります。この仮想的な回線を仮想リンクと呼びます。仮想リンクは、リングネットワーク上の 2 装置間に構築されます。仮想リンクの構築には、仮想リンクを識別するための仮想リンク ID と、仮想リンク間で制御フレームの送受信を行うための仮想リンク VLAN が必要です。

Ring Protocol とスパニングツリーを併用するノードは、自装置の仮想リンク ID と同じ仮想リンク ID を持つ装置同士でスパニングツリートポロジを構成します。同じ仮想リンク ID を持つ装置グループを拠点と呼び、各拠点では独立したスパニングツリートポロジを構成します。

仮想リンクの概要を次の図に示します。

図 24-3 仮想リンクの概要



(凡例)

- ⊗ : スパニングツリーによるブロッキング    ⊘ : Ring Protocolによるブロッキング
- : Ring Protocolとスパニングツリー併用の装置 (本装置A, B, C, E, Fはトランジットノード)    □ : スパニングツリーだけの装置 (本装置Dはマスターノード)
- : 仮想リンク    ○ : スパニングツリーから見た仮想ポート
- : 拠点 (同じ仮想リンクIDを持つ装置グループ)

注 各フロアはそれぞれ独立したスパニングツリートポロジを構成しています。

### (1) 仮想リンク VLAN

仮想リンク間での制御フレームの送受信には、仮想リンク VLAN を使用します。この仮想リンク VLAN は、リングポートのデータ転送用 VLAN として管理している VLAN のうち一つを使用します。また、仮想リンク VLAN は、複数の拠点で同一の VLAN ID を使用できます。

### (2) Ring Protocol の制御 VLAN の扱い

Ring Protocol の制御 VLAN は、スパニングツリーの対象外となります。

そのため、PVST+ では当該 VLAN のツリーを構築しません。また、シングルスパニングツリーおよびマルチプルスパニングツリーの転送状態も適用されません。

### (3) リングポートの状態とコンフィギュレーションの設定値

リングポートのデータ転送用 VLAN の転送状態は、Ring Protocol で決定されます。

例えば、スパンニングツリートポロジでブロッキングと判断しても、Ring Protocol でフォワーディングと判断すれば、そのポートはフォワーディングとなります。したがって、スパンニングツリーでリングポートがブロッキングとなるトポロジを構築すると、ループとなるおそれがあります。このため、リングポートが常にフォワーディングとなるよう、Ring Protocol と共存したスパンニングツリーでは、本装置がルートブリッジまたは 2 番目の優先度になるようにブリッジ優先度の初期値を自動的に高くして動作します。なお、コンフィグレーションで値を設定している場合は、設定した値で動作します。

ブリッジ優先度の設定値を次の表に示します。

表 24-1 ブリッジ優先度の設定値

| 設定項目    | 関連するコンフィグレーション                                                                                  | 初期値 |
|---------|-------------------------------------------------------------------------------------------------|-----|
| ブリッジ優先度 | spanning-tree single priority<br>spanning-tree vlan priority<br>spanning-tree mst root priority | 0   |

また、仮想リンクのポートは固定値で動作し、コンフィグレーションによる設定値は適用されません。

仮想リンクのポートの設定値を次の表に示します。

表 24-2 仮想リンクポートの設定値

| 設定項目   | 関連するコンフィグレーション                                                                                                                           | 初期値 (固定)       |
|--------|------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| リンクタイプ | spanning-tree link-type                                                                                                                  | point-to-point |
| ポート優先度 | spanning-tree port-priority<br>spanning-tree single port-priority<br>spanning-tree vlan port-priority<br>spanning-tree mst port-priority | 0              |
| パスコスト  | spanning-tree cost<br>spanning-tree single cost<br>spanning-tree vlan cost<br>spanning-tree mst cost                                     | 1              |

#### (4) リングポートでのスパンニングツリー機能について

リングポートでは次に示すスパンニングツリー機能は動作しません。

- BPDU フィルタ
- BPDU ガード
- ループガード機能
- ルートガード機能
- PortFast 機能

#### (5) スパンニングツリートポロジ変更時の MAC アドレステーブルクリア

スパンニングツリーでのトポロジ変更時に、シングルリングまたはマルチリングネットワーク全体に対して、MAC アドレステーブルエントリのクリアを促すフラッシュ制御フレームを送信します。これを受信したリングネットワーク内の各装置は、Ring Protocol が動作中のリングポートに対する、MAC アドレステーブルエントリをクリアします。なお、トポロジ変更が発生した拠点の装置は、スパンニングツリープロトコルで MAC アドレステーブルエントリをクリアします。

#### (6) リングポート以外のポートの一時的なブロッキングについて

Ring Protocol とスパンニングツリーを併用する装置で、次に示すイベントが発生した場合、リングポート以外のスパンニングツリーが動作しているポートを一時的にブロッキング状態にします。

- 装置起動（装置再起動も含む）
- コンフィグレーションファイルのランニングコンフィグレーションへの反映
- 系切替
- 1 枚目の BSU アップ
- restart vlan コマンド
- restart spanning-tree コマンド

スパニングツリーが仮想リンク経由の制御フレームを送受信できるようになる前にアクセスネットワーク内だけでトポロジを構築した場合、それだけではループ構成とならないためどのポートもブロッキングされません。したがって、このままでは、リングネットワークとアクセスネットワークにわたるループ構成となります。このため、本機能で一時的にブロッキングしてループを防止します。本機能は PortFast 機能を設定しているポートでも動作します。本機能でのブロッキングは、次のどちらかで行われます。

- イベント発生から 20 秒間
- イベント発生から 20 秒以内に仮想リンク経由で制御フレームを受信した場合は受信から 6 秒間

本機能を有効に動作させるため、次の表に示すコンフィグレーションを「設定値」の範囲内で設定してください。範囲内の値で設定しなかった場合、一時的にループが発生するおそれがあります。

表 24-3 リングポート以外のポートを一時的にブロッキング状態にするときの設定値

| 設定項目                               | 関連するコンフィグレーション                                                                                   | 設定値                     |
|------------------------------------|--------------------------------------------------------------------------------------------------|-------------------------|
| Ring Protocol フラッシュ制御フレームの受信待ち保護時間 | forwarding-shift-time                                                                            | 10 秒以下<br>(デフォルト値 10 秒) |
| スパニングツリー制御フレーム送信間隔                 | spanning-tree single hello-time<br>spanning-tree vlan hello-time<br>spanning-tree mst hello-time | 2 秒以下<br>(デフォルト値 2 秒)   |

### 24.1.3 各種スパニングツリーとの共存について

#### (1) PVST+ との共存

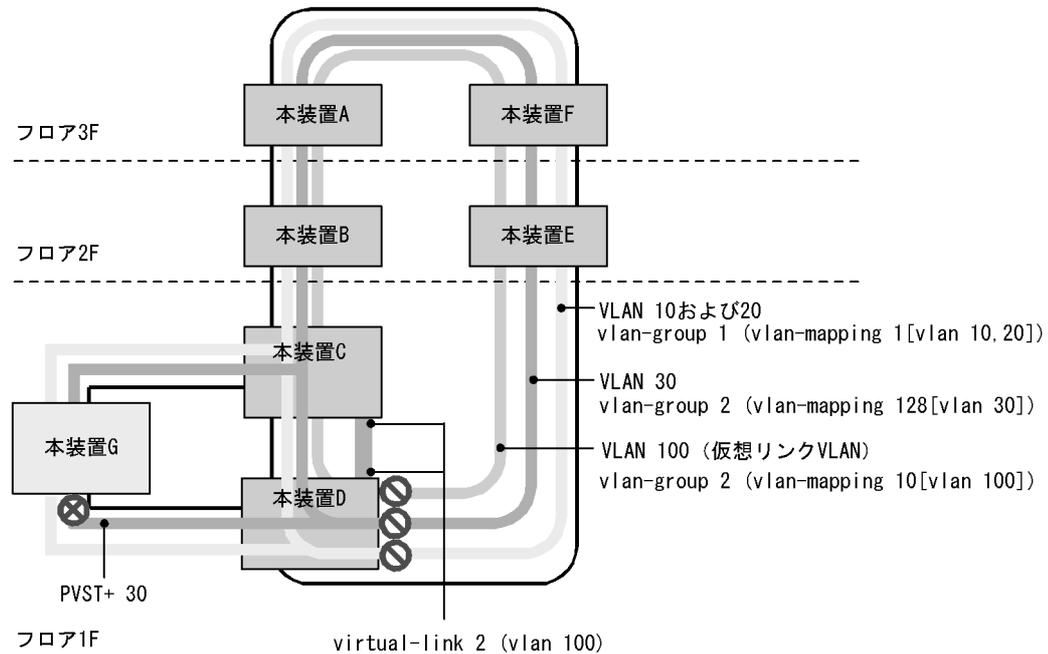
PVST+ は、Ring Protocol の VLAN マッピングに設定された VLAN が一つだけであれば、その VLAN で Ring Protocol と共存できます。コンフィグレーションコマンド `axrp virtual-link` で仮想リンクを設定すると、仮想リンクによるトポロジを構築し Ring Protocol との共存を開始します。

最初の Ring Protocol のコンフィグレーション設定によって、動作中の PVST+ はすべて停止します。その後、VLAN マッピングが設定された VLAN で順次 PVST+ が動作します。VLAN マッピングに複数の VLAN を設定した場合、その VLAN では PVST+ は動作しません。なお、PVST+ が停止している VLAN はループとなるおそれがあります。ポートを閉塞するなどしてループ構成にならないように注意してください。

また、コンフィグレーションコマンド `axrp virtual-link` で仮想リンクを設定していない場合は、仮想リンクを構築できないので意図したトポロジが構築されません。その結果、ループが発生するおそれがあります。

PVST+ と Ring Protocol の共存構成を次の図に示します。ここでは、VLAN マッピング 128 には VLAN 30 が一つだけ設定されているので、PVST+ が動作します。VLAN マッピング 1 には複数 VLAN が設定されているので、PVST+ は動作しません。また、装置 C および D では VLAN 100 を仮想リンク VLAN に設定しているため、両装置間に仮想リンクを構築します。

図 24-4 PVST+ と Ring Protocol の共存構成



|               |                                                                                    |
|---------------|------------------------------------------------------------------------------------|
| 本装置A, B, E, F | : VLAN 10, 20, 30および100を使用したRing Protocolを構成している装置                                 |
| 本装置C, D       | : VLAN 10, 20および30を使用したRing Protocolと、PVST+ 30を併用している装置<br>仮想リンクVLANとしてVLAN 100を使用 |
| 本装置G          | : PVST+ 30だけを使用している装置                                                              |

(凡例)

- ⊗ : スパニングツリーによるブロッキング
- ⊘ : Ring Protocolによるブロッキング
- : Ring Protocolとスパニングツリー併用の装置
- : スパニングツリーだけの装置
- : 仮想リンク

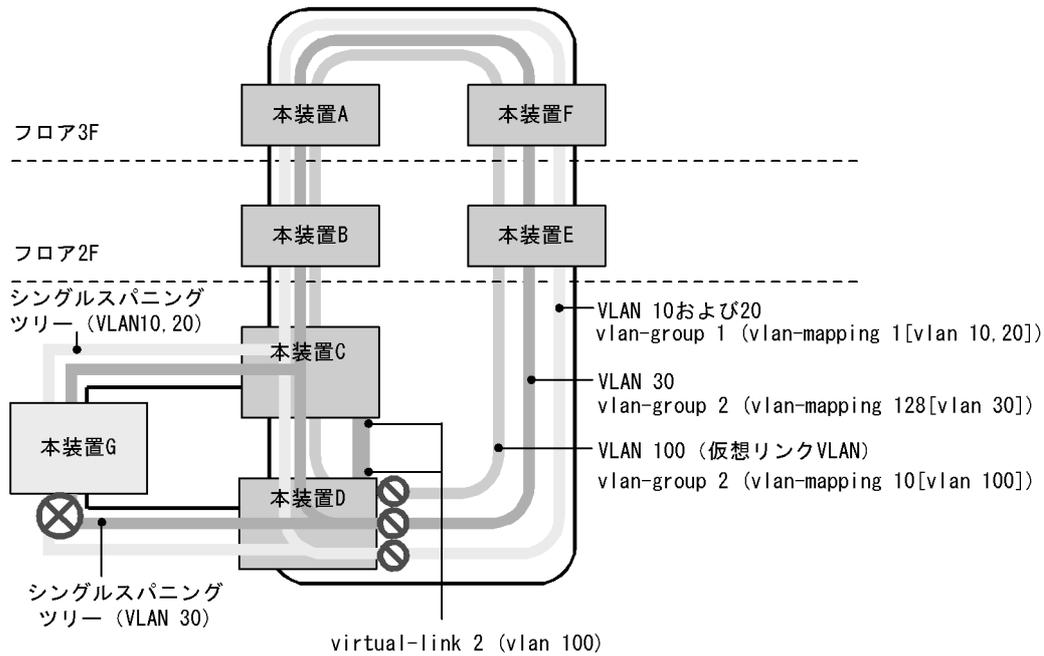
## (2) シングルスパニングツリーとの共存

シングルスパニングツリーは Ring Protocol で運用するすべてのデータ VLAN と共存できます。

シングルスパニングツリーは、コンフィグレーションコマンド `axrp virtual-link` で仮想リンクを設定すると、仮想リンクによるトポロジを構築し Ring Protocol との共存を開始します。コンフィグレーションコマンド `axrp virtual-link` で仮想リンクを設定していない場合は、仮想リンクを構築できないので意図したトポロジが構築されません。その結果ループが発生するおそれがあります。

シングルスパニングツリーと Ring Protocol の共存構成を次の図に示します。ここでは、装置 C, D, および G にシングルスパニングツリーを設定し、装置 A, B, C, D, E, および F に Ring Protocol の VLAN グループを二つ設定しています。シングルスパニングツリーのトポロジは、全 VLAN グループ (全 VLAN マッピング) に所属している VLAN にそれぞれ反映されます。また、装置 C および D では VLAN 100 を仮想リンク VLAN に設定しているので、両装置間に仮想リンクを構築します。

図 24-5 シングルスパンニングツリーと Ring Protocol の共存構成



本装置A, B, E, F : VLAN 10, 20および30を使用したRing Protocolを構成している装置  
 本装置C, D : VLAN 10, 20および30を使用したRing Protocolとシングルスパンニングツリーを併用している装置  
 仮想リンクVLANとしてVLAN 100を使用  
 本装置G : シングルスパンニングツリーだけを使用している装置

(凡例)

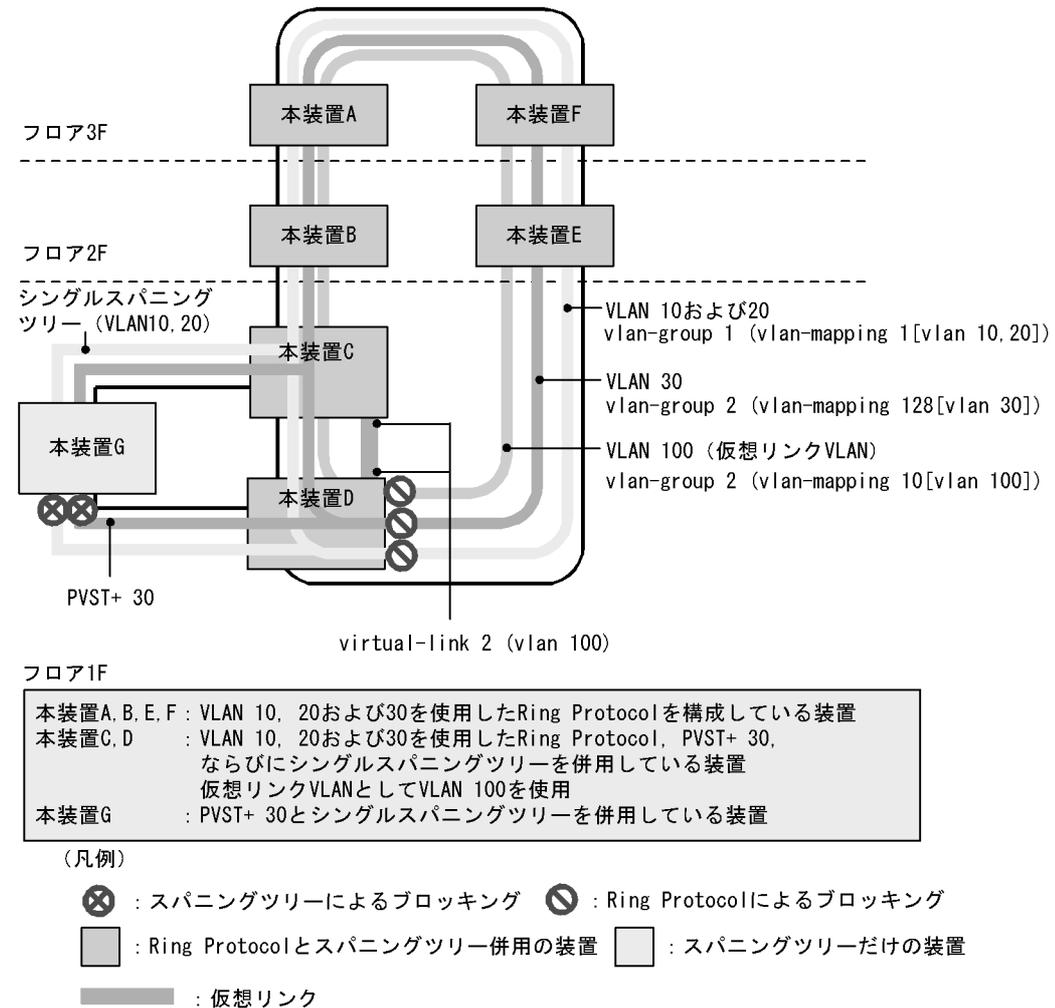
- ⊗ : スパンニングツリーによるブロッキング
- ⊙ : Ring Protocolによるブロッキング
- (黒) : Ring Protocolとスパンニングツリー併用の装置
- (白) : スパンニングツリーだけの装置
- (太線) : 仮想リンク

### (3) PVST+ とシングルスパンニングツリーの同時動作について

Ring Protocol と共存している場合でも、PVST+ とシングルスパンニングツリーの同時動作は可能です。この場合、PVST+ で動作していない VLAN はすべてシングルスパンニングツリーとして動作します (通常の同時動作と同じです)。

シングルスパンニングツリー、PVST+、および Ring Protocol の共存構成を次の図に示します。ここでは、VLAN マッピング 128 には VLAN 30 が一つだけ設定されているので、PVST+ が動作します。VLAN マッピング 1 では PVST+ が動作しないので、シングルスパンニングツリーとして動作し、トポロジーを反映します。また、装置 C および D では VLAN 100 を仮想リンク VLAN に設定しているため、両装置間に仮想リンクを構築します。

図 24-6 シングルスパニングツリー，PVST+，および Ring Protocol の共存構成



#### (4) マルチプルスパニングツリーとの共存

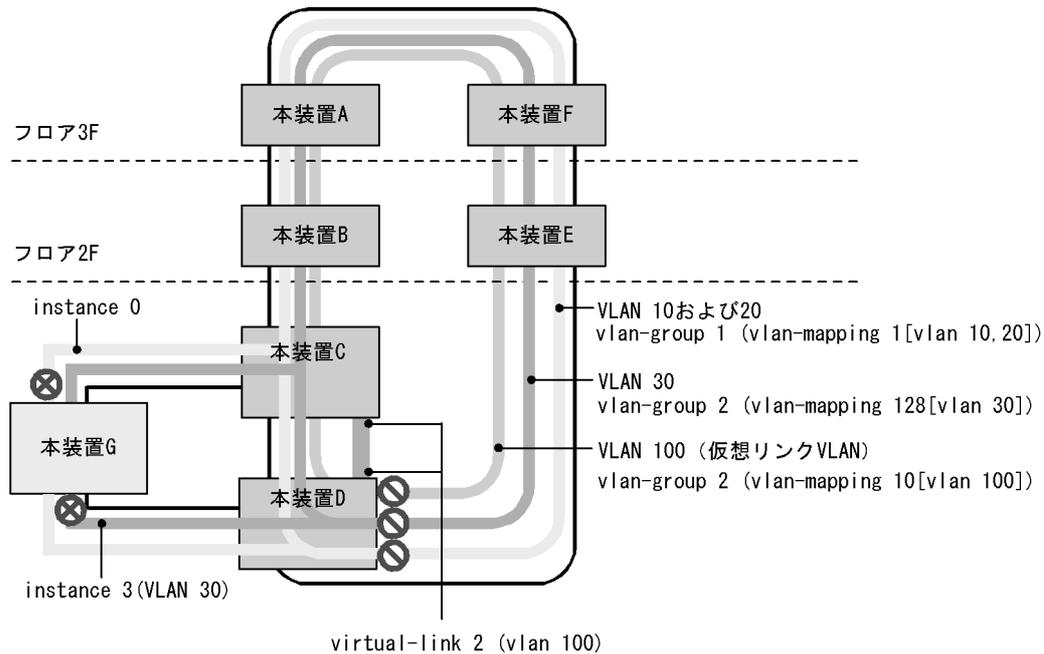
マルチプルスパニングツリーは Ring Protocol で運用するすべてのデータ転送用 VLAN と共存できます。

マルチプルスパニングツリーは、コンフィグレーションコマンド `axrp virtual-link` で仮想リンクを設定すると、仮想リンクによるトポロジを構築し Ring Protocol との共存を開始します。コンフィグレーションコマンド `axrp virtual-link` で仮想リンクを設定していない場合は、仮想リンクを構築できないので意図したトポロジが構築されません。その結果ループが発生するおそれがあります。

MST インスタンスに所属する VLAN と、Ring Protocol の VLAN マッピングで同じ VLAN を設定すると、MST インスタンスと Ring Protocol で共存動作できるようになります。設定した VLAN が一致しない場合、一致していない VLAN はブロッキング状態になります。

マルチプルスパニングツリーと Ring Protocol の共存構成を次の図に示します。ここでは、装置 C, D, および G にマルチプルスパニングツリーを設定し、装置 A, B, C, D, E, および F に Ring Protocol の VLAN グループを二つ設定しています。Ring Protocol の VLAN グループ 1 は CIST, VLAN グループ 2 は MST インスタンス 3 としてマルチプルスパニングツリーのトポロジに反映されます。また、装置 C および D では VLAN 100 を仮想リンク VLAN に設定しているため、両装置間に仮想リンクを構築します。

図 24-7 マルチプルスパニングツリーと Ring Protocol の共存構成



|               |                                                             |
|---------------|-------------------------------------------------------------|
| 本装置A, B, E, F | : VLAN 10, 20および30を使用したRing Protocolを構成している装置               |
| 本装置C, D       | : VLAN 10, 20および30を使用したRing Protocolとマルチプルスパニングツリーを併用している装置 |
|               | 仮想リンクVLANとしてVLAN 100を使用                                     |
| 本装置G          | : マルチプルスパニングツリーだけを使用している装置                                  |

(凡例)

- ⊗ : スパニングツリーによるブロッキング
- ⊙ : Ring Protocolによるブロッキング
- (灰色) : Ring Protocolとスパニングツリー併用の装置
- (白色) : スパニングツリーだけの装置
- (太線) : 仮想リンク

### (5) 共存して動作させない VLAN について

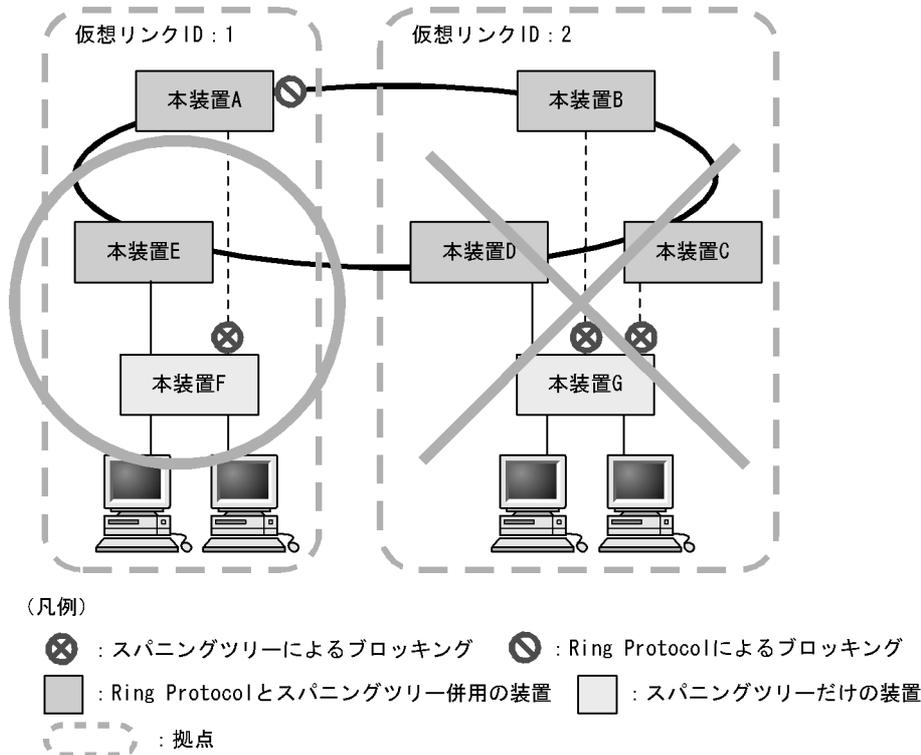
- Ring Protocol だけを適用させる VLAN  
PVST+ をコンフィグレーション設定などで停止させると、その VLAN は Ring Protocol だけが適用される VLAN となります。  
シングルスパニングツリー動作時、またはマルチプルスパニングツリー動作時、Ring Protocol が扱うデータ転送用 VLAN は必ず共存して動作します。
- PVST+ だけを適用させる VLAN  
Ring Protocol で VLAN グループに所属しない VLAN マッピングを設定すると、PVST+ だけが適用される VLAN となります。
- シングルスパニングツリーだけを適用させる VLAN  
Ring Protocol で VLAN グループに所属しない VLAN は、シングルスパニングツリーだけが適用される VLAN となります。
- マルチプルスパニングツリーだけを適用させる VLAN  
Ring Protocol で VLAN グループに所属しない VLAN は、マルチプルスパニングツリーだけが適用される VLAN となります。

## 24.1.4 禁止構成

### (1) 1 拠点当たりの装置数

Ring Protocol とスパニングツリーを併用した本装置は、1 拠点に 2 台配置できます。3 台以上で 1 拠点を構成することはできません。仮想リンクの禁止構成を次の図に示します。

図 24-8 仮想リンクの禁止構成



## 24.1.5 Ring Protocol とスパニングツリー併用時の注意事項

### (1) 仮想リンク VLAN と VLAN マッピングの対応づけについて

仮想リンク VLAN に指定する VLAN は、リング内のデータ転送用 VLAN に所属 (VLAN マッピングおよび VLAN グループに設定) している必要があります。

### (2) 仮想リンク VLAN の設定範囲について

- リングネットワークへの設定  
仮想リンクを構成しているリングネットワークでは、シングルリングおよびマルチリング (共有リンクありのマルチリング構成も含む) どちらの場合でも、仮想リンク間で制御フレームを送受信する可能性のあるすべてのノードに対して仮想リンク VLAN をデータ転送用 VLAN に設定しておく必要があります。設定が不足していると、拠点ノード間で仮想リンクを使って制御フレームの送受信ができず、障害の誤検出を起こすおそれがあります。
- スパニングツリーネットワークへの設定  
仮想リンク VLAN は、リングネットワーク内で使用するため、下流側のスパニングツリーには使用できません。このため、スパニングツリーで制御する下流ポートに対して仮想リンク VLAN を設定すると、ループするおそれがあります。

(3) 仮想リンク VLAN を設定していない場合のスパニングツリーについて

仮想リンク VLAN を設定していない場合は、仮想リンクを構築できないので意図したトポロジーが構築されません。その結果ループが発生するおそれがあります。

(4) Ring Protocol の設定によるスパニングツリー停止について

最初の Ring Protocol のコンフィグレーション設定によって、動作中の PVST+ およびマルチプルスパニングツリーはすべて停止します。PVST+ またはマルチプルスパニングツリーが停止すると当該 VLAN はループとなるおそれがあります。ポートを閉塞するなどしてループ構成にならないように注意してください。

(5) Ring Protocol とスパニングツリー併用時のネットワーク構築について

Ring Protocol およびスパニングツリーを利用するネットワークは基本的にループ構成となります。既設のリングネットワークに対し、アクセスネットワークにスパニングツリーを構築する際は、スパニングツリーネットワーク側の構成ポート（物理ポートまたはチャンネルグループ）を shutdown に設定するなどダウン状態にした上で構築してください。

(6) Ring Protocol の障害監視時間とスパニングツリーの BPDU の送信間隔について

Ring Protocol のヘルスチェックフレームの障害監視時間（health-check holdtime）は、スパニングツリーの BPDU のタイムアウト検出時間（hello-time × 3（秒））よりも小さな値を設定してください。大きな値を設定すると、リングネットワーク内で障害が発生した際に、Ring Protocol が障害を検出する前にスパニングツリーが BPDU のタイムアウトを検出してしまい、トポロジー変更が発生し、ループするおそれがあります。

(7) トランジットノードでのプログラム再起動時の対応について

Ring Protocol プログラムを再起動（運用コマンド restart axrp）する際は、スパニングツリーネットワーク側の構成ポート（物理ポートまたはチャンネルグループ）を shutdown に設定するなどダウン状態にした上で実施してください。再起動後は、トランジットノードのフラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）のタイムアウトを待つか、制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）を利用して経路を切り替えたあとで、ダウン状態にしたポートの shutdown などを解除してください。

(8) リングネットワークでの片方向リンク障害の対応について

Ring Protocol は、片方向リンク障害でのリング障害は検出しません。リングネットワークで片方向リンク障害が発生すると、仮想リンク制御フレームを送受信できなくなるため、スパニングツリーが BPDU タイムアウトを誤検出してしまうことがあります。その結果、ループが発生し、ループ状態は片方向リンク障害が解消されるまで継続するおそれがあります。

Ring Protocol と IEEE802.3ah/UDLD 機能を併用すれば、片方向リンク障害を検出できるようになるため、片方向リンク障害によるループの発生を防止できます。

(9) スパニングツリー併用環境での多重障害からの復旧手順について

リングネットワーク内で 2 か所以上の障害（多重障害）が発生したことによって、仮想リンク制御フレームを送受信できなくなり、スパニングツリーのトポロジー変更が発生する場合があります。多重障害には、Ring Protocol とスパニングツリーを併用した装置で両リングポートに障害が発生した場合も含まれます。この状態からリングネットワーク内のすべての障害を復旧する際は、次に示す手順で復旧してください。

1. スパニングツリーネットワークの構成ポート（物理ポートまたはチャンネルグループ）を shutdown にするなどダウン状態にします。
2. リングネットワーク内の障害箇所を復旧し，マスタノードでリング障害の復旧を検出させます。
3. スパニングツリーネットワーク側の構成ポートの shutdownなどを解除し，復旧させます。

(10) Ring Protocol の VLAN マッピングとマルチプルスパニングツリーの MST インスタンスに所属する VLAN との整合性について

コンフィグレーションの変更過程で，Ring Protocol の VLAN マッピングとマルチプルスパニングツリーの MST インスタンスに所属する VLAN の設定が完全に一致しない場合，一致していない VLAN はブロッキング状態になり，通信できないおそれがあります。

## 24.2 Ring Protocol と GSRP との併用

本装置では、Ring Protocol と GSRP との併用ができます。Ring Protocol の詳細については、「22 Ring Protocol の解説」を参照してください。

### 24.2.1 動作概要

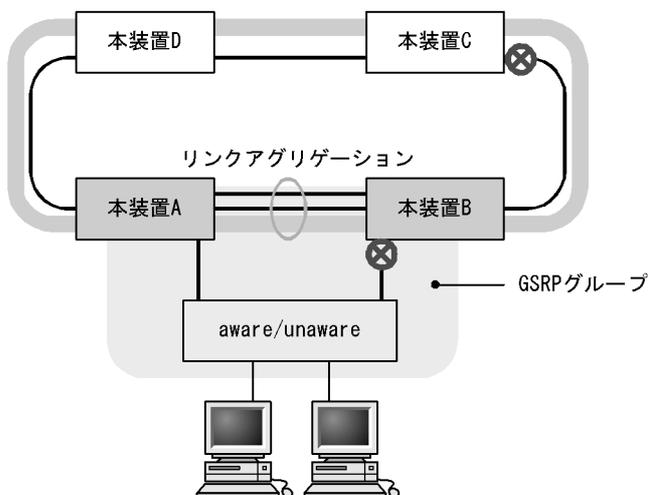
Ring Protocol と GSRP が併用して動作している装置では、Ring Protocol の VLAN マッピングと GSRP の VLAN グループの VLAN 情報が一致している必要があります。この装置のリングポートは GSRP の制御対象外となり、リングポートのデータ転送状態は Ring Protocol で制御します。

障害の監視や障害発生時の経路切り替えは、リングネットワークでは Ring Protocol で、GSRP ネットワークでは GSRP で、独立して実施します。ただし、GSRP ネットワークで経路の切り替え時にマスタに遷移した装置は、GSRP スイッチおよび aware/unaware 装置の MAC アドレステーブルをクリアします。同時に、リングネットワーク用のフラッシュ制御フレームを送信して、リングネットワークを構成する装置の MAC アドレステーブルもクリアします。

GSRP のダイレクトリンクは、リングネットワークと同じ回線を使用できます。また、別の回線にすることもできます。

Ring Protocol と GSRP との併用例を次の図に示します。

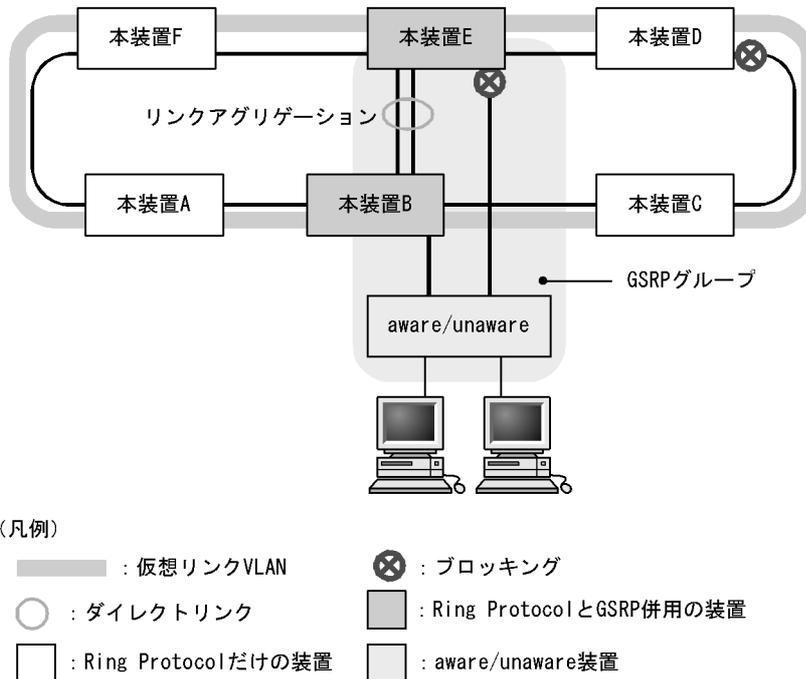
図 24-9 Ring Protocol と GSRP の併用例（ダイレクトリンクをリングネットワークで使用する場合）



(凡例)

- |                        |                             |
|------------------------|-----------------------------|
| — : 仮想リンクVLAN          | ⊗ : ブロッキング                  |
| ○ : ダイレクトリンク           | ■ : Ring ProtocolとGSRP併用の装置 |
| □ : Ring Protocolだけの装置 | □ : aware/unaware装置         |

図 24-10 Ring Protocol と GSRP の併用例 (ダイレクトリンクをリングネットワークで使用しない場合)



## 24.2.2 併用条件

Ring Protocol と GSRP の併用条件を示します。

### (1) Ring Protocol と GSRP を併用動作させたい VLAN の設定条件

Ring Protocol の VLAN マッピングの VLAN と GSRP の VLAN グループの VLAN をすべて一致させてください。

### (2) Ring Protocol または GSRP を単独で動作させたい VLAN の設定条件

すべての VLAN を共存動作させる必要はありません。VLAN 単位に別々のプロトコルを動作させる場合は、Ring Protocol の VLAN マッピングの VLAN と GSRP の VLAN グループの VLAN で一致する VLAN がないようにしてください。

## 24.2.3 リングポートの扱い

リングポートはコンフィグレーションコマンド `gsrp exception-port` の設定有無にかかわらず、GSRP の制御対象外ポートとして動作します。リングポートのデータ転送状態は Ring Protocol だけが制御します。

また、リングポートに次のコンフィグレーションコマンドを設定しても無効になります。

- `gsrp reset-flush-port` (ポートリセット機能を実施するポート)
- `gsrp no-flush-port` (GSRP Flush request フレームを送信しないポート)

## 24.2.4 Ring Protocol の制御 VLAN の扱い

Ring Protocol の制御 VLAN を GSRP の VLAN グループに設定した場合、該当する VLAN を VLAN グループの所属外にします。VLAN グループの所属外になった VLAN については、運用コマンド `show gsrp`

では表示されません。

## 24.2.5 GSRP ネットワーク切り替え時の MAC アドレステーブルクリア

Ring Protocol と GSRP を併用する場合、GSRP ネットワークの経路切り替え時にはリングネットワークを構成する装置の MAC アドレステーブルをクリアする必要があります。MAC アドレステーブルをクリアしないと、すぐに通信が復旧しないおそれがあります。リングネットワーク上の装置の MAC アドレステーブルをクリアするために、GSRP のマスタに遷移した際、リングネットワーク上に設定した仮想リンク VLAN を使用して、リングネットワーク用のフラッシュ制御フレームを送信します。この仮想リンク VLAN は、Ring Protocol のデータ転送用 VLAN グループに所属する必要があります。

GSRP のマスタが送信したフラッシュ制御フレームをリング構成装置が受信すると、MAC アドレステーブルをクリアします。また、送信回数は GSRP のコンフィグレーション (flush-request-count) に従います。

なお、Ring Protocol と GSRP を異なる VLAN で単独動作させる場合は、障害発生時に経路切り替えが発生しても互いのプロトコルに影響を与えません。したがって、MAC アドレステーブルをクリアする必要がないため、仮想リンク VLAN を設定する必要はありません。

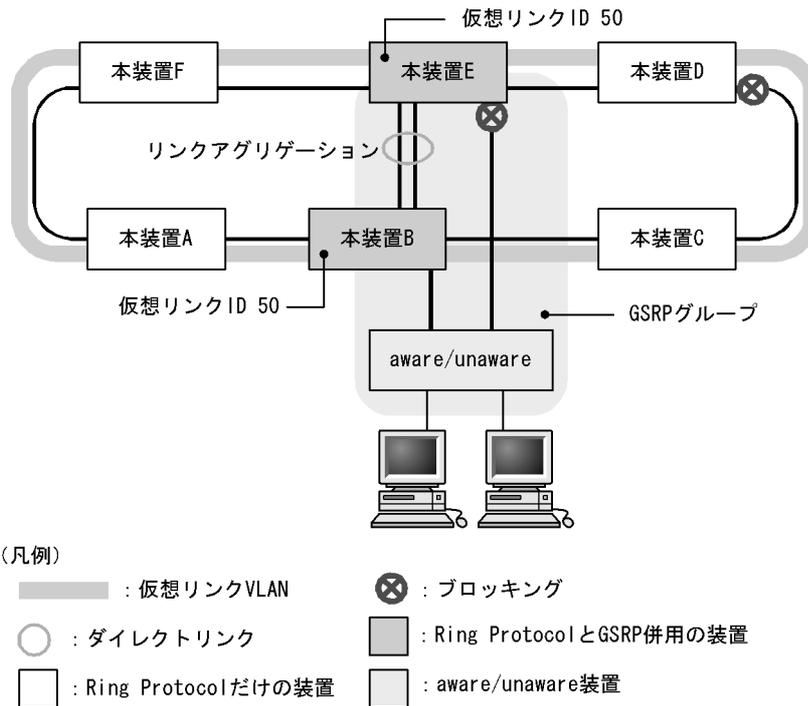
## 24.2.6 Ring Protocol と GSRP 併用動作時の注意事項

### (1) 仮想リンク VLAN の設定について

Ring Protocol と GSRP を併用する場合は、フラッシュ制御フレームを送信するために仮想リンク VLAN の設定が必要です。この仮想リンク VLAN は、Ring Protocol のデータ転送用 VLAN グループに所属する必要があります。

仮想リンク ID の設定を次の図に示します。仮想リンク ID には、同じ GSRP グループ装置で同一の仮想リンク ID を設定する必要があります。また、同じ仮想リンク VLAN が設定されているリングネットワーク内で一意となる値を設定する必要があります。同じ GSRP グループではない本装置 A, C, D, および F に仮想リンク ID 50 を設定すると、該当装置では、フラッシュ制御フレームによる MAC アドレステーブルのクリアができなくなります。

図 24-11 仮想リンク ID の設定



## (2) Ring Protocol の VLAN マッピングまたは GSRP の VLAN グループの変更について

Ring Protocol と GSRP を併用する場合は、Ring Protocol の VLAN マッピングの VLAN と GSRP の VLAN グループの VLAN をすべて一致させる必要があります。コンフィギュレーションの変更過程で一致しない状態になった場合、設定された VLAN の中で、ブロッキング状態となり、通信できない VLAN が発生するおそれがあります。

このため、Ring Protocol と GSRP を併用するためにコンフィギュレーションを変更する場合は、GSRP のバックアップ装置で、priority コマンドや backup-lock コマンドなどの設定によって、マスタへの切り替えが発生しないようにしてから、変更する必要があります。

## (3) 1VLAN グループあたりに設定可能な VLAN 数について

Ring Protocol と併用している VLAN グループに 511 以上の VLAN 数を所属させると、該当する VLAN グループの状態が遷移したときにリングポートが一時的にブロッキング状態になります。

Ring Protocol と併用している VLAN グループに所属させる VLAN 数は 510 以下にしてください。

## (4) GSRP VLAN グループ限定制御機能について

Ring Protocol と GSRP の併用時、次に示す状態では、GSRP VLAN グループ限定制御機能を設定していても、VLAN グループに所属しない VLAN のポートがブロッキング状態になるおそれがあります。

- Ring Protocol のコンフィギュレーションが適切に設定されていないなどの要因で Ring Protocol が動作していない

Ring Protocol 機能が正常に動作していないリング ID の、制御 VLAN に設定している VLAN がブロッキング状態になるおそれがあります。ただし、リングポートはブロッキング状態になりません。

- disable コマンドによって、Ring Protocol 機能を無効にしている

Ring Protocol 機能を無効にしているリング ID の、制御 VLAN に設定している VLAN がブロッキング状態になるおそれがあります。ただし、リングポートはブロッキング状態になりません。

・「24.2.2 併用条件」にある Ring Protocol と GSRP の併用条件を満たしていない

Ring Protocol と GSRP との併用条件を満たしていない VLAN がブロッキング状態になるおそれがあります。

#### (5) レイヤ 3 冗長切替機能の適用について

Ring Protocol と GSRP を同じデータ VLAN で併用動作させる場合は、レイヤ 3 冗長切替機能を適用できません。レイヤ 3 冗長切替機能を適用して GSRP ネットワークとリングネットワークを接続する場合は、Ring Protocol と GSRP でそれぞれ異なるデータ VLAN を設定して、単独動作させてください。

### 24.2.7 単独動作時の動作概要（レイヤ 3 冗長切替機能の適用例）

Ring Protocol と GSRP をそれぞれ異なる VLAN で単独動作させている場合は、レイヤ 3 冗長切替機能でリングネットワークと接続します。この場合の例を次の図に示します。下流ネットワーク（PC など）から本装置 A でレイヤ 3 中継し、VLAN 100 のリングネットワークを介して上流ネットワークと通信を行っています。このとき、本装置 A に障害が発生すると、下流ネットワークと上流ネットワークは装置 B（ダイレクトリンク障害検出機能を設定時）でレイヤ 3 中継し、VLAN 200 のリングネットワークを介して通信を行います。

図 24-12 レイヤ 3 冗長切替機能 (通常運用時)

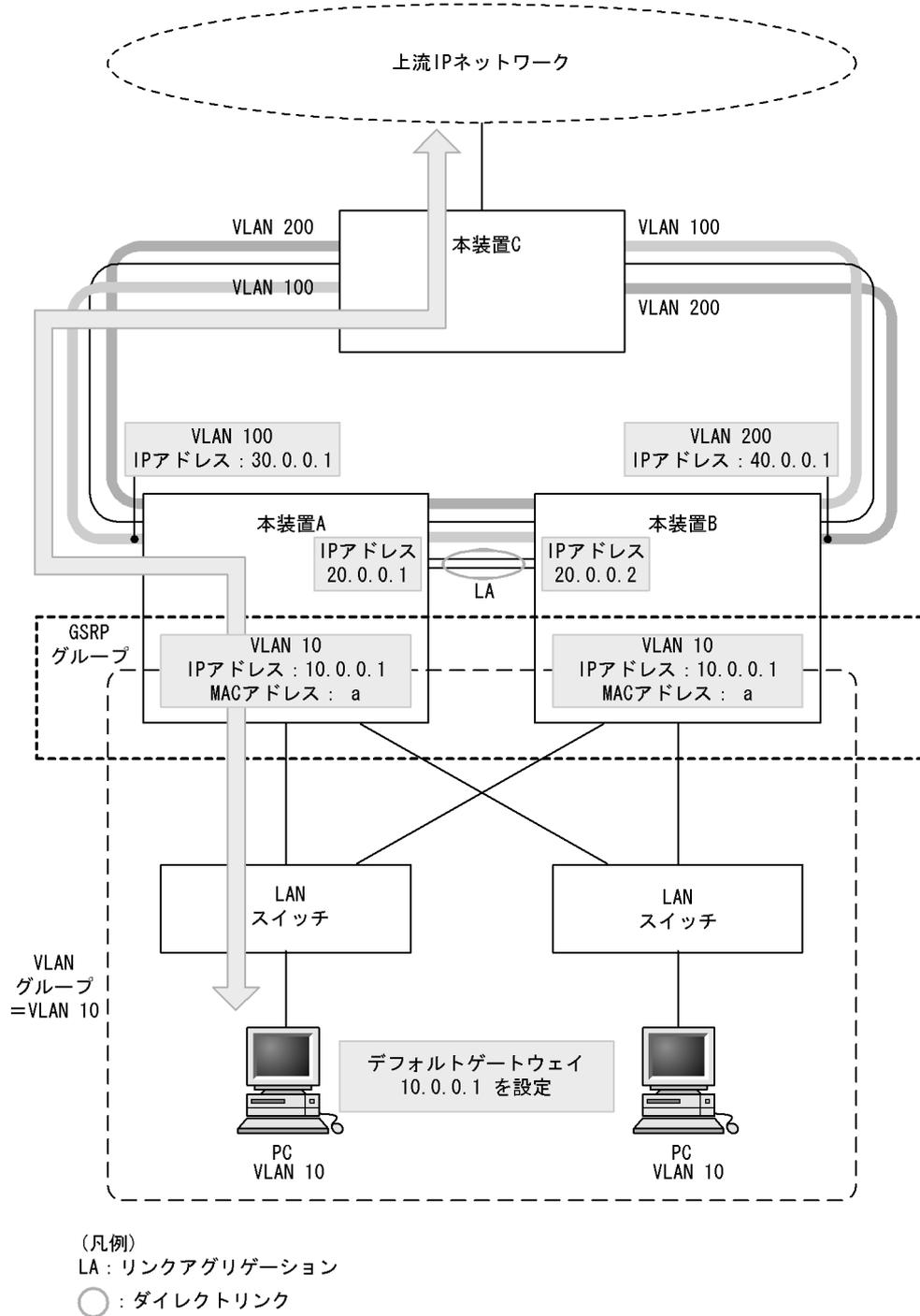
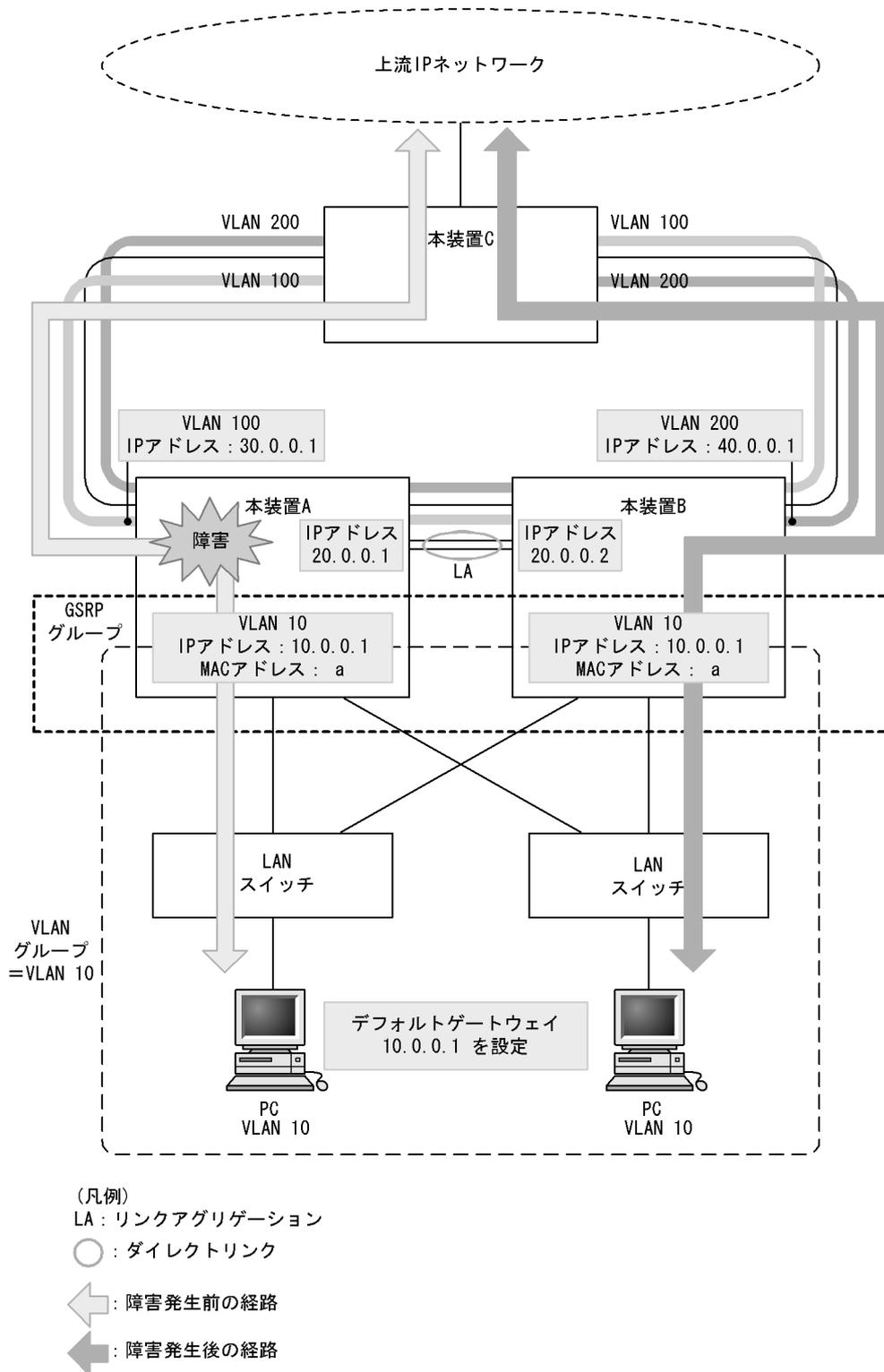


図 24-13 レイヤ 3 冗長切替機能 (障害発生時)



## 24.3 仮想リンクのコンフィグレーション

Ring Protocol とスパニングツリープロトコルを同一装置で併用するための仮想リンクを設定します。また、Ring Protocol と GSRP を併用する場合は、フラッシュフレームを送信するために仮想リンク VLAN の設定が必要です。

### 24.3.1 コンフィグレーションコマンド一覧

仮想リンクのコンフィグレーションコマンド一覧を次の表に示します。

表 24-4 コンフィグレーションコマンド一覧

| コマンド名             | 説明               |
|-------------------|------------------|
| axrp virtual-link | 仮想リンク ID を設定します。 |

### 24.3.2 仮想リンクの設定

#### [ 設定のポイント ]

仮想リンク ID および仮想リンク VLAN を設定します。仮想リンクを設定することで、Ring Protocol とスパニングツリー、または Ring Protocol と GSRP の併用が可能になります。同一拠点内の対向装置にも、同じ仮想リンク ID と仮想リンク VLAN を設定してください。また、仮想リンク VLAN は必ずデータ転送用 VLAN に使用している VLAN から一つ選んで使用してください。

#### [ コマンドによる設定 ]

1. (config)# axrp virtual-link 10 vlan 100  
仮想リンク ID を 10 に、仮想リンク VLAN を 100 に設定します。

### 24.3.3 Ring Protocol と PVST+ との併用設定

#### [ 設定のポイント ]

Ring Protocol と PVST+ とを併用する場合は、併用したい VLAN ID を VLAN マッピングに設定する必要があります。その際、VLAN マッピングに指定する VLAN ID は一つだけです。VLAN マッピングに対して、PVST+ と併用する VLAN 以外の VLAN ID が設定されている場合、その VLAN では PVST+ が動作しません。

#### [ コマンドによる設定 ]

1. (config)# axrp vlan-mapping 1 vlan 10  
VLAN マッピング ID を 1 として、PVST+ と併用する VLAN ID 10 を設定します。
2. (config)# axrp vlan-mapping 2 vlan 20,30  
VLAN マッピング ID を 2 として、Ring Protocol だけで使用する VLAN ID 20 および 30 を設定します。
3. (config)# axrp 1  
(config-axrp)# vlan-group 1 vlan-mapping 1-2  
VLAN グループ 1 に、VLAN マッピング ID 1 および 2 を設定します。

### 24.3.4 Ring Protocol とマルチプルスパニングツリーとの併用設定

#### [ 設定のポイント ]

Ring Protocol とマルチプルスパニングツリーを併用する場合は、併用したい VLAN ID を VLAN マッピングに設定する必要があります。その際、VLAN マッピングに指定する VLAN ID と MST インスタンスに所属する VLAN に指定する VLAN ID を一致させる必要があります。VLAN マッピングと MST インスタンスに所属する VLAN の VLAN ID が一致していない場合、一致していない VLAN の全ポートがブロッキング状態になります。

#### [ コマンドによる設定 ]

1. `(config)# axrp vlan-mapping 1 vlan 10,20,30`  
VLAN マッピング ID を 1 として、MST インスタンス 10 と併用する VLAN ID 10、20、および 30 を設定します。
2. `(config)# axrp vlan-mapping 2 vlan 40,50`  
VLAN マッピング ID を 2 として、MST インスタンス 20 と併用する VLAN ID 40 および 50 を設定します。
3. `(config)# axrp 1`  
`(config-axrp)# vlan-group 1 vlan-mapping 1-2`  
`(config-axrp)# exit`  
VLAN グループ 1 に、VLAN マッピング ID 1 および 2 を設定します。
4. `(config)# spanning-tree mst configuration`  
`(config-mst)# instance 10 vlans 10,20,30`  
MST インスタンス 10 に所属する VLAN に `vlan-mapping 1` で指定した VLAN ID 10、20、および 30 を設定し、Ring Protocol との共存を開始します。
5. `(config-mst)# instance 20 vlans 40,50`  
MST インスタンス 20 に所属する VLAN に `vlan-mapping 2` で指定した VLAN ID 40 および 50 を設定し、Ring Protocol との共存を開始します。

### 24.3.5 Ring Protocol と GSRP との併用設定

#### [ 設定のポイント ]

Ring Protocol と GSRP とを併用する際には、併用したい VLAN ID を VLAN マッピングと GSRP の VLAN グループに設定する必要があります。この際、VLAN マッピング ID と GSRP の VLAN グループ ID は一致している必要はありません。

#### [ コマンドによる設定 ]

1. `(config)# axrp vlan-mapping 1 vlan 10,15`  
VLAN マッピング ID を 1 に、GSRP と併用する VLAN ID 10 および 15 を設定します。
2. `(config)# axrp 1`  
`(config-axrp)# vlan-group 1 vlan-mapping 1`  
`(config-axrp)# exit`

VLAN グループ 1 に , VLAN マッピング ID 1 を設定します。

3. (config)# gsrp 1

(config-gsrp)# vlan-group 3 vlan 10,15

GSRP の VLAN グループ 3 に Ring Protocol と併用する VLAN ID 10 および 15 を設定します。

## 24.4 仮想リンクのオペレーション

### 24.4.1 運用コマンド一覧

仮想リンクの運用コマンド一覧を次の表に示します。

表 24-5 運用コマンド一覧

| コマンド名              | 説明                          |
|--------------------|-----------------------------|
| show spanning-tree | スパニングツリーでの仮想リンクの適用状態を表示します。 |
| show gsrp          | GSRP での仮想リンクの適用を表示します。      |

### 24.4.2 仮想リンクの状態の確認

仮想リンクの情報は show spanning-tree コマンドで確認してください。Port Information で仮想リンクポートが存在していることを確認してください。

show spanning-tree コマンドの実行結果を次の図に示します。

図 24-14 show spanning-tree コマンドの実行結果

```
> show spanning-tree vlan 2
Date 2007/11/04 11:39:43 UTC
VLAN 2 PVST+ Spanning Tree:Enabled Mode:PVST+
 Bridge ID Priority:4096 MAC Address:0012.e205.0900
 Bridge Status:Designated
 Root Bridge ID Priority:0 MAC Address:0012.e201.0900
 Root Cost:0
 Root Port:1/2-3 (VL:10) ... 1
Port Information
 1/1 Up Status:Forwarding Role:Designated
 VL(10) Up Status:Forwarding Role:Root ... 1
>
```

1. VL は、仮想リンク ID を示しています。

show gsrp detail コマンドで仮想リンクが運用されているか確認できます。Virtual Link ID で仮想リンク ID と仮想リンク VLAN を確認してください。

図 24-15 show gsrp detail コマンドの実行結果

```

>show gsrp detail
Date 2008/04/10 12:00:00 UTC

GSRP ID: 3
Local MAC Address : 0012.e2a8.2527
Neighbor MAC Address : 0012.e2a8.2505
Total VLAN Group Counts : 3
GSRP VLAN ID : 105
Direct Port : 1/10-11
GSRP Exception Port : 1/1-5
No Neighbor To Master : manual
Backup Lock : disable
Port Up Delay : 0
Last Flush Receive Time : -
Layer 3 Redundancy : On
Virtual Link ID : 100(VLAN ID : 20)

Advertise Hold Time Local Neighbor
: 5 5
Advertise Hold Timer : 4 -
Advertise Interval : 1 1
Selection Pattern : ports-priority-mac ports-priority-mac

VLAN Group ID Local State Neighbor State
1 Backup Master
2 (disable) -
8 Master -
>

```



# 25 ポリシーベーススイッチング

この章では、ポリシーベーススイッチングの解説と操作方法について説明します。

---

25.1 解説

---

25.2 コンフィグレーション

---

25.3 オペレーション

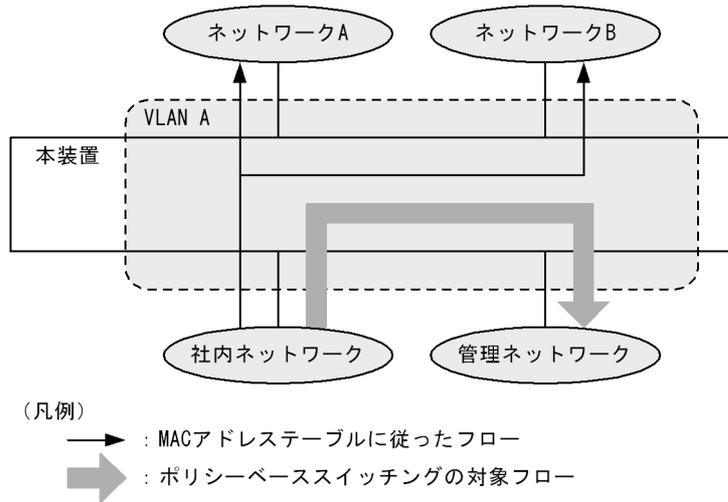
---

## 25.1 解説

ポリシーベーススイッチングは、MAC アドレス学習、コンフィグレーションコマンドで登録された MAC アドレステーブル、およびフラディングに従わないで、ユーザが設定した送信先インタフェースにフレームをレイヤ 2 中継する機能です。

ポリシーベーススイッチングの構成例を次の図に示します。

図 25-1 ポリシーベーススイッチングの構成例



この図で本装置は、社内ネットワークから受信してネットワーク A やネットワーク B へ送信するフレームのうち、特定のフレームだけを管理ネットワークに中継します。このように、本装置が受信したフレームのうち、特定のフレームを同一 VLAN 上の特定のネットワークに中継できます。また、負荷分散や認証などにも適用できます。

このようにポリシーベーススイッチングは、MAC アドレステーブルによる経路情報に関係なく、ユーザが指定した経路に従って中継できます。

なお、BSU-1A、CSU-1A、MSU-1A および MSU-1A1 では、ポリシーベーススイッチングは未サポートです。

### 25.1.1 ポリシーベーススイッチングの制御

ポリシーベーススイッチングはフィルタの一部機能として動作します。

受信側のイーサネットインタフェースに設定したフィルタのフロー検出条件に一致した場合、同アクセスリストに設定されているポリシーベーススイッチングの設定内容に従って、フレームを中継します。

ポリシーベーススイッチングは経路系テーブル容量が extended の場合に動作します。なお、ポリシーベーススイッチングの対象となるのはレイヤ 2 中継のフレームです。

ポリシーベーススイッチングを設定するには、アクセスリストの動作に、経路情報を登録したポリシーベーススイッチングリスト情報を指定します。この指定による機能をポリシーベーススイッチンググループといいます。

## 25.1.2 ポリシーベーススイッチンググループ

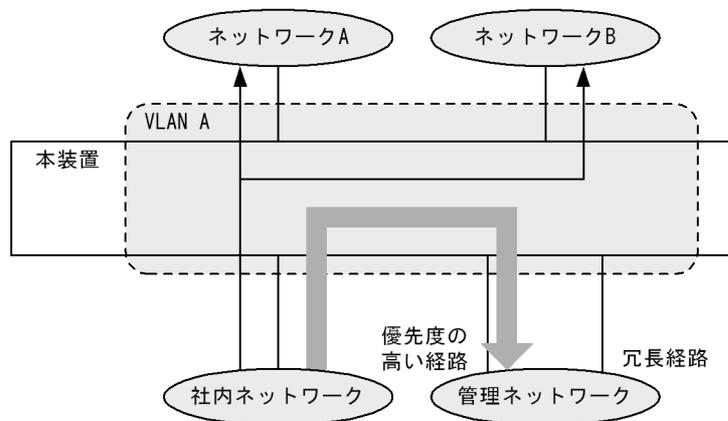
ポリシーベーススイッチンググループでは、一つまたは複数の経路をグループ化して設定できます。各経路は設定された適用順序に従って優先度を持ちます。これによって、送信先インタフェースの状況に合わせて、複数の経路の中から優先度の高い経路を動的に選択します。なお、一つまたは複数の経路をグループ化した情報をポリシーベーススイッチングリスト情報といいます。

ポリシーベーススイッチングリスト情報に複数の経路を指定することで、経路の冗長化ができます。障害などで優先度の高い経路が中継できなくなった場合、同じポリシーベーススイッチングリスト情報に設定している次に優先度の高い経路に切り替えて運用を継続します。

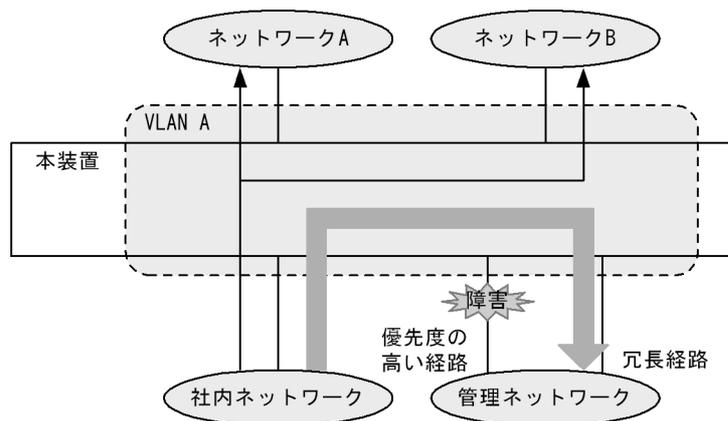
ポリシーベーススイッチンググループの構成例を次の図に示します。

図 25-2 ポリシーベーススイッチンググループの構成例

● 通常時



● 優先度の高い経路がダウンした場合



(凡例)

- : MACアドレステーブルに従ったフロー
- ➡ : ポリシーベーススイッチングの対象フロー

### (1) ポリシーベーススイッチンググループの経路選択

ポリシーベーススイッチンググループでは、ポリシーベーススイッチングリスト情報に登録した複数の経

路から次の情報を基に経路を選択します。

- 中継可否の監視結果と優先度
- デフォルト動作指定
- 経路切り戻し動作指定

#### (a) 中継可否の監視結果と優先度

ポリシーベーススイッチングリスト情報に登録した経路は、次に示す監視の結果によって中継可否が決定します。

- 送信先イーサネットインタフェースのポート状態の監視
- 送信先リンクアグリゲーションのチャンネルグループ状態の監視

また、中継可能な経路のうち、最も優先度の高い経路を選択します。

##### 送信先イーサネットインタフェースのポート状態の監視

次に示すコンフィグレーションコマンドで中継先の経路を指定したとき、送信先イーサネットインタフェースのポートの状態によって中継可否を判断します。

- policy-vlan コマンド  
送信先イーサネットインタフェースの VLAN ID
- policy-interface コマンド  
送信先イーサネットインタフェースの NIF 番号 / ポート番号

送信先イーサネットインタフェースのポートが Up のときだけ、中継可能と判断します。

##### 送信先リンクアグリゲーションのチャンネルグループ状態の監視

次に示すコンフィグレーションコマンドで中継先の経路を指定したとき、送信先リンクアグリゲーションのチャンネルグループの状態によって中継可否を判断します。

- policy-vlan コマンド  
送信先イーサネットインタフェースの VLAN ID
- policy-channel-group コマンド  
チャンネルグループ番号

送信先リンクアグリゲーションのチャンネルグループが Up のときだけ、中継可能と判断します。

##### 優先度による決定

送信先イーサネットインタフェースのポート状態の監視または送信先リンクアグリゲーションのチャンネルグループ状態の監視の結果を基に、ポリシーベーススイッチングリスト情報内で中継可能な経路のうち、コンフィグレーションで指定した適用順序で、最も優先度の高い経路を選択します。

#### (b) デフォルト動作指定

ポリシーベーススイッチングリスト情報に登録している経路がすべて中継できない、または経路が登録されていない場合の動作をデフォルト動作といいます。デフォルト動作はコンフィグレーションコマンド default で指定できます。デフォルト動作指定について次の表に示します。

表 25-1 デフォルト動作指定

| コンフィグレーションでの指定 | デフォルト動作 | 動作説明                                 |
|----------------|---------|--------------------------------------|
| permit 指定      | 通常中継    | 対象のフレームを MAC アドレステーブルに従ってレイヤ 2 中継します |

| コンフィグレーションでの指定 | デフォルト動作 | 動作説明          |
|----------------|---------|---------------|
| deny 指定        | 廃棄      | 対象のフレームを廃棄します |
| 未指定            | 廃棄      | 対象のフレームを廃棄します |

デフォルト動作によって MAC アドレステーブルに従ってフレームをレイヤ 2 中継または廃棄した場合、対象のポリシーベーススイッチングリスト情報を指定しているアクセスリストの統計情報にカウントされます。

### (c) 経路切り戻し動作指定

ポリシーベーススイッチングリスト情報に登録している優先度の高い経路が中継できなくなって優先度の低い経路で中継している状態で、優先度の高い経路が中継可能になった場合の動作を経路切り戻し動作といいます。経路切り戻し動作はコンフィグレーションコマンド `recover` で指定できます。経路切り戻し動作指定について次の表に示します。

表 25-2 経路切り戻し動作指定

| コンフィグレーションでの指定 | 経路切り戻し動作 | 動作説明                          |
|----------------|----------|-------------------------------|
| on 指定          | 切り戻す     | 優先度の高い経路が中継可能になると、経路を切り戻します   |
| off 指定         | 切り戻さない   | 優先度の高い経路が中継可能になっても、経路を切り戻しません |
| 未指定            | 切り戻す     | 優先度の高い経路が中継可能になると、経路を切り戻します   |

経路切り戻し動作として「切り戻す」を指定すると、ポリシーベーススイッチングリスト情報内で中継可能な経路のうち、常に最も優先度の高い経路を選択します。

経路切り戻し動作として「切り戻さない」を指定すると、選択中の経路より優先度の高い経路が中継可能になっても切り戻しません。選択中の経路が中継できなくなると、常により優先度の低い経路へ切り替えます。ポリシーベーススイッチングリスト情報に登録しているすべての経路が中継できない場合、経路を切り戻さないでデフォルト動作になります。ただし、次の場合にはポリシーベーススイッチングリスト情報内で中継可能な経路のうち、最も優先度の高い経路を再選択します。

- 運用コマンド `reset policy-switch-list` の実行
- コンフィグレーションコマンド `recover` で経路切り戻し動作を「切り戻す」に変更
- ポリシーベースプログラムの再起動
- 系切替後、中継可否の監視を一時的に停止する時間が経過

## (2) 起動時のポリシーベーススイッチンググループ

本装置では起動時や再起動時など、ポリシーベースプログラムが動作してから一定時間、中継可否の監視および経路の切り替えを停止します。これは、次に示す理由で、起動したあとの装置状態を収集し終わるまで、中継可否の監視結果が安定しないためです。

- イーサネットインタフェースのポートが Up していない
- リンクアグリゲーションのチャンネルグループが Up していない

ポリシーベースプログラムが動作してからポリシーベーススイッチンググループが中継可否の監視を始めるまでの経路の状態を起動中といいます。起動中はポリシーベーススイッチングの対象フレームをすべて廃棄します。

なお、起動中に次のコンフィグレーションコマンドでポリシーベーススイッチングリスト情報を変更した

場合、中継可否の監視を始めた時点で変更が反映されます。

- default ( policy-switch-list )
- policy-channel-group ( policy-switch-list )
- policy-interface ( policy-switch-list )
- policy-switch-list
- policy-vlan ( policy-switch-list )
- recover ( policy-switch-list )

ポリシーベースプログラムが動作してから中継可否の監視を始めるまでの時間（中継可否の監視を停止する時間）は、コンフィグレーションコマンド `policy-switch-list default-init-interval` で変更できます。起動したあとの、中継可否の監視結果が安定するまでに掛かる時間を目安として指定してください。起動中の状態遷移と遷移条件について次の表に示します。

表 25-3 起動中の状態遷移と遷移条件

| 状態遷移   | 遷移条件                                                                                                                                                                                                                 |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 起動中の終了 | 中継可否の監視を停止する時間が経過すると起動中を終了します。また、起動中を中断した場合も同様に起動中を終了します。                                                                                                                                                            |
| 起動中を中断 | 次の場合に起動中を中断します。 <ul style="list-style-type: none"> <li>• 運用コマンド <code>reset policy-switch-list</code> の実行</li> <li>• コンフィグレーションで、中継可否の監視を停止する時間を現在の経過時間よりも短く変更</li> <li>• ポリシーベースプログラムの再起動</li> <li>• 系切替</li> </ul> |
| 起動中の延長 | コンフィグレーションで、中継可否の監視を停止する時間をより長く変更すると起動中を延長します。この場合、変更後の時間から現在の経過時間を差し引いた時間が経過すると、中継可否の監視を開始します。                                                                                                                      |

起動中に系切替すると、切替中を終了または中断するまでの間、ポリシーベーススイッチングリスト情報の対象フレームはすべて廃棄されます。

起動中を終了または中断すると、ポリシーベーススイッチングリスト情報内で中継可能な経路のうち、最も優先度の高い経路を選択します。

### (3) 系切替時のポリシーベーススイッチンググループ

本装置の BCU、CSU または MSU を冗長化している場合、系切替が発生してから一定時間、中継可否の監視および経路の切り替えを停止します。これは、系切替したあとの装置状態を収集し終わるまで、中継可否の監視結果が安定しないためです。

系切替してからポリシーベーススイッチンググループが中継可否の監視を始めるまでの経路の状態を切替中といいます。切替中は経路を切り替えないで、系切替前に選択していた経路を引き継ぎます。

なお、切替中に次のコンフィグレーションコマンドでポリシーベーススイッチングリスト情報を変更した場合、中継可否の監視を始めた時点で変更が反映されます。

- default ( policy-switch-list )
- policy-channel-group ( policy-switch-list )
- policy-interface ( policy-switch-list )
- policy-switch-list
- policy-vlan ( policy-switch-list )
- recover ( policy-switch-list )

ただし、ポリシーベーススイッチングリスト情報を設定しているアクセスリストのコンフィグレーション

を変更した場合は、ポリシーベーススイッチングリスト情報の対象フレームはすべて廃棄されます。

系切替してから中継可否の監視を始めるまでの時間（中継可否の監視を停止する時間）は、コンフィグレーションコマンド `policy-switch-list default-aging-interval` で変更できます。系切替したあとの、フレームの送受信が安定するまでに掛かる時間を目安として指定してください。切替中の状態遷移と遷移条件について次の表に示します。

表 25-4 切替中の状態遷移と遷移条件

| 状態遷移   | 遷移条件                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 切替中の終了 | 中継可否の監視を停止する時間が経過すると切替中を終了します。<br>また、切替中を中断した場合も同様に切替中を終了します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 切替中を中断 | 次の場合に切替中を中断します。 <ul style="list-style-type: none"> <li>運用コマンド <code>reset policy-switch-list</code> の実行</li> <li>コンフィグレーションで、中継可否の監視を停止する時間を現在の経過時間よりも短く変更</li> <li>ポリシーベースプログラムの再起動</li> <li>次に示すコンフィグレーションコマンドを実行して、BSU または PSP が再起動 <ul style="list-style-type: none"> <li><code>fldm prefer</code></li> <li><code>fwdm prefer</code></li> <li><code>vrf mode</code> <b>【OP-NPAR】</b></li> </ul> </li> <li>運用コマンド <code>restart vlan</code> の実行</li> <li>運用コマンド <code>activate bsu</code> を実行して、装置内で 1 枚目の BSU を active 状態に変更</li> </ul> |
| 切替中の延長 | コンフィグレーションで、中継可否の監視を停止する時間をより長く変更すると切替中を延長します。この場合、変更後の時間から現在の経過時間を差し引いた時間が経過すると、中継可否の監視を開始します。<br>また、BCU、CSU または MSU の系切替が再度発生すると、中継可否の監視を停止する時間をカウントし直すため、切替中を継続します。                                                                                                                                                                                                                                                                                                                                                                      |

切替中を終了または中断すると、ポリシーベーススイッチングリスト情報内で中継可能な経路のうち、最も優先度の高い経路を選択して経路を切り替えます。

なお、系切替については、「コンフィグレーションガイド Vol.2 17. BCU/CSU/MSU の冗長化」を参照してください。

### 25.1.3 ポリシーベーススイッチング対象フレーム

ポリシーベーススイッチングの対象となるフレームについて次の表に示します。

表 25-5 ポリシーベーススイッチングの対象フレーム

| フレーム種別      | アドレス種別   | 対象可否           |
|-------------|----------|----------------|
| 非 IP パケット   |          | 1              |
| IPv4 パケット   | ユニキャスト   | 2              |
|             | マルチキャスト  |                |
|             | ブロードキャスト |                |
| IPv6 パケット   | ユニキャスト   | 3              |
|             | マルチキャスト  |                |
| 自宛非 IP パケット |          | × <sup>4</sup> |
| 自宛 IP パケット  |          | ×              |
| 自発非 IP パケット |          | ×              |
| 自発 IP パケット  |          | ×              |

(凡例) :対象 x:対象外

注 1

次のフレームは対象外です。

- ・ LACPDU
- ・ LLDP PDU
- ・ IEEE802.3ah/UDLD で使用する制御フレーム
- ・ GSRP で使用する制御フレーム
- ・ 回線テストフレーム

これら以外に、他機能との共存によって対象外となるフレームがあります。「25.1.4 ポリシーベーススイッチングと他機能との共存」を参照してください。

なお、アクセスリストの検出条件に一致した場合、ポリシーベーススイッチングは動作しませんが、該当するアクセスリストの統計情報にカウントされます。

また、ポリシーベーススイッチングがデフォルト動作に従っていて、かつデフォルト動作が廃棄のときは廃棄しません。

注 2

次のフレームは対象外です。

- ・ IGMP パケット

なお、アクセスリストの検出条件に一致した場合、ポリシーベーススイッチングは動作しませんが、該当するアクセスリストの統計情報にカウントされます。

また、ポリシーベーススイッチングがデフォルト動作に従っていて、かつデフォルト動作が廃棄のときは廃棄しません。

注 3

次のフレームは対象外です。

- ・ MLD パケット

なお、アクセスリストの検出条件に一致した場合、ポリシーベーススイッチングは動作しませんが、該当するアクセスリストの統計情報にカウントされます。

また、ポリシーベーススイッチングがデフォルト動作に従っていて、かつデフォルト動作が廃棄のときは廃棄しません。

注 4

アクセスリストの検出条件に一致した場合、ポリシーベーススイッチングは動作しませんが、該当するアクセスリストの統計情報にカウントされます。

## 25.1.4 ポリシーベーススイッチングと他機能との共存

ポリシーベーススイッチングと他機能との共存とは、ポリシーベーススイッチングリスト情報を動作に指定したアクセスリストを適用しているイーサネットインタフェースに、他機能を設定することを示します。ポリシーベーススイッチングと他機能との共存を次の表に示します。

表 25-6 ポリシーベーススイッチングと他機能との共存

| 機能名           |                | 共存仕様                                                                                                         |
|---------------|----------------|--------------------------------------------------------------------------------------------------------------|
| VLAN 拡張機能     | BPDU フォワーディング  | BPDU はポリシーベーススイッチングの対象外フレーム ですが、BPDU フォワーディングを設定している場合はポリシーベーススイッチングの対象フレームになります。                            |
|               | EAPOL フォワーディング | EAPOL はポリシーベーススイッチングの対象外フレーム ですが、EAPOL フォワーディングを設定している場合はポリシーベーススイッチングの対象フレームになります。                          |
| Ring Protocol |                | Ring Protocol を設定している場合、本装置のマスターノードのプライマリポートおよびセカンダリポートでは、Ring Protocol の制御フレームはポリシーベーススイッチングの対象外フレーム になります。 |

| 機能名           | 共存仕様                                                                                                                        |
|---------------|-----------------------------------------------------------------------------------------------------------------------------|
| DHCP snooping | 「コンフィグレーションガイド Vol.2 15.1.7 DHCP snooping 使用時の注意事項」を参照してください。                                                               |
| L2 ループ検知      | L2 ループ検知を設定している場合、本装置から送信した L2 ループ検知フレームはポリシーベーススイッチングの対象外フレームになります。なお、本装置以外からの L2 ループ検知フレームはポリシーベーススイッチングの対象フレームになります。     |
| CFM           | CFM を設定している場合、CFM PDU のうちループバックメッセージおよびリンクトレースメッセージはポリシーベーススイッチングの対象外フレーム になります。また、本装置宛での CCM もポリシーベーススイッチングの対象外フレーム になります。 |
| OADP          | OADP を設定している場合、OADP PDU および CDP PDU はポリシーベーススイッチングの対象外フレーム になります。                                                           |

## 注

アクセスリストの検出条件に一致した場合、ポリシーベーススイッチングは動作しませんが、該当するアクセスリストの統計情報にカウントされます。

また、ポリシーベーススイッチングがデフォルト動作に従っていて、かつデフォルト動作が廃棄のときは廃棄しません。

### 25.1.5 ポリシーベーススイッチングの注意事項

#### (1) ポリシーベーススイッチングとフロー制御の併用について

ポリシーベーススイッチングの対象となるフレームを QoS フローリストで検出した場合、ポリシーベーススイッチングによる中継と QoS フローリストで設定したフロー制御がどちらも動作します。

#### (2) ポリシーベーススイッチングリスト情報の経路切り戻し動作として「切り戻さない」を指定した場合について

ポリシーベーススイッチングリスト情報の経路切り戻し動作として「切り戻さない」を指定している状態で運用コマンド `restart vlan` を実行すると、デフォルト動作に従わないことがあります。この場合はすべてのインタフェースの初期化が完了したあと、運用コマンド `reset policy-switch-list` を実行してください。

#### (3) 起動時のポリシーベーススイッチンググループ

ポリシーベースプログラムが動作したあと、中継可否の監視を停止する時間が経過して中継可能な経路のうち最も優先度の高い経路を選択した場合、ポリシーベーススイッチングリスト情報の運用ログやトラップは出力しません。

#### (4) 系切替時のポリシーベーススイッチンググループ

- 系切替の直前に経路の切り替えが発生すると、経路の設定が装置に反映されないことがあります。未設定の経路は、系切替したあと中継可否の監視を停止する時間が経過すると反映されます。
- 系切替したあと、中継可否の監視を停止する時間が経過して中継可能な経路のうち最も優先度の高い経路を再選択した場合、ポリシーベーススイッチングリスト情報の運用ログやトラップは出力しません。

#### (5) ポリシーベースプログラムの再起動

ポリシーベーススイッチンググループとポリシーベースルーティンググループは、ポリシーベースプログラムで制御しています。そのため、ポリシーベースプログラムが再起動すると、どちらの機能にも影響があります。

(6) ポリシーベーススイッチングとストームコントロールの併用について

「[コンフィグレーションガイド Vol.2 25.1.2 ストームコントロール使用時の注意事項](#)」を参照してください。

## 25.2 コンフィグレーション

### 25.2.1 コンフィグレーションコマンド一覧

ポリシーベーススイッチングのコンフィグレーションコマンド一覧を次の表に示します。

表 25-7 コンフィグレーションコマンド一覧

| コマンド名                                        | 説明                                                        |
|----------------------------------------------|-----------------------------------------------------------|
| default                                      | ポリシーベーススイッチングリスト情報のデフォルト動作を設定します。                         |
| policy-channel-group                         | ポリシーベーススイッチングリスト情報に経路を設定します。                              |
| policy-interface                             | ポリシーベーススイッチングリスト情報に経路を設定します。                              |
| policy-switch-list                           | ポリシーベーススイッチングリスト情報を設定します。                                 |
| policy-switch-list<br>default-aging-interval | 系切替時にポリシーベーススイッチングの中継可否の監視を停止する時間を設定します。                  |
| policy-vlan                                  | ポリシーベーススイッチングリスト情報に VLAN インタフェースを設定します。                   |
| recover                                      | ポリシーベーススイッチングリスト情報の経路切り戻し動作を設定します。                        |
| access-list                                  | IPv4 フィルタとして動作するアクセスリストを設定します。                            |
| advance access-group                         | イーサネットインタフェースに対して Advance フィルタを適用し、Advance フィルタ機能を有効にします。 |
| advance access-list                          | Advance フィルタとして動作するアクセスリストを設定します。                         |
| ip access-group                              | イーサネットインタフェースに対して IPv4 フィルタを適用し、IPv4 フィルタ機能を有効にします。       |
| ip access-list extended                      | IPv4 パケットフィルタとして動作するアクセスリストを設定します。                        |
| ipv6 access-list                             | IPv6 パケットフィルタとして動作するアクセスリストを設定します。                        |
| ipv6 traffic-filter                          | イーサネットインタフェースに対して IPv6 フィルタを適用し、IPv6 フィルタ機能を有効にします。       |
| mac access-group                             | イーサネットインタフェースに対して MAC フィルタを適用し、MAC フィルタ機能を有効にします。         |
| mac access-list extended                     | MAC フィルタとして動作するアクセスリストを設定します。                             |
| permit                                       | フィルタでのアクセス中継する条件を指定します。                                   |

注

「コンフィグレーションコマンドレファレンス Vol.2 4. アクセスリスト」を参照してください。

### 25.2.2 ポリシーベーススイッチングの設定

ポリシーベーススイッチングを設定する例を次に示します。

#### (1) ポリシーベーススイッチンググループの設定

IPv4 パケットをフロー検出条件として、ポリシーベーススイッチングリスト情報を設定する例を示します。

[ 設定のポイント ]

アクセスリストを使用してポリシーベーススイッチングリスト情報を設定します。

## [ コマンドによる設定 ]

1. (config)# policy-switch-list 10  
ポリシーベーススイッチングリスト情報をリスト番号 10 で設定します。本リストを作成すると、ポリシーベーススイッチングリスト情報のモードに移行します。
2. (config-pol-sw)# policy-vlan 100  
ポリシーベーススイッチングリスト情報の VLAN ID を 100 で設定します。
3. (config-pol-sw)# policy-interface gigabitethernet 1/2  
ポリシーベーススイッチングリスト情報に優先度の高い経路として、ポート 1/2 を設定します。
4. (config-pol-sw)# policy-interface gigabitethernet 1/3  
ポリシーベーススイッチングリスト情報に冗長経路として、ポート 1/3 を設定します。
5. (config-pol-sw)# default permit  
ポリシーベーススイッチングリスト情報のデフォルト動作に通常中継を設定します。
6. (config-pol-sw)# exit  
ポリシーベーススイッチングリスト情報のモードからグローバルコンフィグレーションモードに戻ります。
7. (config)# ip access-list extended POLICY\_SW\_GROUP  
ip access-list (POLICY\_SW\_GROUP) を作成します。本リストを作成すると、IPv4 パケットフィルタの動作モードに移行します。
8. (config-ext-nacl)# permit tcp any any vlan 100 action policy-switch-list 10  
VLAN100 の IPv4 パケットをポリシーベーススイッチングするポリシーベーススイッチングリスト情報を設定します。リスト番号には 10 を設定します。
9. (config-ext-nacl)# permit ip any any  
すべてのフレームを中継する IPv4 パケットフィルタを設定します。
10. (config-ext-nacl)# exit  
IPv4 パケットフィルタの動作モードからグローバルコンフィグレーションモードに戻ります。
11. (config)# interface gigabitethernet 1/1  
ポート 1/1 のインタフェースモードに移行します。
12. (config-if)# ip access-group POLICY\_SW\_GROUP in layer2-forwarding  
受信側にレイヤ 2 中継を対象とするポリシーベーススイッチングを設定した IPv4 フィルタを有効にします。

## (2) 経路切り戻し動作に「切り戻さない」を設定

中継先の経路を設定済みのポリシーベーススイッチングリスト情報の経路切り戻し動作として、「切り戻さない」を設定する例を次に示します。

## [ 設定のポイント ]

経路切り戻し動作に「切り戻さない」を設定したときは、運用コマンド `show cache policy-switch` で対象のポリシーベーススイッチングリスト情報に反映されていることを確認してください。

## [ コマンドによる設定 ]

1. `(config)# policy-switch-list 10`

リスト番号 10 のポリシーベーススイッチングリスト情報のモードに移行します。

2. `(config-pol-sw)# recover off`

経路切り戻し動作に「切り戻さない」を設定します。設定したあとは運用コマンド `show cache policy-switch 10` を実行してください。

## 25.3 オペレーション

### 25.3.1 運用コマンド一覧

ポリシーベーススイッチングの運用コマンド一覧を次の表に示します。

表 25-8 運用コマンド一覧

| コマンド名                    | 説明                                                                                                                                                                                                                      |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show policy-switch       | 指定したイーサネットインタフェースに設定しているアクセスリスト、およびポリシーベーススイッチングリスト情報を表示します。                                                                                                                                                            |
| show cache policy-switch | 指定したポリシーベーススイッチングリスト情報の経路情報と状態を表示します。                                                                                                                                                                                   |
| reset policy-switch-list | 経路情報を再選択します。                                                                                                                                                                                                            |
| restart policy           | ポリシーベースプログラムを再起動します。                                                                                                                                                                                                    |
| show access-filter       | アクセスグループコマンド ( ip access-group , ipv6 traffic-filter , mac access-group , advance access-group ) で設定したアクセスリスト ( access-list , ip access-list , ipv6 access-list , mac access-list , advance access-list ) の統計情報を表示します。  |
| clear access-filter      | アクセスグループコマンド ( ip access-group , ipv6 traffic-filter , mac access-group , advance access-group ) で設定したアクセスリスト ( access-list , ip access-list , ipv6 access-list , mac access-list , advance access-list ) の統計情報をクリアします。 |

注

「運用コマンドレファレンス Vol.2 2. フィルタ」を参照してください。

### 25.3.2 ポリシーベーススイッチングの確認

#### (1) ポリシーベーススイッチンググループの確認

ポリシーベーススイッチンググループの動作を確認する方法を示します。

show policy-switch コマンドを実行して、イーサネットインタフェースのポート番号からポリシーベーススイッチングリスト情報を設定しているアクセスリストの情報が表示されることを確認します。

図 25-3 show policy-switch コマンドの実行結果

```
> show policy-switch
Date 2012/01/01 12:00:00 UTC
Port Access List Name/Number Sequence Policy Switch List
1/ 1 POLICY_SW_GROUP 10 10
```

show access-filter コマンドを実行して、ポリシーベーススイッチングリスト情報を設定したアクセスリストの動作を確認できます。指定したイーサネットインタフェースのフィルタに「Extended IP access-list:POLICY\_SW\_GROUP layer2-forwarding」および「action policy-switch-list 10」が表示されること、「matched packets」がカウントされていることを確認します。

図 25-4 show access-filter コマンドの実行結果

```
> show access-filter 1/1 POLICY_SW_GROUP in
Date 2012/01/01 12:00:00 UTC
Using Port:1/1 in
Extended IP access-list:POLICY_SW_GROUP layer2-forwarding
 remark "permit Policy SW Group policy"
 permit tcp(6) any any vlan 100 action policy-switch-list 10
 matched packets : 74699826
 permit ip any any
 matched packets : 264176
 implicitly denied packets: 0
```

show cache policy-switch コマンドを実行して、ポリシーベーススイッチングリスト情報内で選択している経路を確認できます。指定したポリシーベーススイッチングリスト情報に設定している経路がすべて表示されること、すべての経路のうち選択している経路を示す「\*>」が表示されることを確認します。

図 25-5 show cache policy-switch コマンドの実行結果（経路の確認）

```
> show cache policy-switch 10
Date 2012/01/01 12:00:00 UTC
Policy Base Switching Default Init Interval : 200
 Start Time : 2012/01/01 00:00:00
 End Time : 2012/01/01 00:03:20
Policy Base Switching Default Aging Interval : 200
 Start Time : 2012/01/01 01:00:00
 End Time : 2012/01/01 01:03:20
Policy Base Switching List : 10
 Default : Permit
 Recover : On
 Priority Sequence VLAN ID Status Output Interface
*> 1 10 100 Up 1/2
 2 20 100 Up 1/3
```

## (2) 経路切り戻し動作の確認

show cache policy-switch コマンドを実行して、ポリシーベーススイッチングリスト情報に設定されている経路切り戻し動作を確認できます。

図 25-6 show cache policy-switch コマンドの実行結果（経路切り戻し動作の確認）

```
> show cache policy-switch 10
Date 2012/01/01 12:00:00 UTC
Policy Base Switching Default Init Interval : 200
 Start Time : 2012/01/01 00:00:00
 End Time : 2012/01/01 00:03:20
Policy Base Switching Default Aging Interval : 200
 Start Time : 2012/01/01 01:00:00
 End Time : 2012/01/01 01:03:20
Policy Base Switching List : 10
 Default : Permit
 Recover : Off
 Priority Sequence VLAN ID Status Output Interface
*> 1 10 100 Up 1/2
 2 20 100 Up 1/3
```

1. 「Recover : Off」の場合は、経路切り戻し動作として「切り戻さない」が設定されています。



# 26 IGMP snooping/MLD snooping の解説

IGMP snooping/MLD snooping はレイヤ 2 スイッチで VLAN 内のマルチキャストトラフィックを制御する機能です。この章では、IGMP snooping/MLD snooping について説明します。

- 
- 26.1 IGMP snooping/MLD snooping の概要
  - 26.2 IGMP snooping/MLD snooping サポート機能
  - 26.3 IGMP snooping
  - 26.4 MLD snooping
  - 26.5 IGMP snooping/MLD snooping 使用時の注意事項
-

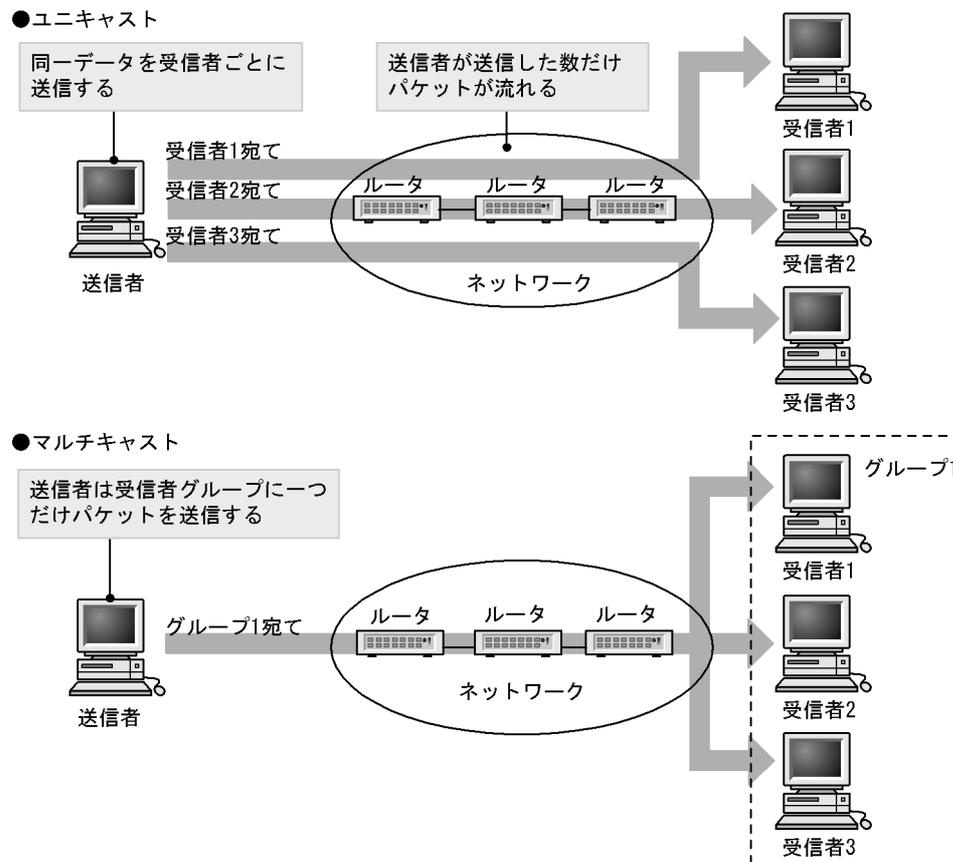
## 26.1 IGMP snooping/MLD snooping の概要

この節では、マルチキャスト、IGMP snooping および MLD snooping の概要について説明します。

### 26.1.1 マルチキャスト概要

同一の情報を複数の受信者に送信する場合、ユニキャストでは送信者が受信者の数だけデータを複製して送信するため、送信者とネットワークの負荷が高くなります。マルチキャストでは送信者がネットワーク内で選択されたグループに対してデータを送信します。送信者は受信者ごとにデータを複製する必要がないため、受信者の数に関係なくネットワークの負荷を軽減できます。マルチキャスト概要を次の図に示します。

図 26-1 マルチキャスト概要



マルチキャストで送信する場合に、宛先アドレスにはマルチキャストグループアドレスを使用します。マルチキャストグループアドレスを次の表に示します。

表 26-1 マルチキャストグループアドレス

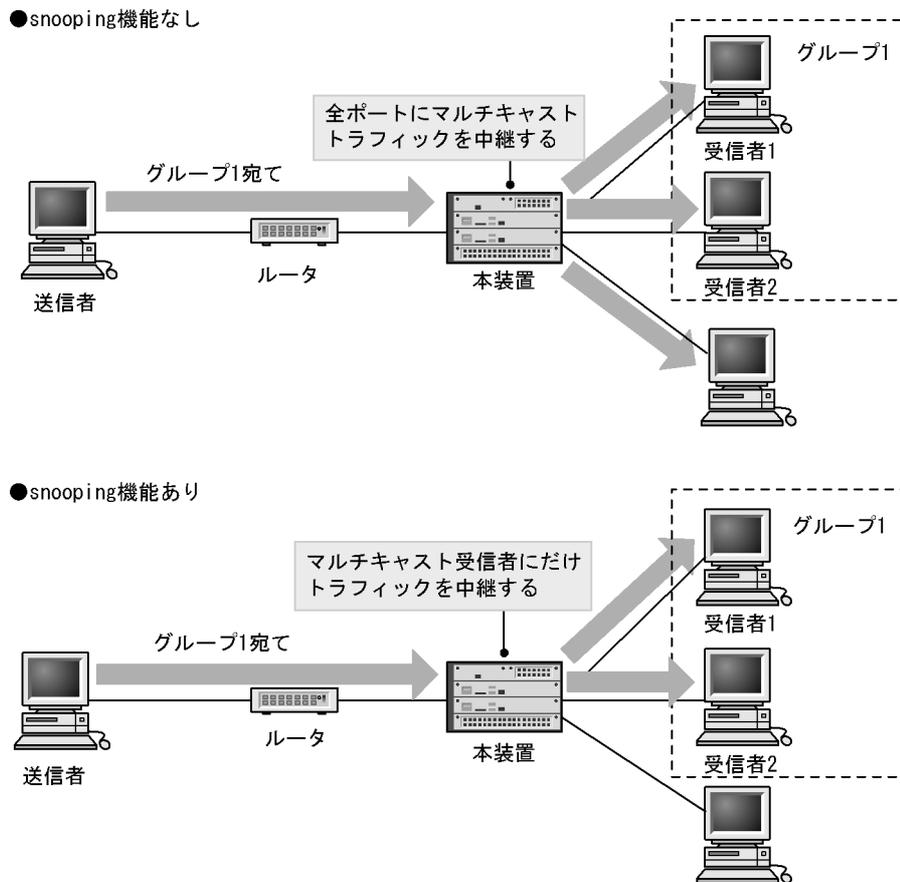
| プロトコル | アドレス範囲                            |
|-------|-----------------------------------|
| IPv4  | 224.0.0.0 ~ 239.255.255.255       |
| IPv6  | 上位 8 ビットが ff(16 進数) となる IPv6 アドレス |

## 26.1.2 IGMP snooping および MLD snooping 概要

レイヤ 2 スイッチはマルチキャストトラフィックを VLAN 内の全ポートに中継します。そのため、レイヤ 2 スイッチが接続されているネットワークでマルチキャストを使用すると、マルチキャストトラフィックの受信者がいないポートに不要なマルチキャストトラフィックが流れることになります。

IGMP snooping および MLD snooping は、IGMP あるいは MLD メッセージを監視して、受信者が接続しているポートに対してマルチキャストトラフィックを中継します。この機能を利用することで、不要なマルチキャストトラフィックの中継を抑止し、ネットワークを効率的に利用することができます。IGMP snooping/MLD snooping 概要を次の図に示します。

図 26-2 IGMP snooping/MLD snooping 概要



マルチキャストトラフィックの受信者が接続するポートを検出するため、本装置はグループ管理プロトコルのパケットを監視します。グループ管理プロトコルは、ルータホスト間でグループメンバーシップ情報を送受信するプロトコルで、IPv4 ネットワークでは IGMP が使用され、IPv6 ネットワークでは MLD が使用されます。ホストから送信されるグループ参加・離脱報告を示すパケットを検出することで、どの接続ポートへマルチキャストトラフィックを中継すべきかを学習します。

## 26.2 IGMP snooping/MLD snooping サポート機能

本装置がサポートする IGMP snooping/MLD snooping 機能を次の表に示します。

表 26-2 サポート機能

| 項目                              | サポート内容                                                                                                                 | 備考                              |             |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------|---------------------------------|-------------|
| インタフェース種別                       | 全イーサネットをサポート<br>フレーム形式は Ethernet V2 だけ                                                                                 | -                               |             |
| IGMP サポートバージョン<br>MLD サポートバージョン | IGMP: Version 1, 2, 3<br>MLD: Version 1, 2                                                                             | -                               |             |
| この機能による学習                       | IPv4                                                                                                                   | 0100.5e00.0000 ~ 0100.5eff.ffff | RFC1112 を参照 |
| MAC アドレス範囲                      | IPv6                                                                                                                   | 3333.0000.0000 ~ 3333.ffff.ffff | RFC2464 を参照 |
| IGMP クエリア<br>MLD クエリア           | クエリア動作は IGMPv2/IGMPv3, MLDv1/<br>MLDv2 の仕様に従う                                                                          | -                               |             |
| マルチキャストルータ接続ポートの<br>設定          | コンフィグレーションによる static 設定                                                                                                | -                               |             |
| IGMP 即時離脱機能                     | IGMPv2 Leave メッセージ, またはマルチキャスト<br>アドレスレコードタイプが<br>CHANGE_TO_INCLUDE_MODE の IGMPv3<br>Report (離脱要求) メッセージの受信による即時<br>離脱 | -                               |             |

(凡例) - : 該当なし

## 26.3 IGMP snooping

ここでは、IGMP snooping の機能と動作について説明します。本装置が送受信する IGMP メッセージのフォーマットおよびタイムは RFC2236 に従います。また、IGMP バージョン 3 (以降、IGMPv3) メッセージのフォーマットおよび設定値は RFC3376 に従います。

### 26.3.1 MAC アドレスの学習

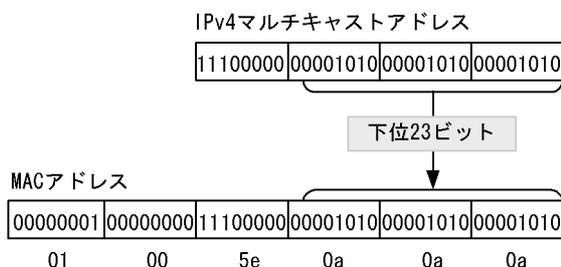
IGMP snooping が設定された VLAN で IGMP メッセージを受信することによってマルチキャスト MAC アドレスを動的に学習します。学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。

#### (1) エントリの登録

IGMPv1/IGMPv2 Report メッセージおよび IGMPv3 Report (加入要求) メッセージを受信すると、メッセージに含まれるマルチキャストグループアドレスからマルチキャスト MAC アドレスを学習し、IGMPv1/IGMPv2/IGMPv3 Report メッセージを受信したポートにだけマルチキャストグループ宛でのトラフィックを転送するエントリを作成します。

IPv4 マルチキャストデータの宛先 MAC アドレスは IP アドレスの下位 23 ビットを MAC アドレスにコピーして生成します。そのため、下位 23 ビットが同じ IP アドレスは MAC アドレスが重複します。例えば、224.10.10.10 と 225.10.10.10 はどちらもマルチキャスト MAC アドレスは 0100.5E0A.0A0A となります。これらのアドレスについては、レイヤ 2 中継で同一 MAC アドレス宛でのパケットとして取り扱います。IPv4 マルチキャストアドレスと MAC アドレスの対応を次の図に示します。

図 26-3 IPv4 マルチキャストアドレスと MAC アドレスの対応



#### (2) エントリの削除

学習したマルチキャスト MAC アドレスは次のどれかの場合に、すべてのポートにグループメンバーが存在しなくなった時点で削除されます。

- IGMPv2 Leave メッセージを受信した場合

IGMPv2 Leave メッセージを受信したポートに対して、本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します (Group-Specific Query メッセージの送信は、クエリア設定時だけです。未設定時は代表クエリアから送信されます)。応答がない場合にエントリからこのポートだけを削除します (このポートへのマルチキャストトラフィックの中継を抑制します)。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。

IGMP 即時離脱機能を使用している場合は、IGMPv2 Leave メッセージを受信すると、エントリから該当ポートをすぐに削除します。クエリアを設定していても、Group-Specific Query メッセージは送信しません。

- IGMPv3 Report (離脱要求) メッセージを受信した場合

IGMPv3 Report (離脱要求) メッセージを受信したポートに対して、本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します (Group-Specific Query メッセージの送信は、クエリア設定時だけです。未設定時は代表クエリアから送信されます)。応答がない場合にエントリからこのポートだけを削除します (このポートへのマルチキャストトラフィックの中継を抑制します)。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。ただし、マルチキャストアドレスレコードタイプが BLOCK\_OLD\_SOURCES の IGMPv3 Report を受信した場合は、次の条件をすべて満たした場合だけ、Group-Specific Query メッセージの送信およびエントリの削除処理を実行します。

- 自装置にクエリア設定をしている
- 該当する VLAN に IPv4 マルチキャストを使用していない

IGMP 即時離脱機能を使用している場合は、マルチキャストアドレスレコードタイプが CHANGE\_TO\_INCLUDE\_MODE の IGMPv3 Report (離脱要求) メッセージを受信すると、エントリから該当ポートをすぐに削除します。クエリアを設定していても、Group-Specific Query メッセージは送信しません。

- IGMPv1/IGMPv2/IGMPv3 Report (加入要求) メッセージを受信してから一定時間経過した場合  
マルチキャストルータは直接接続するインタフェース上にグループメンバーが存在するかを確認するため、定期的に Query メッセージを送信します。本装置はルータからの IGMP Query メッセージを受信した場合、VLAN 内の全ポートに中継します。IGMP Query メッセージに対する応答がない場合、エントリからこのポートだけを削除します。すべてのポートから応答がない場合は、エントリ自体を削除します。

本装置では、エントリを削除するタイムアウト時間を 260 秒 (デフォルト値) としています。260 秒間 IGMPv1/IGMPv2/IGMPv3 Report (加入要求) メッセージを受信しない場合、対応するエントリを削除します。

IGMPv3 で運用している VLAN で他装置が代表クエリアの場合、タイムアウト時間は代表クエリアからの IGMPv3 Query メッセージ (QQIC フィールド) から算出します。自装置が代表クエリアの場合または IGMPv2 で運用している場合は、デフォルト値となります。この場合、該当する VLAN では Query Interval を 125 秒で運用してください。

注 タイムアウト時間は、Query Interval (QQIC フィールドの値) × 2 + Query Response Interval で算出します。

## 26.3.2 IPv4 マルチキャストパケットのレイヤ 2 中継

IPv4 マルチキャストパケットの受信 VLAN 内のレイヤ 2 中継は MAC アドレスベースで処理します。IGMP snooping の結果によってレイヤ 2 中継は、同一 MAC アドレスにマッピングされる IP マルチキャストアドレスの IGMP Report (加入要求) メッセージを受信したポートすべてに中継します。

「26.3.1 MAC アドレスの学習 (1) エントリの登録」の例で述べた 224.10.10.10 と 225.10.10.10 のマルチキャスト MAC アドレスはどちらも 0100.5E0A.0A0A となるので、224.10.10.10 宛のマルチキャストデータをレイヤ 2 中継する際に、225.10.10.10 への IGMP Report (加入要求) メッセージを受信したポートへも中継します。

## 26.3.3 マルチキャストルータとの接続

マルチキャストパケットの中継先にはグループ加入済みホストだけでなく隣接するマルチキャストルータも対象とします。本装置とマルチキャストルータを接続して IGMP snooping を使用する場合は、マルチキャストルータへマルチキャストパケットを中継するためにマルチキャストルータと接続するポート (以降、マルチキャストルータポートとします) をコンフィグレーションで指定します。

本装置は指定したマルチキャストルータポートへは全マルチキャストパケットを中継します。

また、IGMP はルータホスト間で送受信するプロトコルであるため、IGMP メッセージはルータおよびホストが受け取ります。本装置は IGMP メッセージを次の表に示すように中継します。

表 26-3 IGMPv1/IGMPv2 メッセージごとの動作

| IGMPv1/IGMPv2 メッセージの種類      | VLAN 内転送ポート                                                                             | 備考 |
|-----------------------------|-----------------------------------------------------------------------------------------|----|
| Membership Query            | 全ポートへ中継します。                                                                             |    |
| Version 2 Membership Report | マルチキャストルータポートにだけ中継します。                                                                  |    |
| Leave Group                 | ほかのポートにまだグループメンバーが存在する場合はどのポートにも中継しません。<br>ほかのポートにグループメンバーが存在しない場合はマルチキャストルータポートに中継します。 |    |
| Version 1 Membership Report | マルチキャストルータポートにだけ中継します。                                                                  |    |

注

自装置にクエリアを設定している場合の中継動作です。クエリアを設定していない場合は、常にマルチキャストルータポートに中継します。ただし、IGMPv1/IGMPv2/IGMPv3 Report (加入要求) メッセージを受信していないポートで IGMPv2 Leave メッセージを受信した場合、クエリアの設定にかかわらず IGMPv2 Leave メッセージは中継しません。

表 26-4 IGMPv3 メッセージごとの動作

| IGMPv3 メッセージの種類             | VLAN 内転送ポート  | 備考                                                                                  |
|-----------------------------|--------------|-------------------------------------------------------------------------------------|
| Version3 Membership Query   | 全ポートへ中継します。  |                                                                                     |
| Version 3 Membership Report | 加入要求の Report | マルチキャストルータポートにだけ中継します。                                                              |
|                             | 離脱要求の Report | ほかのポートにまだグループメンバーが存在する場合はどのポートにも中継しません。ほかのポートにグループメンバーが存在しない場合はマルチキャストルータポートに中継します。 |

注

自装置にクエリアを設定している場合の中継動作です。クエリアを設定していない場合は、常にマルチキャストルータポートに中継します。ただし、IGMPv1/IGMPv2/IGMPv3 Report (加入要求) メッセージを受信していないポートで離脱要求の IGMPv3 Report メッセージを受信した場合、クエリアの設定にかかわらず IGMPv3 Report (離脱要求) メッセージは中継しません。

### 26.3.4 IGMP クエリア機能

IGMP クエリア機能は、VLAN 内にマルチキャストルータが存在せず、マルチキャストパケットの送信ホストと受信ホストだけが存在する環境で、本装置が IGMP Query メッセージを代理で受信ホストに対して送信する機能です。マルチキャストルータは定期的に IGMP Query メッセージを送信し、ホストからの応答を受け取ることでグループメンバーの存在有無を確認します。マルチキャストルータが存在しない場合、受信ホストからの応答がなくなるためにグループメンバーを監視することができなくなります。この機能によって、VLAN 内にマルチキャストルータが存在しない場合でも、IGMP snooping 機能を使用可能とします。本装置では IGMP Query メッセージを 125 秒間隔で送信します。

IGMP クエリア機能を利用するためには、IGMP snooping 機能を利用する VLAN に IP アドレスを設定する必要があります。

VLAN 内に IGMP Query メッセージを送信する装置が存在する場合、IGMP Query メッセージの送信元 IP アドレスの小さい方が代表クエリアとなって IGMP Query メッセージを送信します。VLAN 内のほかの装置が代表クエリアの場合、本装置は IGMP クエリア機能による Query メッセージの送信を停止します。

代表クエリアが障害などで停止すると新たに代表クエリアを選定します。VLAN 内の他装置が障害などで本装置が代表クエリアに決定すると Query メッセージの送信を開始します。本装置では代表クエリアの監視時間を 255 秒としています。

本装置で送信する IGMP Query のバージョンは、IGMPv2 をデフォルト値としています。装置起動以降、IGMP Query のバージョンは、代表クエリアの IGMP バージョンに従います。

### 26.3.5 IGMP 即時離脱機能

IGMP 即時離脱機能は、IGMPv2 Leave および IGMPv3 Report (離脱要求) メッセージを受信した場合に、該当ポートへのマルチキャスト通信をすぐに停止する機能です。

IGMPv3 Report (離脱要求) メッセージでは、マルチキャストアドレスレコードタイプが CHANGE\_TO\_INCLUDE\_MODE の IGMPv3 Report (離脱要求) メッセージだけを、本機能のサポート対象とします。

### 26.3.6 同一 VLAN 上での IPv4 マルチキャストが動作する場合

本装置では、IPv4 マルチキャストと IGMP snooping の両方を同一の VLAN 上で同時に動作させることができます。この場合の動作を次に示します。

- IPv4 マルチキャストによる VLAN 間のレイヤ 3 中継時に、中継先の VLAN で IGMP snooping が動作している場合、レイヤ 3 中継されたマルチキャストトラフィックは、中継先の VLAN 内で IGMP snooping の学習結果に従って中継されます。
- IPv4 マルチキャストが動作することで本装置が VLAN 内の代表クエリアである場合、IGMP Leave メッセージまたは IGMPv3 Report (離脱要求) メッセージ受信による、Group-Specific Query または Group-and-Source-Specific Query の送信は、受信ポートだけでなく VLAN 内の全ポートに送信します。

## 26.4 MLD snooping

ここでは、MLD snooping の機能と動作について説明します。本装置が送受信する MLD フレームのフォーマットおよび既定値は RFC2710 に従います。また、MLD バージョン 2（以降、MLDv2）メッセージのフォーマットおよび設定値は RFC3810 に従います。

### 26.4.1 MAC アドレスの学習

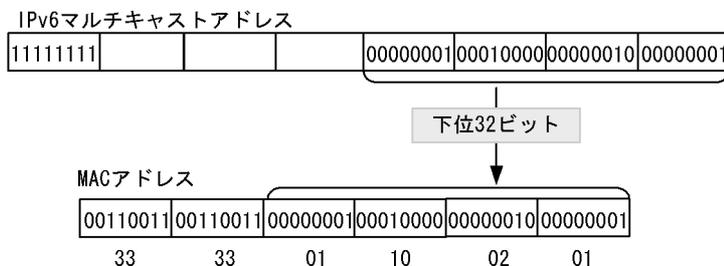
MLD snooping が設定された VLAN で MLD メッセージを受信することによってマルチキャスト MAC アドレスを動的に学習します。学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。

#### (1) エントリの登録

MLDv1 Report メッセージおよび、MLDv2 Report（加入要求）メッセージを受信すると、メッセージに含まれるマルチキャストグループアドレスからマルチキャスト MAC アドレスを学習し、MLDv1/MLDv2 Report メッセージを受信したポートにだけマルチキャストグループ宛でのトラフィックを転送するエントリを作成します。IPv6 マルチキャストデータの宛先 MAC アドレスは IP アドレスの下位 32 ビットを MAC アドレスにコピーして生成します。

IPv6 マルチキャストアドレスはマルチキャストグループを識別するグループ ID フィールドが 112 ビット長のフォーマットと 32 ビット長のフォーマットの 2 種類が規定されています。グループ ID フィールドが 112 ビット長のアドレスフォーマットを使用する場合は、IPv4 マルチキャストアドレスと同様に MAC アドレスの重複が発生します。IPv6 マルチキャストアドレスと MAC アドレスの対応を次の図に示します。

図 26-4 IPv6 マルチキャストアドレスと MAC アドレスの対応



#### (2) エントリの削除

学習したマルチキャスト MAC アドレスは次のどれかの場合に、すべてのポートにグループメンバーが存在しなくなった時点で削除されます。

- MLDv1 Done メッセージを受信した場合  
MLDv1 Done メッセージを受信したポートに対して、本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は、クエリア設定時だけです。未設定時は代表クエリアから送信されます）。応答がない場合にエントリからこのポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑制します）。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。
- MLDv2 Report（離脱要求）メッセージを受信した場合  
MLDv2 Report（離脱要求）メッセージを受信したポートに対して、本装置から Group-Specific Query

メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は、クエリア設定時だけです。未設定時は代表クエリアから送信されます）。応答がない場合にエントリからこのポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑制します）。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。ただし、マルチキャストアドレスレコードタイプが BLOCK\_OLD\_SOURCES の MLDv2 Report を受信した場合は、次の条件をすべて満たした場合だけ、Group-Specific Query メッセージの送信および、エントリ削除処理を実行します。

- ・ 自装置にクエリア設定を行っている
- ・ 該当する VLAN に IPv6 マルチキャストを使用していない
- MLDv1/MLDv2 Report（加入要求）メッセージを受信してから一定時間経過した場合  
マルチキャストルータは直接接続するインタフェース上にグループメンバーが存在するかを確認するために、定期的に MLD Query メッセージを送信します。本装置はルータからの MLD Query メッセージを受信した場合、VLAN 内の全ポートに中継します。MLD Query メッセージに対する応答がない場合、エントリからこのポートだけを削除します。すべてのポートから応答がない場合は、エントリ自体を削除します。  
本装置ではエントリを削除するタイムアウト時間を 260 秒（デフォルト値）としています。260 秒間 MLDv1/MLDv2 Report（加入要求）メッセージを受信しない場合に対応するエントリを削除します。タイムアウト時間は次に示す場合に、動的に設定します。
- 他装置が代表クエリア（MLDv2 での運用）  
代表クエリアからの MLDv2 Query メッセージ（QQIC フィールド）から算出します。
- 自装置が代表クエリアで IPv6 マルチキャストを使用  
MLDv1/MLDv2 にかかわらず、自装置に設定した Query Interval で算出します（ただし、Query Interval を設定していなければ、デフォルト値での運用となります。）
- 他装置が代表クエリア（MLDv1 での運用）で IPv6 マルチキャストを使用  
該当する VLAN に IPv6 マルチキャストを使用していれば、自装置に設定した Query Interval で算出します（ただし、Query Interval を設定していなければデフォルト値での運用となります。）

また、次の場合、タイムアウト時間はデフォルト値での運用となります。

- 自装置が代表クエリアで IPv6 マルチキャストは未使用  
MLDv1/MLDv2 にかかわらず、デフォルト値での運用となります。
- 他装置が代表クエリア（MLDv1 での運用）で IPv6 マルチキャストは未使用  
該当する VLAN に IPv6 マルチキャストを使用していなければ、デフォルト値での運用となります。  
この場合、該当する VLAN では Query Interval を 125 秒で運用してください。

注 タイムアウト時間は、Query Interval（QQIC フィールドの値）× 2+Query Response Interval で算出します。

## 26.4.2 IPv6 マルチキャストパケットのレイヤ 2 中継

IPv6 マルチキャストパケットの受信 VLAN 内のレイヤ 2 中継は IPv4 マルチキャストパケット同様に MAC アドレスベースで処理します。MLD snooping の結果によるレイヤ 2 中継は、同一 MAC アドレスにマッピングされる IPv6 マルチキャストアドレスの MLD Report（加入要求）メッセージを受信したポートすべてに中継します。

## 26.4.3 マルチキャストルータとの接続

マルチキャストパケットの中継先にはグループ加入済みホストだけでなく隣接するマルチキャストルータも対象とします。本装置とマルチキャストルータを接続して MLD snooping を使用する場合、マルチキャ

ストルータへマルチキャストパケットを中継するためにマルチキャストルータと接続するポート（以降、マルチキャストルータポートとします）をコンフィギュレーションで指定します。

本装置は指定したマルチキャストルータポートへは全マルチキャストパケットを中継します。

また、MLD はルータホスト間で送受信するプロトコルであるため、MLD メッセージはルータおよびホストが受け取ります。本装置では MLD メッセージを次の表に示すように中継します。

表 26-5 MLDv1 メッセージごとの動作

| MLDv1 メッセージの種類            | VLAN 内転送ポート                                                                             | 備考 |
|---------------------------|-----------------------------------------------------------------------------------------|----|
| Multicast Listener Query  | 全ポートへ中継します。                                                                             |    |
| Multicast Listener Report | マルチキャストルータポートにだけ中継します。                                                                  |    |
| Multicast Listener Done   | ほかのポートにまだグループメンバーが存在する場合はどのポートにも中継しません。<br>ほかのポートにグループメンバーが存在しない場合はマルチキャストルータポートに中継します。 |    |

注

自装置にクエリアを設定している場合の中継動作です。クエリアを設定していない場合は、常にマルチキャストルータポートに中継します。ただし、MLDv1/MLDv2 Report（加入要求）メッセージを受信していないポートで MLDv1 Done メッセージを受信した場合、クエリアの設定にかかわらず MLDv1 Done メッセージは中継しません。

表 26-6 MLDv2 メッセージごとの動作

| MLDv2 メッセージの種類                     | VLAN 内転送ポート  | 備考                                                                                  |
|------------------------------------|--------------|-------------------------------------------------------------------------------------|
| Version2 Multicast Listener Query  | 全ポートへ中継します。  |                                                                                     |
| Version2 Multicast Listener Report | 加入要求の Report | マルチキャストルータポートにだけ中継します。                                                              |
|                                    | 離脱要求の Report | ほかのポートにまだグループメンバーが存在する場合はどのポートにも中継しません。ほかのポートにグループメンバーが存在しない場合はマルチキャストルータポートに中継します。 |

注

自装置にクエリアを設定している場合の中継動作です。クエリアを設定していない場合は、常にマルチキャストルータポートに中継します。ただし、MLDv1/MLDv2 Report（加入要求）メッセージを受信していないポートで離脱要求の MLDv2 Report メッセージを受信した場合、クエリアの設定にかかわらず MLDv2 Report（離脱要求）メッセージは中継しません。

## 26.4.4 MLD クエリア機能

MLD クエリア機能とは、VLAN 内にマルチキャストルータが存在せず、マルチキャストパケットの送信ホストと受信ホストだけが存在する環境で、本装置が MLD Query メッセージを代理で受信ホストに対して送信する機能です。マルチキャストルータは定期的に MLD Query メッセージを送信し、ホストからの応答を受け取ることでグループメンバーの存在有無を確認します。マルチキャストルータが存在しない場合、受信ホストからの応答がなくなるためにグループメンバーを監視することができなくなります。この機能によって、VLAN 内にマルチキャストルータが存在しない場合でも、MLD snooping 機能を使用可能とします。本装置では Query メッセージを 125 秒間隔で送信します。

MLD クエリア機能を利用するためには、MLD snooping 機能を利用する VLAN に IP アドレスを設定する必要があります。

VLAN 内に MLD Query メッセージを送信する装置が存在する場合、MLD Query メッセージの送信元 IP アドレスの小さい方が代表クエリアとなって MLD Query メッセージを送信します。VLAN 内のほかの装置が代表クエリアの場合、本装置は MLD クエリア機能による MLD Query メッセージの送信を停止します。

代表クエリアが障害などで停止すると新たに代表クエリアを選定します。VLAN 内の他装置が障害などで本装置が代表クエリアに決定すると MLD Query メッセージの送信を開始します。本装置では代表クエリアの監視時間を 255 秒としています。

本装置で送信する MLD Query のバージョンは、MLDv1 をデフォルト値としています。装置起動以降、MLD Query のバージョンは、代表クエリアの MLD バージョンに従います。

### 26.4.5 同一 VLAN 上での IPv6 マルチキャストが動作する場合

本装置では、IPv6 マルチキャストと MLD snooping の両方を同一の VLAN 上で同時に動作させることができます。この場合の動作を次に示します。

- IPv6 マルチキャストによる VLAN 間のレイヤ 3 中継時に、中継先の VLAN で MLD snooping が動作している場合、レイヤ 3 中継されたマルチキャストトラフィックは、中継先の VLAN 内で MLD snooping の学習結果に従って中継されます。
- IPv6 マルチキャストが動作することで本装置が VLAN 内の代表クエリアである場合、MLD Done メッセージまたは MLDv2 Report (離脱要求) メッセージ受信による、Group-Specific Query または Group-and-Source-Specific Query の送信は、受信ポートだけでなく VLAN 内の全ポートに送信します。

## 26.5 IGMP snooping/MLD snooping 使用時の注意事項

### (1) 他機能との共存

「17.3 レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

### (2) 制御パケットのフラッディング

IGMP snooping/MLD snooping が抑止対象とするマルチキャストトラフィックはデータトラフィックであり、ルーティングプロトコルなどの制御パケットは VLAN 内の全ルータや全ホストが受信できるように VLAN 内に flooding する必要があります。そのため、本装置では、次の表に示すアドレス範囲に含まれる宛先 IP アドレスを持つパケットは、VLAN 内の全ポートに中継します。次の表に示すアドレス範囲外の宛先 IP アドレスを持つパケットは、マルチキャスト MAC アドレスの学習結果に従って中継します。

表 26-7 制御パケットのフラッディング

| プロトコル         | アドレス範囲       |
|---------------|--------------|
| IGMP snooping | 224.0.0.0/24 |
| MLD snooping  | ff02::/16    |

ただし、制御パケットのマルチキャスト MAC アドレスと重複するマルチキャストグループアドレスの一部は使用できません。上の表に示したアドレス範囲以外のアドレスで、使用できないマルチキャストグループアドレスを次の表に示します。

表 26-8 使用できないマルチキャストグループアドレス

| プロトコル         | マルチキャストグループアドレス |
|---------------|-----------------|
| IGMP snooping | 224.128.0.0/24  |

トランクポートを設定している場合は、Untagged 制御パケットを受信しないように注意してください。構成上、トランクポートで Untagged 制御パケットを扱う場合は、ネイティブ VLAN を設定してください。

### (3) マルチキャストルータポートの設定

#### (a) 冗長構成時

スパンニングツリーによって冗長構成を採り、スパンニングツリーによってトポロジー変更でルータとの接続が変わる可能性がある場合は、ルータと接続する可能性のある全ポートに対してマルチキャストルータポートの設定をしておく必要があります。

#### (b) レイヤ 2 スイッチ間の接続時

複数のレイヤ 2 スイッチだけで構成される VLAN で、マルチキャストトラフィックの送信ホストを収容するレイヤ 2 スイッチと接続するポートをマルチキャストルータポートに設定しておく必要があります。

冗長構成を採る場合は、送信ホストを収容するレイヤ 2 スイッチと接続する可能性のある全ポートに対してマルチキャストルータポートの設定をしておく必要があります。

### (4) IGMP バージョン 3 ホストとの接続

本装置に IGMPv3 ホストを接続する場合、次のどちらかの対応が必要です。

- 該当する VLAN に IPv4 マルチキャストを使用して、IGMP バージョンを 3 に設定してください。
- IGMPv3 ルータを接続して該当するルータが代表クエリアになるように IP アドレスを設定してください。

また、IGMPv3 ホストからの IGMPv3 メッセージがフラグメント化されない構成で運用してください。

#### (5) MLD バージョン 2 ホストとの接続

本装置に MLDv2 ホストを接続する場合、次のどちらかの対応が必要です。

- 該当する VLAN に IPv6 マルチキャストを使用して、MLD バージョンを 2 に設定してください。
- MLDv2 ルータを接続して該当するルータが代表クエリアになるように IP アドレスを設定してください。

また、MLDv2 ホストからの MLDv2 メッセージがフラグメント化されない構成で運用してください。

#### (6) 運用コマンド実行による MAC アドレスの再学習

IGMP snooping/MLD snooping の運用コマンドのほかに、下記のコマンドを実行した場合、それまでに学習したマルチキャスト MAC アドレスをクリアし、再学習を行います。運用コマンド実行後は、一時的にマルチキャスト通信が中断します。

- copy コマンドで running-config に上書きした場合
- restart vlan コマンド

#### (7) CPU 過負荷時

IGMP snooping/MLD snooping 使用時に CPU が過負荷な状態になった場合、本装置が受信する IGMP/MLD 制御パケットの破棄が発生して、クエリアタイムアウトのメッセージ出力、一時的なマルチキャスト通信断、およびマルチキャストルータポートへの IGMP/MLD 制御パケットの一時的な中継断となることがあります。

#### (8) IPv4 マルチキャストとの同時使用

##### (a) IGMP snooping 設定追加時の一時的通信停止

IPv4 マルチキャストを使用している VLAN に IGMP snooping を追加設定した場合、一時的にマルチキャスト通信が停止します。IGMP snooping 設定後、IGMP Report (加入要求) を受信することでマルチキャスト通信が再開します。

##### (b) 静的グループ参加機能との併用

IPv4 マルチキャストの静的グループ参加機能を使用している VLAN では、ホストから IGMP Report (加入要求) が送信されないおそれがあります。IGMP snooping と同時使用する場合、IGMP Report (加入要求) が送信されないためマルチキャスト通信ができないため、静的グループ参加機能を使用している VLAN でマルチキャスト通信が必要なポートにはマルチキャストルータポートを設定してください。

#### (9) IPv6 マルチキャストとの同時使用

##### (a) MLD snooping 設定追加時の一時的通信停止

IPv6 マルチキャストを使用している VLAN に MLD snooping を追加設定した場合、一時的にマルチキャスト通信が停止します。MLD snooping 設定後、MLD Report (加入要求) を受信することでマルチキャスト通信が再開します。

(b) 静的グループ参加機能との併用

IPv6 マルチキャストの静的グループ参加機能を使用している VLAN では、ホストから MLD Report (加入要求) が送信されないおそれがあります。MLD snooping と同時を使用する場合、MLD Report (加入要求) が送信されないため、静的グループ参加機能を使用している VLAN でマルチキャスト通信が必要なポートにはマルチキャストルータポートを設定してください。

(10) IGMP 即時離脱機能

IGMP 即時離脱機能を使用した場合、IGMPv2 Leave および IGMPv3 Report (離脱要求) メッセージを受信すると、該当ポートへのマルチキャスト通信をすぐに停止します。このため、本機能を使用する場合は、接続ポートに各マルチキャストグループの受信者の端末を 1 台だけ設置することを推奨します。

接続ポートに同一マルチキャストグループの受信者の端末を複数台設置した場合は、一時的にほかの受信者へのマルチキャスト通信が停止します。この場合、受信者からの IGMP Report (加入要求) メッセージを再度受信することで、マルチキャスト通信は再開します。



# 27 IGMP snooping/MLD snooping の設定と運用

IGMP snooping/MLD snooping はレイヤ 2 スイッチで VLAN 内のマルチキャストトラフィックを制御する機能です。この章では、IGMP snooping/MLD snooping の設定と運用方法について説明します。

---

27.1 IGMP snooping のコンフィグレーション

---

27.2 IGMP snooping のオペレーション

---

27.3 MLD snooping のコンフィグレーション

---

27.4 MLD snooping のオペレーション

---

## 27.1 IGMP snooping のコンフィグレーション

### 27.1.1 コンフィグレーションコマンド一覧

IGMP snooping のコンフィグレーションコマンド一覧を次の表に示します。

表 27-1 コンフィグレーションコマンド一覧

| コマンド名                              | 説明                                                 |
|------------------------------------|----------------------------------------------------|
| ip igmp snooping ( global )        | no ip igmp snooping で、本装置の IGMP snooping 機能を抑止します。 |
| ip igmp snooping ( interface )     | 指定したインタフェースの IGMP snooping 機能を設定します。               |
| ip igmp snooping fast-leave        | IGMP 即時離脱機能を設定します。                                 |
| ip igmp snooping mrouter interface | IGMP マルチキャストルータポートを設定します。                          |
| ip igmp snooping querier           | IGMP クエリア機能を設定します。                                 |

### 27.1.2 IGMP snooping の設定

#### [ 設定のポイント ]

IGMP snooping を動作させるには、使用する VLAN の VLAN インタフェースコンフィグレーションモードで、次の設定を行います。例として、VLAN2 に IGMP snooping 機能を有効にする場合を示します。

#### [ コマンドによる設定 ]

1. (config)# interface vlan 2  
(config-if)# ip igmp snooping  
VLAN2 の VLAN インタフェースコンフィグレーションモードに移行して、IGMP snooping 機能を有効にします。

### 27.1.3 IGMP クエリア機能の設定

#### [ 設定のポイント ]

IGMP snooping を設定した VLAN 内にマルチキャストルータが存在しない場合、IGMP クエリア機能を動作させる必要があります。該当 VLAN の VLAN インタフェースコンフィグレーションモードで次の設定を行います。

#### [ コマンドによる設定 ]

1. (config-if)# ip igmp snooping querier  
IGMP クエリア機能を有効にします。

#### [ 注意事項 ]

本設定は該当インタフェースに IPv4 アドレスの設定がないと有効になりません。

### 27.1.4 マルチキャストルータポートの設定

#### [ 設定のポイント ]

IGMP snooping を設定した VLAN 内にマルチキャストルータを接続している場合、該当 VLAN の VLAN インタフェースコンフィギュレーションモードで、次の設定を行います。例として、該当 VLAN 内のポート 1/1 のギガビット・イーサネットインタフェースにマルチキャストルータを接続している場合を示します。

[ コマンドによる設定 ]

1. (config-if)# ip igmp snooping mrouter interface gigabitethernet 1/1  
該当インタフェースで、マルチキャストルータポートを指定します。

## 27.2 IGMP snooping のオペレーション

### 27.2.1 運用コマンド一覧

IGMP snooping の運用コマンド一覧を次の表に示します。

表 27-2 運用コマンド一覧

| コマンド名                   | 説明                                |
|-------------------------|-----------------------------------|
| show igmp-snooping      | IGMP snooping 情報を表示します。           |
| clear igmp-snooping     | IGMP snooping 情報をクリアします。          |
| restart snooping        | snooping プログラムを再起動します。            |
| dump protocols snooping | イベントトレース情報および制御テーブル情報のファイルを出力します。 |

### 27.2.2 IGMP snooping の確認

IGMP snooping 機能を使用した場合の IGMP snooping に関する確認内容には次のものがあります。

#### (1) コンフィグレーション設定後の確認

show igmp-snooping コマンドを実行し、IGMP snooping に関する設定が正しいことを確認してください。

図 27-1 IGMP snooping の設定状態表示

```
> show igmp-snooping 100
Date 2008/10/01 15:20:00 UTC
VLAN: 100
 IP address: 192.168.11.20 Querier: enable
 IGMP querying system: 192.168.11.20
 Querier version: V2
 IPv4 Multicast routing: Off
 Fast-leave: On
 Port(5): 1/1-5
 Mrouter-port: 1/1,3
 Group Counts: 3
```

#### (2) 運用中の確認

次のコマンドで、IGMP snooping の運用中の状態を確認してください。

学習した MAC アドレス、VLAN 内に中継される IPv4 マルチキャストアドレスとその中継先ポートリストの状態は、show igmp-snooping group コマンドで確認してください。

図 27-2 show igmp-snooping group コマンドの実行結果

```
> show igmp-snooping group 100
Date 2007/02/01 15:20:00 UTC
VLAN counts: 1
VLAN: 100 Group counts: 3 IPv4 Multicast routing: Off
 Group Address MAC Address Version Mode
 224.10.10.10 0100.5e0a.0a0a V2 -
 Port-list:1/1-3
 225.10.10.10 0100.5e0a.0a0a V3 INCLUDE
 Port-list:1/1-2
 239.192.1.1 0100.5e40.0101 V2,V3 EXCLUDE
 Port-list:1/1
```

ポートごとの参加グループ表示例を show igmp-snooping port コマンドで確認してください。

図 27-3 show igmp-snooping port コマンドの実行結果

```
> show igmp-snooping port 1/1
Date 2006/10/01 15:20:00 UTC
Port 1/1 VLAN counts: 2
 VLAN: 100 Group counts: 2
 Group Address Last Reporter Uptime Expires
 224.10.10.10 192.168.1.3 00:10 04:10
 239.192.1.1 192.168.1.3 02:10 03:00
 VLAN: 150 Group counts: 1
 Group Address Last Reporter Uptime Expires
 239.10.120.1 192.168.15.10 01:10 02:30
```

## 27.3 MLD snooping のコンフィグレーション

### 27.3.1 コンフィグレーションコマンド一覧

MLD snooping のコンフィグレーションコマンド一覧を次の表に示します。

表 27-3 コンフィグレーションコマンド一覧

| コマンド名                               | 説明                            |
|-------------------------------------|-------------------------------|
| ipv6 mld snooping                   | MLD snooping 機能を使用することを設定します。 |
| ipv6 mld snooping mrouter interface | MLD マルチキャストルータポートを設定します。      |
| ipv6 mld snooping querier           | MLD クエリア機能を設定します。             |
| no ipv6 mld snooping                | MLD snooping 機能の抑止を設定します。     |

### 27.3.2 MLD snooping の設定

#### [ 設定のポイント ]

MLD snooping を動作させるには、使用する VLAN の VLAN インタフェースのインタフェースコンフィグレーションモードで、次の設定を行います。例として、VLAN2 に MLD snooping 機能を有効にする場合を示します。

#### [ コマンドによる設定 ]

1. `(config)# interface vlan 2`  
`(config-if)# ipv6 mld snooping`  
VLAN2 の VLAN インタフェースコンフィグレーションモードに移行して、MLD snooping 機能を有効にします。

### 27.3.3 MLD クエリア機能の設定

#### [ 設定のポイント ]

MLD snooping を設定した VLAN 内にマルチキャストルータが存在しない場合、MLD クエリア機能を動作させる必要があります。該当 VLAN の VLAN インタフェースコンフィグレーションモードで、次の設定を行います。

#### [ コマンドによる設定 ]

1. `(config-if)# ipv6 mld snooping querier`  
MLD クエリア機能を有効にします。

#### [ 注意事項 ]

本設定は該当インタフェースに IPv6 アドレスの設定がないと有効となりません。

### 27.3.4 マルチキャストルータポートの設定

#### [ 設定のポイント ]

MLD snooping を設定した VLAN 内にマルチキャストルータを接続している場合、該当 VLAN の

VLAN インタフェースコンフィグレーションモードで、次の設定を行います。例として、該当 VLAN 内のポート 1/1 のギガビット・イーサネットインタフェースにマルチキャストルータを接続している場合を示します。

[ コマンドによる設定 ]

1. (config-if)# `ipv6 mld snooping mrouter interface gigabitethernet 1/1`  
該当インタフェースでマルチキャストルータポートを指定します。

## 27.4 MLD snooping のオペレーション

### 27.4.1 運用コマンド一覧

MLD snooping の運用コマンド一覧を次の表に示します。

表 27-4 運用コマンド一覧

| コマンド名                   | 説明                                |
|-------------------------|-----------------------------------|
| show mld-snooping       | MLD snooping 情報を表示します。            |
| clear mld-snooping      | MLD snooping 情報をクリアします。           |
| restart snooping        | snooping プログラムを再起動します。            |
| dump protocols snooping | イベントトレース情報および制御テーブル情報のファイルを出力します。 |

### 27.4.2 MLD snooping の確認

MLD snooping 機能を使用した場合の MLD snooping に関する確認内容には次のものがあります。

#### (1) コンフィグレーション設定後の確認

show mld-snooping コマンドを実行し、MLD snooping に関する設定が正しいことを確認してください。

図 27-4 MLD snooping の設定状態表示

```
> show mld-snooping 100
Date 2008/02/01 15:20:00 UTC
VLAN: 100
 IP address: fe80::b1 Querier: enable
 MLD querying system: fe80::b1
 Querier version: V1
 IPv6 Multicast routing: Off
 Port(5): 1/1-5
 Mrouter-port: 1/1,3
 Group Counts: 3
```

#### (2) 運用中の確認

以下のコマンドで、MLD snooping の運用中の状態を確認してください。

学習した MAC アドレス、VLAN 内に中継される IPv6 マルチキャストアドレスとその中継先ポートリストの状態は、show mld-snooping group コマンドで確認してください。

図 27-5 show mld-snooping group コマンドの実行結果

```
> show mld-snooping group 100
Date 2007/02/01 15:20:00 UTC
VLAN counts: 1
VLAN: 100 Group counts: 2 IPv6 Multicast routing: Off
 Group Address MAC Address Version Mode
 ff35::1 3333.0000.0001 V1,V2 EXCLUDE
 Port-list:1/1-3
 ff35::2 3333.0000.0002 V2 EXCLUDE
 Port-list:1/1-2
```

ポートごとの参加グループ表示例を show mld-snooping port コマンドで確認してください。

図 27-6 show mld-snooping port コマンドの実行結果

```
> show mld-snooping port 1/1
Date 2006/10/01 15:20:00 UTC
Port 1/1 VLAN counts: 1
 VLAN: 100 Group counts: 2
 Group Address Last Reporter Uptime Expires
 ff35::1 fe80::b2 00:10 04:10
 ff35::2 fe80::b3 02:10 03:00
```



# 付録

---

付録 A 準拠規格

---

付録 B 謝辞 (Acknowledgments)

---

## 付録 A 準拠規格

### 付録 A.1 TELNET/FTP

表 A-1 TELNET/FTP の準拠する規格および勧告

| 規格番号 (発行年月)      | 規格名                           |
|------------------|-------------------------------|
| RFC854(1983年5月)  | TELNET PROTOCOL SPECIFICATION |
| RFC855(1983年5月)  | TELNET OPTION SPECIFICATIONS  |
| RFC959(1985年10月) | FILE TRANSFER PROTOCOL (FTP)  |

### 付録 A.2 RADIUS/TACACS+

表 A-2 RADIUS/TACACS+ の準拠する規格および勧告

| 規格番号 (発行年月)                        | 規格名                                                |
|------------------------------------|----------------------------------------------------|
| RFC2865(2000年6月)                   | Remote Authentication Dial In User Service(RADIUS) |
| RFC2866(2000年6月)                   | RADIUS Accounting                                  |
| RFC3162(2001年8月)                   | RADIUS and IPv6                                    |
| draft-grant-tacacs-02<br>(1997年1月) | The TACACS+ Protocol Version 1.78                  |

### 付録 A.3 NTP

表 A-3 NTP の準拠する規格および勧告

| 規格番号 (発行年月)      | 規格名                                                                          |
|------------------|------------------------------------------------------------------------------|
| RFC1305(1992年3月) | Network Time Protocol (Version 3) Specification, Implementation and Analysis |

### 付録 A.4 DNS

表 A-4 DNS リゾルバの準拠する規格および勧告

| 規格番号 (発行年月)      | 規格名                                             |
|------------------|-------------------------------------------------|
| RFC1034(1987年3月) | Domain names - concepts and facilities          |
| RFC1035(1987年3月) | Domain names - implementation and specification |

## 付録 A.5 イーサネット

表 A-5 イーサネットインタフェースの準拠規格

| 種別                                                                      | 規格                            | 名称                                                                                                                                                                                                            |
|-------------------------------------------------------------------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10BASE-T ,<br>100BASE-TX ,<br>1000BASE-T ,<br>1000BASE-X ,<br>10GBASE-R | IEEEStd 802.3x-1997           | Specification for 802.3x Full Duplex Operation                                                                                                                                                                |
|                                                                         | IEEE802.2 1998<br>Edition     | IEEE Standard for Information Technology -<br>Telecommunications and Information Exchange Between<br>Systems - Local and Metropolitan Area Networks - Specific<br>Requirements - Part 2: Logical Link Control |
|                                                                         | IEEE802.3 2000<br>Edition     | Carrier sense multiple access with collision detection (CSMA/<br>CD) access method and physical layer Specifications                                                                                          |
| 10GBASE-R                                                               | IEEE 802.3ae<br>Standard-2002 | Media Access Control(MAC) Parameters, Physical Layer, and<br>Management Parameters for 10Gb/s Operation                                                                                                       |

## 付録 A.6 リンクアグリゲーション

表 A-6 リンクアグリゲーションの準拠規格

| 規格                                     | 名称                                    |
|----------------------------------------|---------------------------------------|
| IEEE802.3ad<br>(IEEE Std 802.3ad-2000) | Aggregation of Multiple Link Segments |

## 付録 A.7 VLAN

表 A-7 VLAN の準拠規格および勧告

| 規格                                   | 名称                                  |
|--------------------------------------|-------------------------------------|
| IEEE802.1Q<br>(IEEE Std 802.1Q-2003) | Virtual Bridged Local Area Networks |

注 GVRP/GMRP はサポートしていません。

## 付録 A.8 スパニングツリー

表 A-8 スパニングツリーの準拠規格および勧告

| 規格                                                | 名称                                                                               |
|---------------------------------------------------|----------------------------------------------------------------------------------|
| IEEE802.1D<br>(ANSI/IEEE Std 802.1D-1998 Edition) | Media Access Control (MAC) Bridges<br>(The Spanning Tree Algorithm and Protocol) |
| IEEE802.1t<br>(IEEE Std 802.1t-2001)              | Media Access Control (MAC) Bridges -<br>Amendment 1                              |
| IEEE802.1w<br>(IEEE Std 802.1w-2001)              | Media Access Control (MAC) Bridges -<br>Amendment 2: Rapid Reconfiguration       |
| IEEE802.1s<br>(IEEE Std 802.1s-2002)              | Virtual Bridged Local Area Networks -<br>Amendment 3: Multiple Spanning Trees    |

## 付録 A.9 IGMP snooping/MLD snooping

表 A-9 IGMP snooping/MLD snooping の準拠規格および勧告

| 規格番号 (発行年月)      | 規格名                                                                                                                   |
|------------------|-----------------------------------------------------------------------------------------------------------------------|
| RFC4541(2006年5月) | Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches |

---

## 付録 B 謝辞 (Acknowledgments)

[SNMP]

\*\*\*\*\*

Copyright 1988-1996 by Carnegie Mellon University  
All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

\*\*\*\*\*

Some of this software has been modified by BBN Corporation and is a derivative of software developed by Carnegie Mellon University. Use of the software remains subject to the original conditions set forth above.

\*\*\*\*\*

Some of this software is Copyright 1989 by TGV, Incorporated but subject to the original conditions set forth above.

\*\*\*\*\*

Some of this software is Copyright (C) 1983,1988 Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of California at Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided "as is" without express or implied warranty.

\*\*\*\*\*

\* Primary Author:  
Steve Waldbusser

\* Additional Contributors:  
Erik Schoenfelder (schoenfr@ibr.cs.tu-bs.de): additions, fixes and enhancements for Linux by 1994/1995.  
David Waitzman: Reorganization in 1996.

Wes Hardaker <hardaker@ece.ucdavis.edu>: Some bug fixes in his UC Davis CMU SNMP distribution were adopted by David Waitzman

David Thaler <thalerd@eecs.umich.edu>: Some of the code for making the agent embeddable into another application were adopted by David Waitzman

Many more over the years...

[NTP]

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.

Copyright (C) David L. Mills 1992-2003 Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.

[PIM sparse-mode pimd]

```
/*
 * Copyright (c) 1998-2001
 * The University of Southern California/Information Sciences Institute.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 * notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in the
 * documentation and/or other materials provided with the distribution.
 * 3. Neither the name of the project nor the names of its contributors
 * may be used to endorse or promote products derived from this software
 * without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
 * CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
 * GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 */
```

```

/*
 * Part of this program has been derived from mouted.
 * The mouted program is covered by the license in the accompanying file
 * named "LICENSE.mouted".
 *
 * The mouted program is COPYRIGHT 1989 by The Board of Trustees of
 * Leland Stanford Junior University.
 *
 */

```

[pim6dd]

```

/*
 * Copyright (C) 1998 WIDE Project.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 * notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in the
 * documentation and/or other materials provided with the distribution.
 * 3. Neither the name of the project nor the names of its contributors
 * may be used to endorse or promote products derived from this software
 * without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
 * CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
 * GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 */

```

[pim6sd]

```

/*
 * Copyright (C) 1999 LSIT Laboratory.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without

```

```
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. Neither the name of the project nor the names of its contributors
* may be used to endorse or promote products derived from this software
* without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS" AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*/
/*
* Questions concerning this software should be directed to
* Mickael Hoerd (hoerd@clarinet.u-strasbg.fr) LSIIT Strasbourg.
*
*/
/*
* This program has been derived from pim6dd.
* The pim6dd program is covered by the license in the accompanying file
* named "LICENSE.pim6dd".
*/
/*
* This program has been derived from pimd.
* The pimd program is covered by the license in the accompanying file
* named "LICENSE.pimd".
*
*/
```

[RADIUS]

Copyright 1992 Livingston Enterprises , Inc.  
Livingston Enterprises , Inc. 6920 Koll Center Parkway Pleasanton , CA 94566

Permission to use , copy , modify , and distribute this software for any  
purpose and without fee is hereby granted , provided that this copyright

and permission notice appear on all copies and supporting documentation , the name of Livingston Enterprises , Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission , and notice be given in supporting documentation that copying and distribution is by permission of Livingston Enterprises , Inc. Livingston Enterprises , Inc. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

[totd]

WIDE

Copyright (C) 1998 WIDE Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by WIDE Project and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

University of Tromsø

Copyright (C) 1999,2000,2001,2002 University of Tromsø, Norway. All rights reserved.

Author: Feike W. Dillema, The Pasta Lab, Institutt for Informatikk University of Tromsø, Norway

Permission to use, copy, modify and distribute this software and its documentation is hereby granted, provided that both the copyright notice and this permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation.

THE UNIVERSITY OF TROMSØ ALLOWS FREE USE OF THIS SOFTWARE IN ITS "AS IS" CONDITION. THE UNIVERSITY OF TROMSØ DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.

The author requests users of this software to send back any improvements or extensions that they

make and grant him and/or the University the rights to redistribute these changes without restrictions.

Invenia Innovation A.S.

Copyright (C) Invenia Innovation A.S., Norway. All rights reserved.

Author: Feike W. Dillema, Invenia Innovation A.S., Norway.

Permission to use, copy, modify and distribute this software and its documentation is hereby granted, provided that both the copyright notice and this permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation.

INVENIA INNOVATION A.S. ALLOWS FREE USE OF THIS SOFTWARE IN ITS "AS IS" CONDITION. INVENIA INNOVATION A.S. DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.

The author requests users of this software to send back any improvements or extensions that they make and grant him and/or the Invenia Innovation the rights to redistribute these changes without restrictions.

Todd C. Miller

Copyright (C) 1998 Todd C. Miller <Todd.Miller@courtesan.com> All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[libtacplus]

Copyright (C) 1998, 2001, 2002, Juniper Networks, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the

distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[tftp]

Copyright (C) 1983, 1993

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[libfetch]

Copyright (C) 1998 Dag-Erling Coïdan Smøgrav

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and

the following disclaimer in this position and unchanged.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[IPv6 DHCP]

Copyright (C) 1998-2004 WIDE Project.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE

ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT

LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[iides]

Internet Initiative Japan Inc.

Copyright (c) 1996 Internet Initiative Japan Inc.

All rights reserved.

1. Redistributions of source code must retain the above copyright notice, this list of conditions and

the following disclaimer.

2. Redistribution with functional modification must include prominent notice stating how and when and by whom it is modified.

3. Redistributions in binary form have to be along with the source code or documentation which include above copyright notice, this list of conditions and the following disclaimer.

4. All commercial advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by Internet Initiative Japan Inc.

THIS SOFTWARE IS PROVIDED BY ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

[Net-SNMP]

CMU/UCD

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Networks Associates Technology, Inc

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

\* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

\* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

\* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written

permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Cambridge Broadband Ltd.

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

\* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

\* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

\* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Sun Microsystems, Inc.

Copyright (c) 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

\* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

\* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

\* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Sparta, Inc  
Copyright (c) 2003-2004, Sparta, Inc  
All rights reserved.

\* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

\* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

\* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Cisco/BUPTNIC  
Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.  
All rights reserved.

\* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

\* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

\* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

#### Apache License Version 2.0

Apache License  
Version 2.0, January 2004  
<http://www.apache.org/licenses/>

#### TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

##### 1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. **Grant of Copyright License.** Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.
3. **Grant of Patent License.** Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.
4. **Redistribution.** You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

- (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
- (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
- (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
- (d) If the Work includes a "NOTICE" text file as part of its distribution, then any derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. **Submission of Contributions.** Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.
6. **Trademarks.** This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. **Disclaimer of Warranty.** Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. **Limitation of Liability.** In no event and under no legal theory, whether in tort (including negligence),

contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. **Accepting Warranty or Additional Liability.** While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

## END OF TERMS AND CONDITIONS

### APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");  
you may not use this file except in compliance with the License.  
You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.



---

# 索引

## 数字

---

1000BASE-X〔接続インタフェース〕 353  
1000BASE-X 接続時の注意事項 357  
1000BASE-X 接続仕様 353  
10BASE-T/100BASE-TX/1000BASE-T 自動認識 343  
10BASE-T/100BASE-TX/1000BASE-T 接続時の注意事項 348  
10BASE-T/100BASE-TX/1000BASE-T 接続仕様 343  
10GBASE-R〔接続インタフェース〕 359  
10GBASE-R 接続時の注意事項 360  
10GBASE-R 接続仕様 359

## B

---

BSU/NIF の管理 289  
BSU シングルアクト運転 17  
BSU ダブルアクト運転 17  
BSU トリプルアクト運転 17  
BSU を管理する上で必要な運用コマンド一覧 290  
BSU を管理する上で必要なコンフィグレーションコマンド一覧 290

## C

---

CLI 環境情報 169  
CLI 設定のカスタマイズ 169  
CONTROL フィールドの値と送受信サポート内容 334

## I

---

IGMP snooping 609  
IGMP snooping/MLD snooping 概要 607  
IGMP snooping/MLD snooping 使用時の注意事項 617  
IGMP snooping/MLD snooping の解説 605  
IGMP snooping/MLD snooping の概要 606  
IGMP snooping/MLD snooping の設定と運用 621  
IGMP snooping および MLD snooping 概要 607  
IGMP snooping の運用コマンド一覧 624  
IGMP snooping のコンフィグレーションコマンド一覧 622  
IGMPv1/IGMPv2 メッセージごとの動作 611  
IGMPv3 メッセージごとの動作 611  
IGMP クエリア機能〔IGMP snooping〕 611  
IGMP 即時離脱機能〔IGMP snooping〕 612  
IPv4 マルチキャストアドレスと MAC アドレスの対応 609

IPv4 マルチキャストパケットのレイヤ 2 中継〔IGMP snooping〕 610  
IPv6 マルチキャストアドレスと MAC アドレスの対応 613  
IPv6 マルチキャストパケットのレイヤ 2 中継〔MLD snooping〕 614  
IP アドレスの設定〔本装置〕 201

## L

---

L2 プロトコルフレーム透過機能のコンフィグレーションコマンド一覧 443  
LLC の扱い 334  
LLC 副層フレームフォーマット 334

## M

---

MAC VLAN のコンフィグレーションコマンド一覧 422  
MAC アドレス学習 387  
MAC アドレス学習の運用コマンド一覧 394  
MAC アドレス学習のコンフィグレーションコマンド一覧 392  
MAC アドレスの学習〔IGMP snooping〕 609  
MAC アドレスの学習〔MLD snooping〕 613  
MAC 副層フレームフォーマット 333  
MDI/MDI-X のピンマッピング 347  
MLD snooping 613  
MLD snooping の運用コマンド一覧 628  
MLD snooping のコンフィグレーションコマンド一覧 626  
MLDv1 メッセージごとの動作 615  
MLDv2 メッセージごとの動作 615  
MLD クエリア機能〔MLD snooping〕 615

## N

---

NIF を管理する上で必要な運用コマンド一覧 292  
NIF を管理する上で必要なコンフィグレーションコマンド一覧 292

## P

---

PSP シングルアクト運転 19  
PSP ダブルアクト運転 19  
PVST+ の運用コマンド一覧 470  
PVST+ のコンフィグレーションコマンド一覧 465

## R

- RADIUS 217
- RADIUS/TACACS+ に関するコンフィグレーション  
コマンド一覧 241
- RADIUS/TACACS+ の解説 217
- RADIUS/TACACS+ の概要 217
- RADIUS/TACACS+ の適用機能および範囲 217
- RADIUS のサポート範囲 218
- Ring Protocol とスパニングツリー /GSRP の併用  
563
- Ring Protocol の運用コマンド一覧 559
- Ring Protocol の解説 505
- Ring Protocol のコンフィグレーションコマンド一覧  
546
- Ring Protocol の設定と運用 545

## T

- TACACS+ 217
- Tag 変換のコンフィグレーションコマンド一覧 440
- TYPE/LENGTH フィールドの扱い 333

## V

- VLAN 397
- VLAN debounce 機能のコンフィグレーションコマ  
ンド一覧 447
- VLAN 拡張機能 435
- VLAN 拡張機能の運用コマンド一覧 450
- VLAN 基本機能のコンフィグレーションコマンド一  
覧 404
- VLAN トンネリングのコンフィグレーションコマ  
ンド一覧 438
- VLAN の運用コマンド一覧 429
- VLAN マッピング 530

## X

- XID および TEST レスポンス 334

## い

- イーサネット 331
- イーサネット共通のコンフィグレーションコマンド一  
覧 336
- イーサネットで使用する運用コマンド一覧 342

## う

- 運用端末の接続とリモート操作に関する運用コマンド  
一覧 204

- 運用端末の接続とリモート操作に関するコンフィグ  
レーションコマンド一覧 198

## お

- オートネゴシエーション〔1000BASE-X〕354
- オートネゴシエーション〔10BASE-T/100BASE-TX/  
1000BASE-T〕345

## か

- 仮想リンク 565
- 仮想リンクの運用コマンド一覧 586
- 仮想リンクのコンフィグレーションコマンド一覧  
583

## け

- 経路切り戻し動作 593

## こ

- コマンド操作 163
- コマンド入力モードの切り換えおよびユーティリティ  
に関する運用コマンド一覧 164
- コンソールの接続形態 156
- コンフィグレーション 173
- コンフィグレーションコマンド一覧〔VLAN インタ  
フェースへの IP アドレスの設定〕427
- コンフィグレーションの編集および操作に関する運用  
コマンド一覧 178
- コンフィグレーションの編集および操作に関するコン  
フィグレーションコマンド一覧 178

## さ

- サポート機能〔IGMP snooping/MLD snooping〕608

## し

- 時刻設定および NTP に関する運用コマンド一覧 248
- 時刻設定および NTP に関するコンフィグレーション  
コマンド一覧 248
- 時刻の設定と NTP 247
- 自動 MDIX 機能 347
- ジャンボフレーム〔1000BASE-X〕356
- ジャンボフレーム〔10BASE-T/100BASE-TX/  
1000BASE-T〕348
- ジャンボフレーム〔10GBASE-R〕360
- ジャンボフレームサポート機能〔1000BASE-X〕357
- ジャンボフレームサポート機能〔10BASE-T/  
100BASE-TX/1000BASE-T〕348
- ジャンボフレームサポート機能〔10GBASE-R〕360

収容条件 23  
 受信フレームの廃棄条件 335  
 省電力機能 295  
 省電力機能の運用コマンド一覧 320  
 省電力機能のコンフィグレーションコマンド一覧 311  
 シングルスパニングツリーの運用コマンド一覧 478  
 シングルスパニングツリーのコンフィグレーションコマンド一覧 473

## す

スケジュール時間帯 304  
 スパニングツリー 451  
 スパニングツリー共通機能の運用コマンド一覧 501  
 スパニングツリー共通機能のコンフィグレーションコマンド一覧 497  
 スパニングツリー動作モードのコンフィグレーションコマンド一覧 459

## せ

接続インタフェース〔1000BASE-X〕353  
 接続インタフェース〔10BASE-T/100BASE-TX/1000BASE-T〕343  
 接続インタフェース〔10GBASE-R〕359

## そ

装置管理者モード変更のパスワードの設定 210  
 装置構成 7  
 装置の管理 257  
 装置へのログイン 155  
 装置を管理する上で必要な運用コマンド一覧 273  
 装置を管理する上で必要なコンフィグレーションコマンド一覧 273  
 ソフトウェア管理に関する運用コマンド一覧 326  
 ソフトウェアの管理 325

## つ

通常時間帯 304

## て

デフォルト動作 592  
 伝送速度および、全二重および半二重モードごとの接続仕様〔1000BASE-X〕354  
 伝送速度および、全二重および半二重モードごとの接続仕様〔10BASE-T/100BASE-TX/1000BASE-T〕344

## と

同時にログインできるユーザ数の設定 211

## に

認証方式シーケンス〔end-by-reject 設定時〕224  
 認証方式シーケンス〔end-by-reject 未設定時〕223

## は

バックアップ・リストアに使用する運用コマンド一覧 283  
 パッドの扱い 335

## ふ

フレームフォーマット〔MAC/LLC 副層制御〕333  
 フローコントロール〔1000BASE-X〕354  
 フローコントロール〔10BASE-T/100BASE-TX/1000BASE-T〕345  
 フローコントロール〔10GBASE-R〕359  
 フローコントロールの受信動作〔1000BASE-X〕355  
 フローコントロールの受信動作〔10BASE-T/100BASE-TX/1000BASE-T〕345  
 フローコントロールの受信動作〔10GBASE-R〕360  
 フローコントロールの送信動作〔1000BASE-X〕354  
 フローコントロールの送信動作〔10BASE-T/100BASE-TX/1000BASE-T〕345  
 フローコントロールの送信動作〔10GBASE-R〕359  
 プロトコル VLAN のコンフィグレーションコマンド一覧 415

## ほ

ポート VLAN のコンフィグレーションコマンド一覧 410  
 ホスト名・DNS に関するコンフィグレーションコマンド一覧 255  
 ホスト名と DNS 253  
 ポリシーベーススイッチング 589  
 ポリシーベーススイッチンググループ 591  
 ポリシーベーススイッチングの運用コマンド一覧 602  
 ポリシーベーススイッチングのコンフィグレーションコマンド一覧 599  
 ポリシーベーススイッチングリスト情報 591  
 本装置の概要 1

## ま

マネージメントポートで使用する運用コマンド一覧 204

- マネージメントポートのコンフィグレーションコマンド一覧 198
- マルチキャストグループアドレス 606
- マルチキャストルータとの接続〔IGMP snooping〕 610
- マルチキャストルータとの接続〔MLD snooping〕 614
- マルチプルスパニングツリーの運用コマンド一覧 492
- マルチプルスパニングツリーのコンフィグレーションコマンド一覧 486

## り

---

- リモート運用端末 158
- リモート運用端末からのログインを許可する IP アドレスの設定 211
- リモート運用端末から本装置へのログイン 191
- リモート運用端末と本装置との通信の確認 205
- リモート運用端末の接続形態 156
- リンクアグリゲーション 363
- リンクアグリゲーション拡張機能のコンフィグレーションコマンド一覧 377
- リンクアグリゲーション基本機能のコンフィグレーションコマンド一覧 368
- リンクアグリゲーションの運用コマンド一覧 379

## れ

---

- レイヤ 2 スイッチ概説 381
- レイヤ 2 中継遮断機能のコンフィグレーションコマンド一覧 449

## ろ

---

- ログイン制御の概要 209
- ログインセキュリティと RADIUS/TACACS+ 207
- ログインセキュリティに関する運用コマンド一覧 208
- ログインセキュリティに関するコンフィグレーションコマンド一覧 208
- ログインユーザの作成と削除 209