
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.2

Ver. 11.7 対応

AX63S-S002-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 - S002 - 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
1.1.7 フィルタ使用時の注意事項	・ 「(2) IPv4 オプション付きパケットに対するフィルタ」の記述を変更しました。
5.1.4 フロー検出使用時の注意事項	・ 「(2) IPv4 オプション付きパケットに対する QoS フロー検出」の記述を変更しました。
17.1.5 系切替時の通信無停止対応機能一覧	・ ポリシーベーススイッチングおよびポリシーベースルーティングに関する記述を追加しました。 ・ IPv4 マルチキャストルーティングプロトコルに関する記述を変更しました。
28.1.6 インフォーム	・ 本項を追加しました。
28.2.6 SNMPv2C によるインフォーム送信の設定	・ 本項を追加しました。
28.2.14 SNMPv2C による VRF へのインフォーム送信の設定	・ 本項を追加しました。
28.3.2 SNMP マネージャとの通信の確認	・ インフォームの記述を追加しました。
30.1.4 本装置での sFlow 統計の動作について	・ ポリシーベースルーティングの記述を追加しました。

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
仮想ルータの MAC アドレスと IP アドレス	・ MAC アドレスに関する記述を追加しました。
トラッキング機能	・ VRRP ボーリングに関する記述を追加しました。

【Ver. 11.4 対応版】

表 変更履歴

項目	追加・変更内容
フィルタ使用時の注意事項	・ 「(11) DHCP snooping とフィルタの関係」を追加しました。
レイヤ 2 認証	・ Web 認証の従来のダイナミック VLAN モードをレガシーモードに変更しました。 ・ Web 認証および MAC 認証について、ダイナミック VLAN モードサポートに伴い記述を追加しました。
レイヤ 2 認証と他機能との共存	・ 他機能との共存仕様を変更しました。
同一ポート内での共存	・ 共存仕様を変更しました。
認証前端末の通信許可	・ 本項を追加しました。
レイヤ 2 認証共通コンフィグレーション	・ 本節を追加しました。
Web 認証の解説	・ 従来のダイナミック VLAN モードをレガシーモードに変更しました。 ・ ダイナミック VLAN モードサポートに伴い記述を追加しました。
Web 認証の設定と運用	・ 従来のダイナミック VLAN モードをレガシーモードに変更しました。 ・ ダイナミック VLAN モードサポートに伴い記述を追加しました。

項目	追加・変更内容
MAC 認証の解説	• ダイナミック VLAN モードサポートに伴い記述を追加しました。
MAC 認証の設定と運用	• ダイナミック VLAN モードサポートに伴い記述を追加しました。
DHCP snooping	• 本章を追加しました。
NIF の冗長化	• 本章を追加しました。

【Ver. 11.3 対応版】

表 変更履歴

項目	追加・変更内容
アクセスリストロギング	• 本章を追加しました。
本装置での sFlow 統計の動作について	• 「(1) sFlow 統計収集の対象パケットに関する注意点」にアクセスリストロギング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
フローモード	• フロー検出拡張モードに関する記述を追加しました。
フロー検出条件	• Advance 条件に関する記述を追加しました。
アクセスリスト	• Advance 条件に関する記述を追加しました。
フローモードの設定	• 「(2) フロー検出拡張モードの設定」を追加しました。
MAC ヘッダ・IP ヘッダ・TCP/UDP ヘッダで中継・廃棄をする設定	• 本項を追加しました。
フローモード	• フロー検出拡張モードに関する記載を追加しました。
フロー検出条件	• Advance 条件に関する記載を追加しました。
QoS フローリスト	• Advance 条件に関する記載を追加しました。
フローモードの設定	• 「(2) フロー検出拡張モードの設定」を追加しました。
優先度決定使用時の注意事項	• 「(8) フロー検出拡張モードでの DSCP マッピング」を追加しました。
VRRP のサポート規格	• 「(5) 障害検出時間について」を追加しました。
VRRP 使用時の注意事項	• 「(7) VRRP 状態遷移時間について」を追加しました。
ログの VRF への syslog 出力の設定	• 本項を追加しました。

【Ver. 11.1 対応版】

表 変更履歴

項目	追加・変更内容
サポート機能	• 「(5) syslog サーバへの動作ログ記録」を追加しました。
認証処理に関する設定	• 「(8) syslog サーバへの出力設定」を追加しました。
BCU/CSU/MSU の冗長化	• AX6600S の記述を追加しました。
冗長構成の運用方法	• コールドスタンバイ 2 についての記述を追加しました。
PSP の冗長化	• 本章を追加しました。

項目	追加・変更内容
CFM	<ul style="list-style-type: none"> 本章を追加しました。

【Ver. 11.0 対応版】

表 変更履歴

項目	追加・変更内容
帯域監視使用時の注意事項	<ul style="list-style-type: none"> デフォルトユーザ優先度書き換えとの併用動作の記述を追加しました。
ユーザ優先度書き換え	<ul style="list-style-type: none"> デフォルトユーザ優先度書き換えとの併用動作の記述を追加しました。
優先度決定の解説	<ul style="list-style-type: none"> 階層化シェーパのユーザ指定の記述を追加しました。
フローに対するユーザの設定	<ul style="list-style-type: none"> 本項を追加しました。
VLAN ユーザマッピングの設定	<ul style="list-style-type: none"> 本項を追加しました。
階層化シェーパのユーザの確認	<ul style="list-style-type: none"> 本項を追加しました。
階層化シェーパの解説	<ul style="list-style-type: none"> 本節を追加しました。
階層化シェーパ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。
階層化シェーパのオペレーション	<ul style="list-style-type: none"> 本節を追加しました。
廃棄制御	<ul style="list-style-type: none"> 階層化シェーパ NIF に関する記述を追記しました。
バッファ管理	<ul style="list-style-type: none"> 本項を追加しました。
早期検出テールドロップ	<ul style="list-style-type: none"> 本項を追加しました。
廃棄制御使用時の注意事項	<ul style="list-style-type: none"> 本項を追加しました。
階層化シェーパのバッファ管理とテールドロップの設定	<ul style="list-style-type: none"> 本項を追加しました。
階層化シェーパのバッファ管理とテールドロップの確認	<ul style="list-style-type: none"> 本項を追加しました。
階層化シェーパ機能サポート NIF	<ul style="list-style-type: none"> 本項を追加しました。
送信制御をサポートしていない NIF	<ul style="list-style-type: none"> 本項を追加しました。
レイヤ 2 認証	<ul style="list-style-type: none"> 本章を追加しました。
パケット転送時の負荷分散	<ul style="list-style-type: none"> 「(1) ポートごとの振り分け」に NK1GS-8M に関する記述を追記しました。
GSRP の解説	<ul style="list-style-type: none"> GSRP VLAN グループ限定制御機能の記述を追加しました。
装置障害時の動作	<ul style="list-style-type: none"> 「(2) 自動での切り替え (ダイレクトリンク障害検出による切り替え)」にダイレクト障害検出機能, GSRP スイッチ単独起動時のマスタ遷移機能の記述を追加しました。
GSRP VLAN グループ限定制御機能	<ul style="list-style-type: none"> 本項を追加しました。
GSRP の設定と運用	<ul style="list-style-type: none"> GSRP VLAN グループ限定制御機能の記述を追加しました。
GSRP VLAN グループ限定制御機能の設定	<ul style="list-style-type: none"> 本項を追加しました。
VRRP のサポート規格	<ul style="list-style-type: none"> draft-ietf-vrrp-unified-spec-02 サポートに伴い記述を変更しました。
グループ切替機能	<ul style="list-style-type: none"> 本項を追加しました。
Flush Request 機能	<ul style="list-style-type: none"> 本項を追加しました。
VRRP 使用時の注意事項	<ul style="list-style-type: none"> 「(5) IPv6 VRRP と RA の連携について」を追加しました。
VRRP 動作モードの設定	<ul style="list-style-type: none"> draft-ietf-vrrp-unified-spec-02 の設定の記述を追加しました。
仮想ルータのグループ化	<ul style="list-style-type: none"> 本項を追加しました。
グループ構成の変更	<ul style="list-style-type: none"> 本項を追加しました。

項目	追加・変更内容
仮想ルータの設定確認	<ul style="list-style-type: none"> グループ情報の確認例を追加しました。
SNMPv1, SNMPv2C による VRF からの MIB アクセス許可の設定	<ul style="list-style-type: none"> 本項を追加しました。
SNMPv3 による VRF からの MIB アクセス許可の設定	<ul style="list-style-type: none"> 本項を追加しました。
SNMPv1, SNMPv2C による VRF へのトラップ送信の設定	<ul style="list-style-type: none"> 本項を追加しました。
SNMPv3 による VRF へのトラップ送信の設定	<ul style="list-style-type: none"> 本項を追加しました。
ポートミラーリング	<ul style="list-style-type: none"> 送受信フレームの別ポートへのミラーリングに関する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
Web 認証	<ul style="list-style-type: none"> コンフィギュレーションの設定例を修正しました。 認証除外の設定方法の記述を追加しました。
RADIUS 認証方式の事前準備	<ul style="list-style-type: none"> NAS-IPv6-Address を追加しました。
MAC 認証	<ul style="list-style-type: none"> 認証除外の設定方法の記述を追加しました。
RADIUS 認証方式の事前準備	<ul style="list-style-type: none"> NAS-IPv6-Address を追加しました。
L2 ループ検知	<ul style="list-style-type: none"> 本章を追加しました。

【Ver. 10.6 対応版】

表 変更履歴

項目	追加・変更内容
Web 認証	<ul style="list-style-type: none"> 固定 VLAN モードの記述を追加しました。
MAC 認証	<ul style="list-style-type: none"> 本章を追加しました。
冗長構成の運用方法	<ul style="list-style-type: none"> 記述を変更しました。
障害発生時の BSU 動作	<ul style="list-style-type: none"> フェイルセーフモードの記述を追加しました。 固定モードの記述を追加しました。
パケット転送時の負荷分散	<ul style="list-style-type: none"> 本項を追加しました。
冗長構成時の注意事項	<ul style="list-style-type: none"> 本項を追加しました。
コンフィギュレーションコマンド設定例	<ul style="list-style-type: none"> 「(1) BSU の冗長構成を設定する」の記述を変更しました。 「(3) BSU の固定モード, 送信元 MAC アドレスごとの振り分けの設定」を追加しました。 「(4) BSU の固定モード, 送信元 MAC アドレスごとの振り分け設定時における BSU 増設時の設定手順」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
認証手順	<ul style="list-style-type: none"> ログイン画面などについて説明を追加しました。

項目	追加・変更内容
認証エラーメッセージ	• エラーメッセージを追加しました。
Web 認証画面入れ替え機能	• 本項を追加しました。
Web 認証画面の登録	• 本項を追加しました。
登録した Web 認証画面の削除	• 本項を追加しました。
Web 認証画面の情報表示	• 本項を追加しました。
Web 認証画面作成手順	• 本節を追加しました。

【Ver. 10.4 対応版】

表 変更履歴

項目	追加・変更内容
RADIUS 認証方式 + 外部 DHCP サーバ + 複数の認証後 VLAN 使用時の構成	• 本項を追加しました。
認証 VLAN	• スイッチ間非同期モードの記述を追加しました。
GSRP の切り替え制御	• GSRP Flush request フレームの中継機能に関する記述を追加しました。
GSRP 使用時の注意事項	• GSRP Flush request フレームの中継について記述を追加しました。

【Ver. 10.3 対応版】

表 変更履歴

項目	追加・変更内容
uRPF	• 本章を追加しました。
コンフィギュレーションコマンド一覧	• qos-queue-group, qos-queue-list, traffic-shaper rate コマンドの記述を追加しました。
帯域監視解説	• 本節を追加しました。
帯域監視のコンフィギュレーション	• 本節を追加しました。
帯域監視のオペレーション	• 本節を追加しました。
スケジューリング	• RR, 4PQ+4WFQ, 2PQ+4WFQ+2BEQ, 4WFQ+4BEQ のスケジューリングを追加しました。
ポート帯域制御	• ポート帯域制御機能を追加しました。
Web 認証	• 本章を追加しました。
電源 (PS) の冗長化	• AX6700S の記述を追加しました。
基本制御機構 / 管理スイッチング機構の冗長化	• AX6700S の記述を追加しました。
系切替時の通信無停止対応機能一覧	• 本項を追加しました。
基本スイッチング機構の冗長化	• 本章を追加しました。
ストームコントロール	• 本章を追加しました。
IEEE802.3ah/UDLD	• 本章を追加しました。
sFlow 統計 (フロー統計) 機能	• 本章を追加しました。
ポートミラーリング	• 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 フィルタ

1	フィルタ	1
1.1	解説	2
1.1.1	フィルタの概要	2
1.1.2	フロー検出	3
1.1.3	フローモード	3
1.1.4	フロー検出条件	4
1.1.5	アクセスリスト	10
1.1.6	暗黙の廃棄	12
1.1.7	フィルタ使用時の注意事項	12
1.2	コンフィグレーション	16
1.2.1	コンフィグレーションコマンド一覧	16
1.2.2	フローモードの設定	16
1.2.3	MAC ヘッダで中継・廃棄をする設定	17
1.2.4	IP ヘッダ・TCP/UDP ヘッダで中継・廃棄をする設定	18
1.2.5	MAC ヘッダ・IP ヘッダ・TCP/UDP ヘッダで中継・廃棄をする設定	20
1.2.6	複数インタフェースフィルタの設定	21
1.3	オペレーション	22
1.3.1	運用コマンド一覧	22
1.3.2	フィルタの確認	22
2	アクセスリストロギング	25
2.1	解説	26
2.1.1	アクセスリストロギングの概要	26
2.1.2	アクセスリストログの表示内容	27
2.1.3	ログ出力インターバル機能	30
2.1.4	スレッシュホールド機能	30
2.1.5	ソフトウェアパケット制御機能	30
2.1.6	ログ出力の開始と停止について	31
2.1.7	アクセスリストロギングの注意事項	31
2.2	コンフィグレーション	33
2.2.1	コンフィグレーションコマンド一覧	33
2.2.2	ハードウェアモードの設定	33
2.2.3	アクセスリストロギングの設定	33
2.2.4	syslog サーバへアクセスリストログを通知する設定	34
2.2.5	アクセスリストログ情報を長期間保持する設定	35
2.3	オペレーション	36
2.3.1	運用コマンド一覧	36

2.3.2	アクセスリストロギング情報の確認	36
2.3.3	アクセスリストログ情報の確認	36
2.3.4	ログ出力の開始と停止	37

3

uRPF	39
3.1 解説	40
3.1.1 uRPF の概要	40
3.1.2 サポートモード	40
3.1.3 uRPF 使用時の注意事項	41
3.2 コンフィグレーション	43
3.2.1 コンフィグレーションコマンド一覧	43
3.2.2 装置全体での uRPF 設定	43
3.2.3 IPv4 の uRPF 設定	43
3.2.4 IPv6 の uRPF 設定	44
3.3 オペレーション	45
3.3.1 uRPF 設定が有効かどうかの確認	45
3.3.2 装置全体での uRPF による廃棄パケット数確認	45
3.3.3 インタフェースごとの uRPF による廃棄パケット数確認	46

第 2 編 QoS

4

QoS 制御の概要	47
4.1 QoS 制御構造	48
4.2 QoS 制御共通のコンフィグレーション	50
4.2.1 コンフィグレーションコマンド一覧	50
4.3 QoS 制御共通のオペレーション	52
4.3.1 運用コマンド一覧	52

5

フロー制御	53
5.1 フロー検出解説	54
5.1.1 フローモード	54
5.1.2 フロー検出条件	55
5.1.3 QoS フローリスト	61
5.1.4 フロー検出使用時の注意事項	63
5.2 フロー検出コンフィグレーション	66
5.2.1 フローモードの設定	66
5.2.2 複数インタフェースの QoS 制御の指定	67
5.3 フロー検出のオペレーション	68

5.3.1	IPv4 パケットをフロー検出条件とした QoS 制御の動作確認	68
5.4	帯域監視解説	69
5.4.1	帯域監視	69
5.4.2	帯域監視ストームコントロールモード	70
5.4.3	帯域監視使用時の注意事項	72
5.5	帯域監視のコンフィグレーション	74
5.5.1	帯域監視ストームコントロールモードの設定	74
5.5.2	最大帯域制御の設定	74
5.5.3	最低帯域監視違反時のキューイング優先度の設定	74
5.5.4	最低帯域監視違反時の DSCP 書き換えの設定	75
5.5.5	最大帯域制御と最低帯域監視の組み合わせの設定	76
5.6	帯域監視のオペレーション	77
5.6.1	最大帯域制御の確認	77
5.6.2	最低帯域監視違反時のキューイング優先度の確認	77
5.6.3	最低監視帯域違反時の DSCP 書き換えの確認	77
5.6.4	最大帯域制御と最低帯域監視の組み合わせの確認	78
5.7	マーカー解説	79
5.7.1	ユーザ優先度書き換え	79
5.7.2	DSCP 書き換え	80
5.7.3	マーカー使用時の注意事項	81
5.8	マーカーのコンフィグレーション	82
5.8.1	ユーザ優先度書き換えの設定	82
5.8.2	DSCP 書き換えの設定	82
5.9	マーカーのオペレーション	84
5.9.1	ユーザ優先度書き換えの確認	84
5.9.2	DSCP 書き換えの確認	84
5.10	優先度決定の解説	85
5.10.1	出力優先度とキューイング優先度の直接指定	85
5.10.2	DSCP マッピング	86
5.10.3	階層化シェーバのユーザ指定	87
5.10.4	VLAN ユーザマッピング	88
5.10.5	優先度決定のデフォルト動作	89
5.10.6	優先度決定使用時の注意事項	90
5.11	優先度決定コンフィグレーション	92
5.11.1	出力優先度の設定	92
5.11.2	DSCP マッピングの設定	92
5.11.3	フローに対するユーザの設定	93
5.11.4	VLAN ユーザマッピングの設定	94
5.12	優先度のオペレーション	95
5.12.1	優先度の確認	95
5.12.2	階層化シェーバのユーザの確認	95
5.12.3	VLAN ユーザマッピングの確認	96

6

送信制御	97
6.1 レガシーシェーパ解説	98
6.1.1 レガシーシェーパの概要	98
6.1.2 スケジューリング	99
6.1.3 キュー数指定	101
6.1.4 ポート帯域制御	101
6.2 レガシーシェーパのコンフィグレーション	103
6.2.1 スケジューリングの設定	103
6.2.2 キュー数指定の設定	103
6.2.3 ポート帯域制御の設定	103
6.3 レガシーシェーパのオペレーション	105
6.3.1 スケジューリングの確認	105
6.3.2 キュー数指定の確認	105
6.3.3 ポート帯域制御の確認	106
6.4 階層化シェーパの解説	107
6.4.1 シェーパモード	108
6.4.2 階層化シェーパのスケジューリング	116
6.4.3 階層化シェーパの帯域制御	119
6.4.4 シェーパ自動設定機能	123
6.4.5 デフォルトユーザ優先度書き換え	123
6.4.6 階層化シェーパ使用時の注意事項	124
6.5 階層化シェーパのコンフィグレーション	125
6.5.1 シェーパモードの設定	125
6.5.2 ユーザ帯域制御およびスケジューリングの設定	125
6.5.3 ポート帯域制御の設定	125
6.5.4 シェーパ自動設定機能の設定	126
6.6 階層化シェーパのオペレーション	127
6.6.1 ユーザ数の確認	127
6.6.2 階層化シェーパの確認	127
6.7 廃棄制御解説	129
6.7.1 廃棄制御	129
6.7.2 バッファ管理	131
6.7.3 早期検出テールドロップ	132
6.7.4 廃棄制御使用時の注意事項	132
6.8 廃棄制御のコンフィグレーション	134
6.8.1 キューイング優先度の設定	134
6.8.2 階層化シェーパのバッファ管理とテールドロップの設定	134
6.9 廃棄制御のオペレーション	136
6.9.1 キューイング優先度の確認	136
6.9.2 階層化シェーパのバッファ管理とテールドロップの確認	136
6.10 NIF 種別と送信制御機能との対応	138

6.10.1	レガシーシェーバ機能サポート NIF	138
6.10.2	階層化シェーバ機能サポート NIF	140
6.10.3	送信制御をサポートしていない NIF	143

第3編 レイヤ2 認証

7	レイヤ2 認証	145
7.1	概要	146
7.1.1	レイヤ2 認証種別	146
7.1.2	認証方式	147
7.2	レイヤ2 認証と他機能との共存について	148
7.2.1	レイヤ2 認証と他機能との共存	148
7.2.2	同一ポート内での共存	150
7.2.3	レイヤ2 認証共存時の認証優先	153
7.3	レイヤ2 認証共通の機能	155
7.3.1	設定時の認証単位	155
7.3.2	認証前端末の通信許可	155
7.3.3	認証済み端末のポート間移動	157
7.4	レイヤ2 認証使用時の注意事項	162
7.4.1	本装置の設定および状態変更時の注意	162
7.4.2	RADIUS サーバ使用時の注意	162
7.5	レイヤ2 認証共通コンフィグレーション	164
7.5.1	コンフィグレーションコマンド一覧	164
7.5.2	レイヤ2 認証共通コンフィグレーションコマンドのパラメータ設定	164
8	IEEE802.1X の解説	165
8.1	IEEE802.1X の概要	166
8.1.1	サポート機能	167
8.2	拡張機能の概要	173
8.2.1	認証モード	173
8.2.2	端末検出動作切り替えオプション	178
8.2.3	端末要求再認証抑止機能	180
8.2.4	RADIUS サーバ接続機能	180
8.2.5	EAPOL フォワーディング機能	181
8.2.6	VLAN 単位認証 (動的) の動作モード	181
8.3	IEEE802.1X 使用時の注意事項	182

9	IEEE802.1X の設定と運用	185
9.1	IEEE802.1X のコンフィグレーション	186
9.1.1	コンフィグレーションコマンド一覧	186
9.1.2	IEEE802.1X の基本的な設定	187
9.1.3	認証モードオプションの設定	188
9.1.4	認証処理に関する設定	191
9.1.5	RADIUS サーバ関連の設定	195
9.2	IEEE802.1X のオペレーション	196
9.2.1	運用コマンド一覧	196
9.2.2	IEEE802.1X 状態の表示	196
9.2.3	IEEE802.1X 認証状態の変更	198
10	Web 認証の解説	199
10.1	概要	200
10.2	システム構成例	201
10.2.1	固定 VLAN モード	201
10.2.2	ダイナミック VLAN モード	203
10.2.3	レガシーモード	205
10.2.4	IP アドレス設定方法による構成例	207
10.3	認証機能	211
10.3.1	認証前端末の通信許可	211
10.3.2	認証ネットワークへのログイン	211
10.3.3	認証ネットワークからのログアウト	213
10.3.4	認証済み端末のポート間移動	216
10.3.5	アカウント機能	216
10.4	認証手順	219
10.5	内蔵 Web 認証 DB および RADIUS サーバの準備	223
10.5.1	内蔵 Web 認証 DB の準備	223
10.5.2	RADIUS サーバの準備	223
10.6	認証エラーメッセージ	226
10.7	Web 認証画面入れ替え機能	229
10.8	系切替時の引き継ぎ情報	230
10.9	Web 認証使用時の注意事項	231
11	Web 認証の設定と運用	233
11.1	コンフィグレーション	234
11.1.1	コンフィグレーションコマンド一覧	234
11.1.2	固定 VLAN モードのコンフィグレーション	235
11.1.3	ダイナミック VLAN モードのコンフィグレーション	238

11.1.4	レガシーモードのコンフィグレーション	244
11.1.5	Web 認証のパラメータ設定	256
11.1.6	認証除外の設定方法	260
11.2	オペレーション	263
11.2.1	運用コマンド一覧	263
11.2.2	Web 認証の設定情報表示	263
11.2.3	Web 認証の状態表示	265
11.2.4	Web 認証の認証状態表示	266
11.2.5	内蔵 Web 認証 DB の作成	267
11.2.6	内蔵 Web 認証 DB のバックアップ	268
11.2.7	Web 認証画面の登録	268
11.2.8	登録した Web 認証画面の削除	269
11.2.9	Web 認証画面の情報表示	269
11.3	Web 認証画面作成手順	270
11.3.1	ログイン画面 (login.html)	270
11.3.2	ログアウト画面 (logout.html)	273
11.3.3	認証エラーメッセージファイル (webauth.msg)	275
11.3.4	Web 認証固有タグ	276
11.3.5	その他の画面サンプル	277

12 MAC 認証の解説 283

12.1	概要	284
12.2	システム構成例	285
12.2.1	固定 VLAN モード	285
12.2.2	ダイナミック VLAN モード	287
12.3	認証機能	289
12.3.1	認証失敗後の動作	289
12.3.2	認証解除方式	289
12.3.3	認証済み端末のポート間移動	291
12.3.4	アカウント機能	291
12.4	内蔵 MAC 認証 DB および RADIUS サーバの準備	294
12.4.1	内蔵 MAC 認証 DB の準備	294
12.4.2	RADIUS サーバの準備	294
12.5	MAC 認証使用時の注意事項	298

13 MAC 認証の設定と運用 299

13.1	コンフィグレーション	300
13.1.1	コンフィグレーションコマンド一覧	300
13.1.2	固定 VLAN モードのコンフィグレーション	300
13.1.3	ダイナミック VLAN モードのコンフィグレーション	303
13.1.4	MAC 認証のパラメータ設定	305

13.1.5	認証除外の設定方法	307
13.2	オペレーション	310
13.2.1	運用コマンド一覧	310
13.2.2	MAC 認証の設定情報表示	310
13.2.3	MAC 認証の統計情報表示	311
13.2.4	MAC 認証の認証状態表示	311
13.2.5	内蔵 MAC 認証 DB の作成	312
13.2.6	内蔵 MAC 認証 DB のバックアップ	312

14	認証 VLAN 【OP-VAA】	313
14.1	解説	314
14.1.1	機能概要	314
14.1.2	認証手順	315
14.1.3	認証 VLAN で使用する VLAN	316
14.1.4	認証 VLAN の応用構成	316
14.1.5	スイッチ間非同期モード	318
14.1.6	認証 VLAN 使用上の注意	320
14.2	コンフィグレーション	323
14.2.1	コンフィグレーションコマンド一覧	323
14.2.2	認証 VLAN の基本的な設定	323
14.2.3	冗長構成	326
14.2.4	認証 VLAN のパラメータ設定	330
14.3	オペレーション	332
14.3.1	運用コマンド一覧	332
14.3.2	認証 VLAN 動作確認	332

第4編 セキュリティ

15	DHCP snooping	333
15.1	解説	334
15.1.1	概要	334
15.1.2	DHCP パケットの監視	335
15.1.3	DHCP パケットの受信レート制限	340
15.1.4	端末フィルタ	341
15.1.5	ダイナミック ARP 検査	343
15.1.6	ARP パケットの受信レート制限	346
15.1.7	DHCP snooping 使用時の注意事項	346
15.2	コンフィグレーション	349
15.2.1	コンフィグレーションコマンド一覧	349

15.2.2	基本設定	349
15.2.3	DHCP パケットの受信レート制限	352
15.2.4	端末フィルタ	352
15.2.5	ダイナミック ARP 検査	352
15.2.6	ARP パケットの受信レート制限	353
15.2.7	固定 IP アドレスを持つ端末を接続した場合	353
15.2.8	本装置の配下に DHCP リレーが接続された場合	354
15.2.9	本装置の配下に Option82 を付与する DHCP リレーが接続された場合	356
15.2.10	syslog サーバへの出力	358
15.3	オペレーション	359
15.3.1	運用コマンド一覧	359
15.3.2	DHCP snooping バインディングデータベースの確認	359
15.3.3	DHCP snooping 統計情報の確認	359
15.3.4	ダイナミック ARP 検査の確認	360
15.3.5	DHCP snooping ログメッセージの確認	360

第 5 編 冗長化構成による高信頼化機能

16	電源機構 (P S) の冗長化	361
16.1	解説	362
16.2	PS の状態確認, および PS に関するコンフィグレーション	363
16.2.1	コンフィグレーション・運用コマンド一覧	363
16.2.2	PS 冗長構成で運用する場合のコンフィグレーション	363
16.2.3	PS の状態確認	363
17	BCU/CSU/MSU の冗長化	365
17.1	解説	366
17.1.1	冗長化時の装置構成	366
17.1.2	冗長構成での動作	367
17.1.3	装置起動時の待機系および運用系との整合性確認	368
17.1.4	運用系システムの管理情報の同期および同期契機	368
17.1.5	系切替時の通信無停止対応機能一覧	369
17.1.6	コンフィグレーション不一致時の動作	371
17.1.7	運用コマンドおよび ACH スイッチによる系切替	371
17.1.8	冗長構成時の注意事項	372
17.2	オペレーション	373
17.2.1	運用コマンド一覧	373
17.2.2	待機系の状態確認	373
17.2.3	系切替の実施	373

17.2.4	情報同期の実施	373
--------	---------	-----

18 BSU の冗長化【AX6700S】 375

18.1	解説	376
18.1.1	冗長化時の装置構成	376
18.1.2	冗長構成の運用方法	376
18.1.3	障害発生時の BSU 動作	377
18.1.4	パケット転送時の負荷分散	379
18.1.5	運用時の同期情報および同期契機	380
18.1.6	冗長構成時の注意事項	381
18.2	コンフィグレーション	382
18.2.1	コンフィグレーションコマンド一覧	382
18.2.2	BSU の冗長構成の設定	382
18.2.3	待機系の電力消費量を下げる設定	382
18.2.4	BSU の固定モードおよび送信元 MAC アドレスごとの振り分けの設定	383
18.2.5	BSU の固定モードおよび送信元 MAC アドレスごとの振り分け設定時に BSU を増設する設定	383
18.3	オペレーション	385
18.3.1	運用コマンド一覧	385
18.3.2	運用系および待機系の状態確認	385
18.3.3	系切替の実施	386

19 PSP の冗長化【AX6600S】 387

19.1	解説	388
19.1.1	冗長化時の装置構成	388
19.1.2	冗長構成の運用方法	388
19.1.3	障害発生時の PSP 動作	389
19.1.4	パケット転送時の負荷分散	390
19.1.5	運用時の同期情報および同期契機	391
19.2	コンフィグレーション	392
19.2.1	コンフィグレーションコマンド一覧	392
19.2.2	すべての PSP を運用系とする設定	392
19.2.3	PSP の冗長構成の設定	392
19.2.4	待機系 PSP の電力消費量を下げる設定	392
19.3	オペレーション	393
19.3.1	運用コマンド一覧	393
19.3.2	運用系および待機系 PSP の状態確認	393

20 NIF の冗長化【AX6700S】【AX6600S】 395

20.1	解説	396
20.1.1	冗長化時の装置構成	396

20.1.2	冗長構成での動作	397
20.1.3	冗長構成の運用方法	398
20.1.4	NIF 冗長機能に関する注意事項	398
20.2	コンフィグレーション	399
20.2.1	コンフィグレーションコマンド一覧	399
20.2.2	NIF の冗長構成の設定	399
20.3	オペレーション	401
20.3.1	運用コマンド一覧	401
20.3.2	冗長化 NIF の状態確認	401

21	GSRP の解説	403
21.1	GSRP の概要	404
21.1.1	概要	404
21.1.2	特長	405
21.1.3	サポート仕様	406
21.2	GSRP の基本原理	407
21.2.1	ネットワーク構成	407
21.2.2	GSRP 管理 VLAN	408
21.2.3	GSRP の切り替え制御	408
21.2.4	マスタ, バックアップの選択方法	410
21.3	GSRP の動作概要	412
21.3.1	GSRP の状態	412
21.3.2	装置障害時の動作	412
21.3.3	リンク障害時の動作	415
21.3.4	バックアップ固定機能	417
21.3.5	GSRP VLAN グループ限定制御機能	417
21.3.6	GSRP 制御対象外ポート	417
21.4	レイヤ 3 冗長切替機能	418
21.4.1	概要	418
21.5	GSRP のネットワーク設計	420
21.5.1	VLAN グループ単位のロードバランス構成	420
21.5.2	GSRP グループの多段構成	421
21.5.3	レイヤ 3 冗長切替機能での上流ネットワーク障害による切り替え	422
21.6	GSRP 使用時の注意事項	426

22	GSRP の設定と運用	431
22.1	コンフィグレーション	432
22.1.1	コンフィグレーションコマンド一覧	432
22.1.2	GSRP の基本的な設定	432
22.1.3	マスタ, バックアップの選択に関する設定	435
22.1.4	レイヤ 3 冗長切替機能の設定	436

22.1.5	GSRP VLAN グループ限定制御機能の設定	436
22.1.6	GSRP 制御対象外ポートの設定	436
22.1.7	GSRP のパラメータの設定	437
22.1.8	ポートリセット機能の設定	439
22.1.9	ダイレクトリンク障害検出の設定	439
22.2	オペレーション	441
22.2.1	運用コマンド一覧	441
22.2.2	GSRP の状態の確認	441
22.2.3	コマンドによる状態遷移	443
22.2.4	遅延状態のポートのアクティブポート即時反映	443
23	VRRP	445
23.1	解説	446
23.1.1	仮想ルータの MAC アドレスと IP アドレス	446
23.1.2	VRRP における障害検出の仕組み	448
23.1.3	マスタの選出方法	448
23.1.4	ADVERTISEMENT パケットの認証	449
23.1.5	アクセプトモード	450
23.1.6	トラッキング機能	450
23.1.7	VRRP のサポート規格	456
23.1.8	グループ切替機能	458
23.1.9	Flush Request 機能	461
23.1.10	VRRP 使用時の注意事項	462
23.2	コンフィグレーション	465
23.2.1	コンフィグレーションコマンド一覧	465
23.2.2	VRRP のコンフィグレーションの流れ	466
23.2.3	仮想ルータへの IPv4 アドレス設定	466
23.2.4	仮想ルータへの IPv6 アドレス設定	467
23.2.5	優先度の設定	467
23.2.6	ADVERTISEMENT パケット送信間隔の設定	468
23.2.7	自動切り戻し抑止の設定	469
23.2.8	自動切り戻し抑止時間の設定	469
23.2.9	障害監視インタフェースと VRRP ポーリングの設定	470
23.2.10	VRRP 動作モードの設定	473
23.2.11	仮想ルータのグループ化	473
23.2.12	グループ構成の変更	476
23.3	オペレーション	480
23.3.1	運用コマンド一覧	480
23.3.2	仮想ルータの設定確認	480
23.3.3	track の設定確認	481
23.3.4	切り戻し処理の実行	481

第6編 ネットワークの障害検出による高信頼化機能

24	IEEE802.3ah/UDLD	483
24.1	解説	484
24.1.1	概要	484
24.1.2	サポート仕様	484
24.1.3	IEEE802.3ah/UDLD 使用時の注意事項	485
24.2	コンフィグレーション	486
24.2.1	コンフィグレーションコマンド一覧	486
24.2.2	IEEE802.3ah/UDLD の設定	486
24.3	オペレーション	488
24.3.1	運用コマンド一覧	488
24.3.2	IEEE802.3ah/OAM 情報の表示	488
25	ストームコントロール	491
25.1	解説	492
25.1.1	ストームコントロールの概要	492
25.1.2	ストームコントロール使用時の注意事項	492
25.2	コンフィグレーション	494
25.2.1	コンフィグレーションコマンド一覧	494
25.2.2	ストームコントロールの設定	494
26	L2 ループ検知	497
26.1	解説	498
26.1.1	概要	498
26.1.2	動作仕様	499
26.1.3	適用例	499
26.1.4	L2 ループ検知使用時の注意事項	501
26.2	コンフィグレーション	504
26.2.1	コンフィグレーションコマンド一覧	504
26.2.2	L2 ループ検知の設定	504
26.3	オペレーション	507
26.3.1	運用コマンド一覧	507
26.3.2	L2 ループ状態の確認	507
27	CFM	509
27.1	解説	510
27.1.1	概要	510
27.1.2	CFM の構成要素	511

27.1.3	ドメインの設計	516
27.1.4	Continuity Check	520
27.1.5	Loopback	522
27.1.6	Linktrace	523
27.1.7	共通動作仕様	526
27.1.8	CFM で使用するデータベース	528
27.1.9	CFM 使用時の注意事項	530
27.2	コンフィギュレーション	532
27.2.1	コンフィギュレーションコマンド一覧	532
27.2.2	CFM の設定 (複数ドメイン)	532
27.2.3	CFM の設定 (同一ドメイン, 複数 MA)	534
27.3	オペレーション	536
27.3.1	運用コマンド一覧	536
27.3.2	MP 間の接続確認	536
27.3.3	MP 間のルート確認	536
27.3.4	ルート上の MP の状態確認	537
27.3.5	CFM の状態の確認	537
27.3.6	障害の詳細情報の確認	538

第 7 編 リモートネットワーク管理

28	SNMP を使用したネットワーク管理	539
28.1	解説	540
28.1.1	SNMP 概説	540
28.1.2	MIB 概説	543
28.1.3	SNMPv1, SNMPv2C オペレーション	545
28.1.4	SNMPv3 オペレーション	551
28.1.5	トラップ	554
28.1.6	インフォーム	555
28.1.7	RMON MIB	556
28.1.8	SNMP マネージャとの接続時の注意事項	559
28.2	コンフィギュレーション	560
28.2.1	コンフィギュレーションコマンド一覧	560
28.2.2	SNMPv1, SNMPv2C による MIB アクセス許可の設定	560
28.2.3	SNMPv3 による MIB アクセス許可の設定	561
28.2.4	SNMPv1, SNMPv2C によるトラップ送信の設定	561
28.2.5	SNMPv3 によるトラップ送信の設定	562
28.2.6	SNMPv2C によるインフォーム送信の設定	562
28.2.7	リンクトラップの抑止	563
28.2.8	RMON イーサネットヒストリグループの制御情報の設定	564

28.2.9	RMON による特定 MIB 値の閾値チェック	564
28.2.10	SNMPv1, SNMPv2C による VRF からの MIB アクセス許可の設定【OP-NPAR】	565
28.2.11	SNMPv3 による VRF からの MIB アクセス許可の設定【OP-NPAR】	565
28.2.12	SNMPv1, SNMPv2C による VRF へのトラップ送信の設定【OP-NPAR】	566
28.2.13	SNMPv3 による VRF へのトラップ送信の設定【OP-NPAR】	566
28.2.14	SNMPv2C による VRF へのインフォーム送信の設定【OP-NPAR】	567
28.3	オペレーション	568
28.3.1	運用コマンド一覧	568
28.3.2	SNMP マネージャとの通信の確認	568

29 ログ出力機能 571

29.1	解説	572
29.2	コンフィグレーション	573
29.2.1	コンフィグレーションコマンド一覧	573
29.2.2	ログの syslog 出力の設定	573
29.2.3	ログの VRF への syslog 出力の設定	573
29.2.4	ログの E-Mail 出力の設定	574

30 sFlow 統計（フロー統計）機能 575

30.1	解説	576
30.1.1	sFlow 統計の概要	576
30.1.2	sFlow 統計エージェント機能	577
30.1.3	sFlow パケットフォーマット	577
30.1.4	本装置での sFlow 統計の動作について	584
30.2	コンフィグレーション	586
30.2.1	コンフィグレーションコマンド一覧	586
30.2.2	sFlow 統計の基本的な設定	586
30.2.3	sFlow 統計コンフィグレーションパラメータの設定例	590
30.3	オペレーション	594
30.3.1	運用コマンド一覧	594
30.3.2	コレクタとの通信の確認	594
30.3.3	sFlow 統計機能の運用中の確認	594
30.3.4	sFlow 統計のサンプリング間隔の調整方法	595

第 8 編 隣接装置情報の管理

31 LLDP 599

31.1	解説	600
------	----	-----

31.1.1	概要	600
31.1.2	サポート仕様	600
31.1.3	LLDP 使用時の注意事項	602
31.2	コンフィグレーション	604
31.2.1	コンフィグレーションコマンド一覧	604
31.2.2	LLDP の設定	604
31.3	オペレーション	605
31.3.1	運用コマンド一覧	605
31.3.2	LLDP 情報の表示	605

32 OADP 607

32.1	解説	608
32.1.1	概要	608
32.1.2	サポート仕様	609
32.1.3	OADP 使用時の注意事項	610
32.2	コンフィグレーション	612
32.2.1	コンフィグレーションコマンド一覧	612
32.2.2	OADP の設定	612
32.3	オペレーション	614
32.3.1	運用コマンド一覧	614
32.3.2	OADP 情報の表示	614

第9編 ポートミラーリング

33 ポートミラーリング 617

33.1	解説	618
33.1.1	ポートミラーリングの概要	618
33.1.2	ポートミラーリングの注意事項	619
33.2	コンフィグレーション	620
33.2.1	コンフィグレーションコマンド一覧	620
33.2.2	ポートミラーリングの設定	620

付録 623

付録 A	準拠規格	624
付録 A.1	uRPF	624
付録 A.2	Diff-serv	624
付録 A.3	IEEE802.1X	624
付録 A.4	Web 認証	624

付録 A.5	MAC 認証	625
付録 A.6	DHCP snooping	625
付録 A.7	VRRP	625
付録 A.8	IEEE802.3ah/UDLD	625
付録 A.9	CFM	626
付録 A.10	SNMP	626
付録 A.11	SYSLOG	628
付録 A.12	sFlow	628
付録 A.13	LLDP	628

索引

629

1

フィルタ

フィルタは、受信したフレームを中継したり、廃棄したりする機能です。この章ではフィルタ機能の解説と操作方法について説明します。

1.1 解説

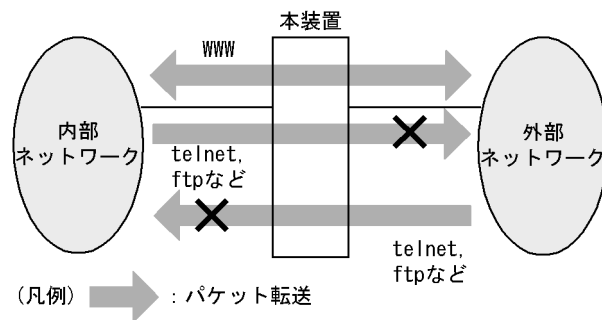
1.2 コンフィグレーション

1.3 オペレーション

1.1 解説

フィルタは、受信したある特定のフレームを中継または廃棄する機能です。フィルタはネットワークのセキュリティを確保するために使用します。フィルタを使用すれば、ユーザごとにネットワークへのアクセスを制限できます。例えば、内部ネットワークと外部ネットワーク間で WWW は中継しても、telnet や ftp は廃棄したいなどの運用ができます。外部ネットワークからの不正なアクセスを防ぎ、また、内部ネットワークから外部ネットワークへ不要な情報の漏洩を防ぐことができます。フィルタを使用したネットワーク構成例を次に示します。

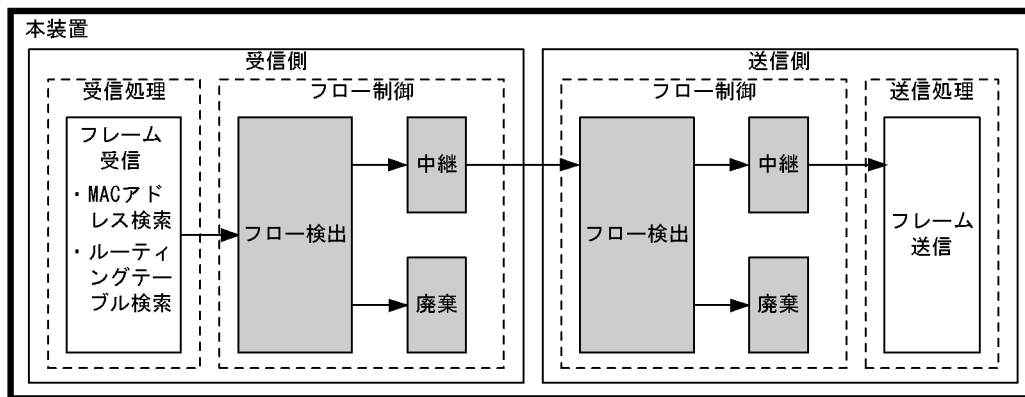
図 1-1 フィルタを使用したネットワーク構成例



1.1.1 フィルタの概要

本装置のフィルタの機能ブロックを次の図に示します。

図 1-2 本装置のフィルタの機能ブロック



(凡例) : この節で説明するブロック

この図に示したフィルタの各機能ブロックの概要を次の表に示します。

表 1-1 フィルタの各機能ブロックの概要

機能部位		機能概要
フロー制御部	フロー検出	MAC アドレスやプロトコル種別、IP アドレス、TCP/UDP のポート番号などの条件に一致するフロー（特定フレーム）を検出します。
	中継・廃棄	フロー検出したフレームに対し、中継または廃棄します。

本装置では、MAC アドレス、プロトコル種別、IP アドレス、TCP/UDP のポート番号などのフロー検出

と、中継や廃棄という動作を組み合わせたフィルタエントリを作成し、フィルタを実施します。

本装置のフィルタの仕組みを次に示します。

1. 各インタフェースに設定したフィルタエントリをユーザが設定した優先順に検索します。
2. 一致したフィルタエントリが見つかった時点で検索を終了します。
3. 該当したフレームはフィルタエントリで設定した動作に従って、中継や廃棄が実行されます。
4. すべてのフィルタエントリに一致しなかった場合は、そのフレームを廃棄します。廃棄動作の詳細は、「1.1.6 暗黙の廃棄」を参照してください。

1.1.2 フロー検出

フロー検出とは、フレームの一連の流れであるフローを MAC ヘッダ、IP ヘッダ、TCP ヘッダなどの条件に基づいて検出する機能です。アクセスリストで設定します。アクセスリストの詳細は、「1.1.5 アクセスリスト」を参照してください。

本装置では、イーサネットインタフェース・VLAN インタフェースで、イーサネット V2 形式および IEEE802.3 の SNAP/RFC1042 形式フレームのフロー検出ができます。インタフェースには、検出する中継種別ごとにレイヤ 2 中継のフロー検出、レイヤ 3 中継のフロー検出をそれぞれ設定してください。

フローモードのフロー検出拡張モードを設定した場合は、中継種別ごとのフロー検出に加えて、レイヤ 2 中継とレイヤ 3 中継の両方を対象にしたフロー検出を設定できます。

レイヤ 2 中継は、次のフレームが該当します。

- 本装置がレイヤ 2 スイッチ中継するフレーム
- 本装置宛の非 IP パケット
- 宛先 MAC アドレスが Broadcast または Multicast のフレーム

注

宛先 MAC アドレスが自装置の MAC アドレスである非 IP パケット

レイヤ 3 中継は、次のフレームが該当します。

- 本装置が IPv4 パケット中継するパケット
- 本装置が IPv6 パケット中継するパケット
- 本装置宛の IPv4、IPv6 パケット
- 宛先 IP アドレスが Broadcast または Multicast の IP パケット

注

宛先 MAC アドレスが自装置の MAC アドレスで、かつ宛先 IP アドレスが自装置の IP アドレスである IP パケット

1.1.3 フローモード

本装置では、フロー検出動作を決めるフローモードとして、MAC モードとフロー検出拡張モードを用意しています。MAC モードは VLAN 単位で設定し、フロー検出拡張モードは装置単位で設定します。

なお、MAC モードとフロー検出拡張モードは同時に設定できません。

(1) MAC モード

本装置では、レイヤ 2 中継する非 IP パケット、IP パケットを MAC ヘッダでフロー検出できるフロー

1. フィルタ

モードである MAC モードを用意しています。MAC モードは `flow mac mode` コマンドで指定します。

MAC モードは、VLAN インタフェースに設定した場合に有効となります。また、イーサネットインタフェースにフィルタ・QoS フロー検出を設定した場合は、該当するイーサネットインタフェースが属するすべての VLAN インタフェースに対して MAC モードを設定できません。

なお、MAC モードはフィルタ・QoS で共通の機能です。

(2) フロー検出拡張モード

本装置では、非 IP パケット、IP パケットのすべてをフロー検出対象とし、MAC ヘッダ、IP ヘッダ、レイヤ 4 ヘッダの組み合わせ (Advance 条件) でフロー検出できるフロー検出拡張モードを用意しています。Advance 条件でフロー検出する場合、イーサネットインタフェースではレイヤ 2 中継フレームが、VLAN インタフェースではレイヤ 2 中継フレームとレイヤ 3 中継パケットの両方がフロー検出対象になります。フロー検出拡張モードは `fldm prefer` コマンドで指定します。

なお、フロー検出拡張モード設定ありから設定なしに変更する場合、すべての Advance 条件の設定を削除する必要があります。

(3) フローモードの動作比較

フローモードとフロー動作の関係を次の表に示します。

表 1-2 フローモードとフロー動作の関係

フローモード	対象となるフレーム	フロー動作
設定なし	レイヤ 2 中継する非 IP パケット	MAC アドレス、イーサネットタイプなどの MAC ヘッダでフレームを検出します。
	レイヤ 2 またはレイヤ 3 中継する IPv4、IPv6 パケット	IP ヘッダ、レイヤ 4 ヘッダでフレームを検出します。
MAC モード	レイヤ 2 中継するすべてのフレーム	MAC アドレス、イーサネットタイプなどの MAC ヘッダでフレームを検出します。
	レイヤ 3 中継する IPv4、IPv6 パケット	IP ヘッダ、レイヤ 4 ヘッダでフレームを検出します。
フロー検出拡張モード	レイヤ 2 中継する非 IP パケット	MAC アドレス、イーサネットタイプなどの MAC ヘッダでフレームを検出します。
	レイヤ 2 またはレイヤ 3 中継する IPv4、IPv6 パケット	MAC ヘッダ、IP ヘッダ、レイヤ 4 ヘッダでフレームを検出します。

1.1.4 フロー検出条件

フロー検出するためには、コンフィグレーションでフローを識別するための条件を指定します。フロー検出条件は大きく MAC 条件、IPv4 条件、IPv6 条件、およびフロー検出拡張モードで設定できる Advance 条件に分類されます。

- MAC 条件は、主に MAC アドレスなどの MAC ヘッダでフレームを検出します。
- IPv4 条件は、主に IPv4 アドレスなどの IPv4 ヘッダでフレームを検出します。
- IPv6 条件は、主に IPv6 アドレスなどの IPv6 ヘッダでフレームを検出します。
- Advance 条件は、MAC 条件と IPv4 条件、または MAC 条件と IPv6 条件の組み合わせでフレームを検出します。

フロー検出するインタフェースおよび中継種別ごとに、指定可能なフロー検出条件を次の表に示します。

表 1-3 指定可能なフロー検出条件

フロー検出条件	VLAN			イーサネット			
	レイヤ 2 中継指定		レイヤ 3 中継指定	レイヤ 2 中継およびレイヤ 3 中継両方指定	レイヤ 2 中継指定	レイヤ 3 中継指定	レイヤ 2 中継およびレイヤ 3 中継両方指定
	MAC モード設定あり	MAC モード設定なし					
MAC 条件			-	-		-	-
IPv4 条件	-			-		-	-
IPv6 条件	-			-		-	-
Advance 条件	-	-	-			-	-

(凡例) : 指定できる - : 指定できない

注

Advance 条件はフロー検出拡張モードを設定している場合に指定できます。

指定可能なフロー検出条件の詳細項目を次の表に示します。

表 1-4 指定可能なフロー検出条件の詳細項目

種別	設定項目	VLAN				イーサネット	
		レイヤ 2 中継指定		レイヤ 3 中継指定	レイヤ 2 中継およびレイヤ 3 中継両方指定		
		MAC モード設定あり	MAC モード設定なし				
MAC 条件	コンフィグレーション	VLAN ID ¹	-	-	-	-	
	MAC ヘッダ	送信元 MAC アドレス			-	-	
		宛先 MAC アドレス			-	-	
		イーサネットタイプ			-	-	
VLAN Tag ヘッダ ²	ユーザ優先度			-	-		
IPv4 条件	コンフィグレーション	VLAN ID ¹	-	-	-	-	
	VLAN Tag ヘッダ ²	ユーザ優先度	-			-	

1. フィルタ

種別	設定項目	VLAN				イーサネット		
		レイヤ 2 中継指定	レイヤ 3 中継指定	レイヤ 2 中継およびレイヤ 3 中継両方指定	レイヤ 2 中継指定			
						MACモード設定あり	MACモード設定なし	
IPv6 条件	IPv4 ヘッダ 3 4	上位プロトコル	-			-		
		送信元 IP アドレス	-			-		
		宛先 IP アドレス	-			-		
		ToS	-	-		-	-	
		DSCP	-			-		
		Precedence	-			-		
		フラグメントパケット識別 5	-			-		
	IPv4-TCP ヘッダ	送信元ポート番号	-			-		
		宛先ポート番号	-			-		
		TCP 制御フラグ 6	-	-		-	-	
	IPv4-UDP ヘッダ	送信元ポート番号	-			-		
		宛先ポート番号	-			-		
	IPv4-ICMP ヘッダ	ICMP タイプ値	-			-		
		ICMP コード値	-			-		
	IPv4-IGMP ヘッダ	IGMP コード値	-			-		
	IPv6 条件	コンフィグレーション	VLAN ID 1	-	-	-		
		VLAN Tag ヘッダ 2	ユーザ優先度	-			-	
		IPv6 ヘッダ 3 7	上位プロトコル	-			-	
送信元 IP アドレス 8			-			-		
宛先 IP アドレス			-			-		
Traffic Class			-	-		-	-	
DSCP		-			-			
IPv6-TCP ヘッダ	送信元ポート番号	-			-			

種別	設定項目	VLAN				イーサネット	
		レイヤ 2 中継指定		レイヤ 3 中継指定	レイヤ 2 中継およびレイヤ 3 中継両方指定	レイヤ 2 中継指定	
		MAC モード 設定あり	MAC モード 設定なし				
Advance 条件	宛先ポート番号	-			-		
	TCP 制御フラグ ⁶	-	-		-	-	
	IPv6-UDP ヘッダ	送信元ポート番号	-			-	
		宛先ポート番号	-			-	
	IPv6-ICMP ヘッダ	ICMP タイプ	-			-	
		ICMP コード値	-			-	
	コンフィグレーション	VLAN ID ¹	-	-	-	-	
	MAC ヘッダ	送信元 MAC アドレス	-	-	-	9	
		宛先 MAC アドレス	-	-	-	9	
		イーサネットタイプ	-	-	-		
VLAN Tag ヘッダ ²	ユーザ優先度	-	-	-			
	カスタマ Tag なしのパケット	-	-	-			
	カスタマ Tag の VLAN ID	-	-	-	10	10	
	カスタマ Tag のユーザ優先度	-	-	-	10	10	
IPv4 ヘッダ ^{3 4}	上位プロトコル	-	-	-			
	送信元 IP アドレス	-	-	-			
	宛先 IP アドレス	-	-	-			
	ToS	-	-	-			
	DSCP	-	-	-			
	Precedence	-	-	-			
	フラグメントパケット識別 ⁵	-	-	-			
IPv4-TCP ヘッダ	送信元ポート番号	-	-	-			
	宛先ポート番号	-	-	-			
	TCP 制御フラグ ⁶	-	-	-			

1. フィルタ

種別	設定項目	VLAN				イーサネット
		レイヤ 2 中継指定	レイヤ 3 中継指定	レイヤ 2 中継およびレイヤ 3 中継両方指定	レイヤ 2 中継指定	
						MAC モード 設定あり
IPv4-UDP ヘッダ	送信元ポート番号	-	-	-		
	宛先ポート番号	-	-	-		
IPv4-ICMP ヘッダ	ICMP タイプ値	-	-	-		
	ICMP コード値	-	-	-		
IPv4-IGMP ヘッダ	IGMP コード値	-	-	-		
IPv6 ヘッダ 3 7	上位プロトコル	-	-	-		
	送信元 IP アドレス	-	-	-		
	宛先 IP アドレス	-	-	-		
	Traffic Class	-	-	-		
	DSCP	-	-	-		
IPv6-TCP ヘッダ	送信元ポート番号	-	-	-		
	宛先ポート番号	-	-	-		
	TCP 制御フラグ ⁶	-	-	-		
IPv6-UDP ヘッダ	送信元ポート番号	-	-	-		
	宛先ポート番号	-	-	-		
IPv6-ICMP ヘッダ	ICMP タイプ	-	-	-		
	ICMP コード値	-	-	-		

(凡例) : 指定できる : 指定できる (一部検出できない) - : 指定できない

注 1

本装置のフロー検出で検出できる VLAN ID は、VLAN コンフィグレーションで入力した VLAN に対して付与する値です。入力フレームまたは出力フレームの属する VLAN ID を検出します。複数の VLAN ID をフロー検出の対象とする場合は、VLAN リストで作成した VLAN リスト名称を指定してください。

注 2

VLAN Tag ヘッダの指定についての補足を次に示します。なお、カスタム Tag とは 2 段目の VLAN Tag を指します。

ユーザ優先度

1 段目の VLAN Tag のユーザ優先度です。VLAN Tag なしのパケットは検出しません。

カスタム Tag なしのパケット

2 段目の VLAN Tag がいないパケットです。VLAN Tag が 2 段以上あるパケットは検出しません。

カスタム Tag の VLAN ID

2 段目の VLAN Tag の VLAN ID です。VLAN Tag が 1 段以下のパケットは検出しません。

カスタム Tag のユーザ優先度

2 段目の VLAN Tag のユーザ優先度です。VLAN Tag が 1 段以下のパケットは検出しません。

(i) VLAN Tag 1段のフォーマット

MAC-DA	MAC-SA	1段目の VLAN Tag	Ether Type	Data	FCS
--------	--------	------------------	---------------	------	-----

(ii) VLAN Tag 2段のフォーマット

MAC-DA	MAC-SA	1段目の VLAN Tag	2段目の VLAN Tag	Ether Type	Data	FCS
--------	--------	------------------	------------------	---------------	------	-----

注 3

IP アドレスに own-address または own パラメータを指定することで、フロー検出を設定したインタフェースの IP アドレスが自動で検出できます。IPv4 アドレスの場合は、own-address および own を指定したインタフェースがマルチホームのときはプライマリ IPv4 アドレスが対象になります。IPv6 アドレスの場合は、own-address および own を指定したインタフェースがマルチホームでないときはフロー検出条件に指定できます。

注 4

ToS フィールドの指定についての補足を次に示します。

ToS : ToS フィールドの 3 ビット～ 6 ビットの値です。

Precedence : ToS フィールドの上位 3 ビットの値です。

Bit0 Bit1 Bit2 Bit3 Bit4 Bit5 Bit6 Bit7

Precedence	ToS	-
------------	-----	---

DSCP : ToS フィールドの上位 6 ビットの値です。

Bit0 Bit1 Bit2 Bit3 Bit4 Bit5 Bit6 Bit7

DSCP	-
------	---

注 5

アクセスリストのパラメータである fragments パラメータを指定した場合は、IP ヘッダだけをフロー検出条件として指定できます。

注 6

ack/fin/psh/rst/syn/urg フラグが 1 または 0 のパケットを検出します。また、ack または rst フラグが 1 のパケットも検出できます。

注 7

トラフィッククラスフィールドの指定についての補足を次に示します。

トラフィッククラス：トラフィッククラスフィールドの値です。

1. フィルタ

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
トラフィッククラス							

DSCP : トラフィッククラスフィールドの上位 6 ビットの値です。

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP						-	

注 8

上位 64bit だけ設定できます。

注 9

送信側インタフェースでレイヤ 3 中継パケットの MAC アドレスを指定しても、送信時の MAC アドレスは検出できません。指定した場合、送信時の MAC アドレスではなく受信時の MAC アドレスを検出します。

注 10

送信側インタフェースでは、送信時のカスタム Tag (2 段目の VLAN Tag) を検出できません。指定した場合、送信時のカスタム Tag ではなく受信時のカスタム Tag を検出します。送信側インタフェースでのフロー検出を次の表に示します。

表 1-5 送信側インタフェースでのカスタム Tag の VLAN ID およびユーザ優先度のフロー検出

フレーム中継時の VLAN Tag		送信側インタフェースでのフロー検出	
フレーム受信時	フレーム送信時	カスタム Tag の VLAN ID	カスタム Tag のユーザ優先度
なし	なし	-	-
	1 段	-	-
1 段	なし	-	-
	1 段	-	-
	2 段	0 として検出	0 として検出
2 段	1 段	-	-
	2 段	受信時の 2 段目の VLAN Tag	受信時の 2 段目の VLAN Tag
	3 段	受信時の 2 段目の VLAN Tag	受信時の 2 段目の VLAN Tag
上記以外		受信時の 2 段目の VLAN Tag	受信時の 2 段目の VLAN Tag

(凡例) - : 検出できない

1.1.5 アクセスリスト

フィルタのフロー検出を実施するためにはコンフィグレーションでアクセスリストを設定します。フロー検出条件に応じて設定するアクセスリストが異なります。また、フロー検出条件ごとに検出可能なフレーム種別が異なります。フロー検出条件と対応するアクセスリスト、および検出可能なフレーム種別の関係を次の表に示します。

表 1-6 フロー検出条件と対応するアクセスリスト，検出可能なフレーム種別の関係

設定可能なフロー検出条件	対応するアクセスリスト	検出可能なフレーム種別								
		フローモードなし			MAC モード			フロー検出拡張モード		
		非 IP	IPv4	IPv6	非 IP	IPv4	IPv6	非 IP	IPv4	IPv6
MAC 条件	mac access-list		-	-					-	-
IPv4 条件 1	access-list ip access-list	-		-	- 2	- 2	- 2	-		-
IPv6 条件 1	ipv6 access-list	-	-		- 2	- 2	- 2	-	-	
Advance 条件	advance access-list	- 3	- 3	- 3	- 2	- 2	- 2			

(凡例) : 検出できる - : 検出できない

注 1

layer2-forwarding を指定している場合，本装置宛ての IP パケットは検出できません。

注 2

MAC モードを設定している VLAN インタフェースでは，IPv4 条件，IPv6 条件，および Advance 条件を適用できません。

注 3

フローモードなしの場合，Advance 条件をインタフェースに適用できません。

フィルタエントリの適用順序は，アクセスリストのパラメータであるシーケンス番号によって決定します。

(1) イーサネットインタフェースと VLAN インタフェース同時に設定した場合の動作

イーサネットインタフェースと，該当するイーサネットインタフェースが属している VLAN インタフェースに対してフィルタエントリを設定し，該当するイーサネットインタフェースからの受信フレームに対してフィルタを実施した場合は，イーサネットインタフェース上のフィルタエントリを優先します。

(2) 同一インタフェースに複数のフロー検出条件を同時に設定した場合の動作

同一インタフェースに複数のフロー検出条件を設定して，該当インタフェースの送受信フレームに対してフィルタを実施した場合は，次の順番でフレームを検出します。

1. MAC 条件
2. IPv4 条件
3. IPv6 条件
4. Advance 条件

例えば，MAC 条件でフロー検出したフレームは，Advance 条件ではフロー検出されません。また，統計情報もカウントされません。

(3) フィルタできないフレーム

次に示すフレームは，フィルタの有無にかかわらず，フィルタできません。

- 本装置が自発的に送信するパケット / フレーム ¹
- 本装置がレイヤ 3 中継するフレームのうち次のパケット / フレーム

1. フィルタ

- IPv4 オプション付きの packets ²
- 本装置でフラグメントし送信するフレーム ³
- IPv6 拡張ヘッダ (Hop by Hop) 付きの packets ³
- ARP/NDP の未解決で本装置に一時的に滞留し送信するフレーム ³

注 1

本装置が自発的に送信する packets / フレームは、フロー検出することができません。

注 2

IPv4 オプション付きの packets は、フロー検出することができません。

注 3

送信側インタフェースでは、フロー検出することができません。

1.1.6 暗黙の廃棄

フィルタを設定したインタフェースでは、フロー検出条件に一致しないフレームは廃棄します。

暗黙の廃棄のフィルタエントリは、アクセスリストを生成すると自動生成されます。アクセスリストを一つも設定しない場合は、すべてのフレームを中継します。

Advance 条件とそれ以外の MAC 条件、IPv4 条件、および IPv6 条件を同時に設定した場合、MAC 条件、IPv4 条件、および IPv6 条件のフロー検出対象フレームは、Advance 条件以外のフィルタエントリまたは暗黙の廃棄のフィルタエントリに必ず一致します。このため、フロー検出順番が遅い Advance 条件ではフロー検出されません。

1.1.7 フィルタ使用時の注意事項

(1) 本装置が自発的に送信する packets / フレームに対するフィルタ

本装置が自発的に送信するフレームは、フロー検出できないため廃棄できません。

(2) IPv4 オプション付き packets に対するフィルタ

レイヤ 2 中継する IPv4 オプション付き packets をフロー検出する場合は、フロー検出条件に MAC ヘッダ、IPv4 ヘッダを指定してください。TCP/UDP/ICMP/IGMP ヘッダをフロー検出条件に指定しても、指定したフロー検出条件に従ったフロー検出をしません。

また、レイヤ 3 中継する IPv4 オプション付き packets はフロー検出しません。

(3) 拡張ヘッダのある IPv6 packets に対するフィルタ

拡張ヘッダのある IPv6 packets をフロー検出する場合は、フロー検出条件に MAC ヘッダ、IPv6 ヘッダを指定してください。TCP/UDP/ICMP ヘッダをフロー検出条件に指定しても、フロー検出しません。

(4) IPv4 フラグメント packets に対するフィルタ

IPv4 フラグメント packets の 2 番目以降のフラグメント packets は TCP/UDP/ICMP/IGMP ヘッダが packets 内にありません。フラグメント packets を受信した際のフィルタを次に示します。

表 1-7 IPv4 フラグメントパケットとフィルタの関係

フロー検出条件	フロー検出条件とパケットの一致 / 不一致	動作	先頭パケット	2 番目以降のパケット
IPv4 ヘッダだけ	IPv4 ヘッダ一致	中継	中継	中継
		廃棄	廃棄	廃棄
	IPv4 ヘッダ不一致	中継	次のエントリを検索	次のエントリを検索
		廃棄	次のエントリを検索	次のエントリを検索
IPv4 ヘッダ + TCP/ UDP/ICMP/IGMP ヘッダ	IPv4 ヘッダ一致, TCP/UDP/ICMP/ IGMP ヘッダ一致	中継	中継	-
		廃棄	廃棄	-
	IPv4 ヘッダ一致, TCP/UDP/ICMP/ IGMP ヘッダ不一致	中継	次のエントリを検索	次のエントリを検索
		廃棄	次のエントリを検索	次のエントリを検索
	IPv4 ヘッダ不一致, TCP/UDP/ICMP/ IGMP ヘッダ不一致	中継	次のエントリを検索	次のエントリを検索
		廃棄	次のエントリを検索	次のエントリを検索

(凡例)

- : TCP/UDP/ICMP/IGMP ヘッダがパケットに無いため、常に TCP/UDP/ICMP/IGMP ヘッダ不一致として扱うので該当しない

注

アクセスリストのパラメータである fragments パラメータを指定することで、2 番目以降のフラグメントパケットだけを検出できます。

(5) IPv6 フラグメントパケットに対するフィルタ

IPv6 フラグメントパケットに対しての 2 番目以降のフラグメントパケットは TCP/UDP/ICMP ヘッダがパケット内にありません。IPv6 フラグメントパケットを受信した際のフィルタを次に示します。

表 1-8 IPv6 フラグメントパケットとフィルタの関係

フロー検出条件	フロー検出条件とパケットの一致 / 不一致	動作	先頭パケット	2 番目以降のパケット
IPv6 ヘッダだけ	IPv6 ヘッダ一致	中継	中継	中継
		廃棄	廃棄	廃棄
	IPv6 ヘッダ不一致	中継	次のエントリを検索	次のエントリを検索
		廃棄	次のエントリを検索	次のエントリを検索
IPv6 ヘッダ + TCP/ UDP/ICMP ヘッダ	IPv6 ヘッダ一致, TCP/UDP/ICMP ヘッダ一致	中継	次のエントリを検索	-
		廃棄	次のエントリを検索	-
	IPv6 ヘッダ一致, TCP/UDP/ICMP ヘッダ不一致	中継	次のエントリを検索	次のエントリを検索
		廃棄	次のエントリを検索	次のエントリを検索

1. フィルタ

フロー検出条件	フロー検出条件とパケットの一致 / 不一致	動作	先頭パケット	2 番目以降のパケット
	IPv6 ヘッダ不一致, TCP/UDP/ICMP ヘッダ不一致	中継	次のエントリを検索	次のエントリを検索
		廃棄	次のエントリを検索	次のエントリを検索

(凡例) - : TCP/UDP/ICMP ヘッダがパケットに無いため該当しない

注

アクセスリストのパラメータである ipv6 パラメータを指定した場合だけ、有効なフィルタエントリです。

(6) マルチキャストフレーム・ブロードキャストフレームに対するフィルタ

マルチキャストフレーム・ブロードキャストフレームは、レイヤ 2 中継・レイヤ 3 中継ともに実施されます。マルチキャストフレーム・ブロードキャストフレームをフィルタする場合は、該当するインタフェースに対して、次のどちらかを適用してください。

- レイヤ 2 中継指定のフィルタエントリおよびレイヤ 3 中継指定のフィルタエントリ
- Advance 条件で、レイヤ 2 中継およびレイヤ 3 中継両方指定のフィルタエントリ
この場合、統計情報は 2 回カウントされます。

(7) VLAN Tag 付きフレームに対するフィルタ

本装置では、2 段までの VLAN Tag があるフレームについて、IPv4 ヘッダ・IPv6 ヘッダをフロー検出条件としたフィルタができます。3 段以上の VLAN Tag があるフレームをフィルタする場合は、MAC ヘッダをフロー検出条件としたフィルタエントリを適用してください。

(8) フィルタエントリ適用時の動作

本装置では、インタフェースに対してフィルタを適用すると、暗黙の廃棄エントリから適用します。そのため、ユーザが設定したフィルタエントリが適用されるまでの間、暗黙の廃棄に一致するフレームが一時的に廃棄されます。また、暗黙の廃棄エントリの統計情報が採られます。

注

- 1 エントリ以上を設定したアクセスリストをアクセスグループコマンドによりインタフェースに適用する場合
- アクセスリストをアクセスグループコマンドにより適用し、一つ目のエントリを追加する場合

(9) フィルタエントリ変更時の動作

本装置では、インタフェースに適用済みのフィルタエントリを変更すると、変更が反映されるまでの間、検出の対象となるフレームが検出されなくなります。そのため、一時的にほかのフィルタエントリまたは暗黙の廃棄エントリで検出されます。

(10) VLAN インタフェースの送信側での統計情報

本装置でフラッディングされるパケットまたは宛先 MAC アドレスがマルチキャストアドレスのパケットをレイヤ 2 中継する場合、次に示す三つの条件をすべて満たすと、VLAN インタフェースの送信側に設定したアクセスリストの統計情報が実際の値より 65536 の倍数分少なくなることがあります。この統計情報とは、運用コマンド show access-filter および MIB の統計情報の両方を指します。

なお、フィルタ動作には影響ありません。

- イーサネットインタフェースまたは VLAN インタフェースの受信側に設定したアクセスリストに、レイヤ 2 中継パケットが一致した場合
- VLAN インタフェースの送信側に設定したアクセスリストにレイヤ 2 中継パケットが一致し、一致する前の統計情報が「(65536 の倍数) - 2」の場合
- パケットをレイヤ 2 中継する VLAN インタフェースに、三つ以上のイーサネットインタフェースが所属している場合

(11) DHCP snooping とフィルタの関係

DHCP snooping とフィルタの関係について次に示します。

- DHCP snooping が有効な場合、プロトコル名称 bootps および bootpc の両方のレイヤ 3 中継パケットはインタフェースの受信側でフロー検出できません。
- 端末フィルタが有効なポートで受信した IPv4 パケットはインタフェースの受信側でフロー検出できません。端末フィルタの動作に従います。

1.2 コンフィグレーション

1.2.1 コンフィグレーションコマンド一覧

フィルタで使用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 1-9 コンフィグレーションコマンド一覧

コマンド名	説明
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または VLAN インタフェースに対して Advance 条件による 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 条件でフロー検出を行い、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。
advance access-list resequence	Advance フィルタのフィルタ条件適用順序のシーケンス番号を再設定します。
deny	フィルタでのアクセスを廃棄する条件を指定します。
ip access-group	イーサネットインタフェースまたは VLAN 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。
ip access-list resequence	IPv4 アドレスフィルタおよび IPv4 パケットフィルタのフィルタ条件適用順序のシーケンス番号を再設定します。
ip access-list standard	IPv4 アドレス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 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 resequence	IPv6 フィルタのフィルタ条件適用順序のシーケンス番号を再設定します。
ipv6 traffic-filter	イーサネットインタフェースまたは VLAN 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または VLAN 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。
mac access-list resequence	MAC フィルタのフィルタ条件適用順序のシーケンス番号を再設定します。
permit	フィルタでのアクセスを中継する条件を指定します。
remark	フィルタの補足説明を指定します。
fdm prefer ¹	フィルタ・QoS 制御のフローモード、フロー検出拡張モードを設定します。
flow mac mode ²	フィルタ・QoS 制御のフローモード、MAC モードを設定します。

注 1

「コンフィグレーションコマンドレファレンス Vol.1 9. 装置の管理」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 2. フローモード」を参照してください。

1.2.2 フローモードの設定

(1) MAC モードの設定

フィルタの MAC モードを指定する例を次に示します。

[設定のポイント]

MAC モードは、装置の基本的な動作条件を決定するため、最初に設定します。

[コマンドによる設定]

1. (config)# interface vlan 10
VLAN10 のインタフェースモードに移行します。
2. (config-if)# flow mac mode
flow mac mode を有効にします。

[注意事項]

イーサネットインタフェースにフィルタ・QoS フロー検出を設定した場合は、該当するイーサネットインタフェースが属するすべての VLAN インタフェースに対して MAC モードを設定できません。MAC モードを設定した VLAN 配下のイーサネットインタフェースに対してフィルタ・QoS フロー検出を設定できません。MAC モードを設定しない場合は、イーサネットインタフェース・VLAN インタフェース共に、フィルタ・QoS フロー検出を設定できます。

(2) フロー検出拡張モードの設定

フィルタのフロー検出拡張モードを指定する例を次に示します。

[設定のポイント]

フロー検出拡張モードは、装置の基本的な動作条件を決定するため、最初に設定します。

[コマンドによる設定]

1. (config)# fldm prefer default standard-advance
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、フロー系テーブル容量を standard-advance に設定します。コンフィグレーションの変更を確認して 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。

[注意事項]

すべての VLAN に MAC モードが設定されていない場合は、フロー検出拡張モードに変更できます。また、すべてのインタフェースに Advance 条件のアクセスリストおよび QoS フローリストが設定されていない場合は、フロー検出拡張モード設定なしに変更できます。

1.2.3 MAC ヘッダで中継・廃棄をする設定

MAC ヘッダをフロー検出条件として、フレームを中継・廃棄指定する例を次に示します。

[設定のポイント]

フレーム受信時に MAC ヘッダによってフロー検出を行い、フィルタエントリに一致したフレームを廃棄・中継します。

[コマンドによる設定]

1. フィルタ

1. `(config)# mac access-list extended IPX_DENY`
mac access-list (IPX_DENY) を作成します。本リストを作成することによって、MAC フィルタの動作モードに移行します。
2. `(config-ext-macl)# deny any any ipx`
イーサネットタイプが IPX のフレームを廃棄する MAC フィルタを設定します。
3. `(config-ext-macl)# permit any any`
すべてのフレームを中継する MAC フィルタを設定します。
4. `(config-ext-macl)# exit`
MAC 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。
5. `(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。
6. `(config-if)# mac access-group IPX_DENY in layer2-forwarding`
受信側にレイヤ 2 中継を対象とする MAC フィルタを有効にします。

1.2.4 IP ヘッダ・TCP/UDP ヘッダで中継・廃棄をする設定

(1) IPv4 アドレスをフロー検出条件とする設定

IPv4 アドレスをフロー検出条件とし、フレームを中継・廃棄指定する例を次に示します。

[設定のポイント]

フレーム受信時に送信元 IPv4 アドレスによってフロー検出を行い、フィルタエントリに一致したフレームを中継します。フィルタエントリに一致しない IP パケットはすべて廃棄します。

[コマンドによる設定]

1. `(config)# ip access-list standard FLOOR_A_PERMIT`
ip access-list (FLOOR_A_PERMIT) を作成します。本リストを作成することによって、IPv4 アドレスフィルタの動作モードに移行します。
2. `(config-std-nacl)# permit 192.168.0.0 0.0.0.255`
送信元 IP アドレス 192.168.0.0/24 ネットワークからのフレームを中継する IPv4 アドレスフィルタを設定します。
3. `(config-std-nacl)# exit`
IPv4 アドレス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。
4. `(config)# interface vlan 10`
VLAN10 のインタフェースモードに移行します。
5. `(config-if)# ip access-group FLOOR_A_PERMIT in layer3-forwarding`
受信側にレイヤ 3 中継を対象とする IPv4 フィルタを有効にします。

(2) IPv4 パケットをフロー検出条件とする設定

IPv4 telnet パケットをフロー検出条件とし、フレームを中継・廃棄指定する例を次に示します。

[設定のポイント]

フレーム受信時に IP ヘッダ・TCP/UDP ヘッダによってフロー検出を行い、フィルタエントリに一致したフレームを廃棄します。

[コマンドによる設定]

1. **(config)# ip access-list extended TELNET_DENY**
ip access-list (TELNET_DENY) を作成します。本リストを作成することによって、IPv4 パケットフィルタの動作モードに移行します。
2. **(config-ext-nacl)# deny tcp any any eq telnet**
telnet のパケットを廃棄する IPv4 パケットフィルタを設定します。
3. **(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。
4. **(config-ext-nacl)# exit**
IPv4 アドレス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。
5. **(config)# interface vlan 10**
VLAN10 のインタフェースモードに移行します。
6. **(config-if)# ip access-group TELNET_DENY in layer2-forwarding**
受信側にレイヤ 2 中継を対象とする IPv4 フィルタを有効にします。

(3) IPv6 パケットをフロー検出条件とする設定

IPv6 パケットをフロー検出条件として、フレームを中継・廃棄指定する例を次に示します。

[設定のポイント]

フレーム受信時に IP アドレスによってフロー検出を行い、フィルタエントリに一致したフレームを中継します。フィルタエントリに一致しない IP パケットはすべて廃棄します。

[コマンドによる設定]

1. **(config)# ipv6 access-list FLOOR_B_PERMIT**
ipv6 access-list (FLOOR_B_PERMIT) を作成します。本リストを作成することによって、IPv6 パケットフィルタの動作モードに移行します。
2. **(config-ipv6-acl)# permit ipv6 2001:100::1/64 any**
送信元 IP アドレス 2001:100::1/64 からのフレームを中継する IPv6 パケットフィルタを設定します。
3. **(config-ipv6-acl)# exit**
IPv6 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。
4. **(config)# interface gigabitethernet 1/1**

1. フィルタ

ポート 1/1 のインタフェースモードに移行します。

5. (config-if)# ipv6 traffic-filter FLOOR_B_PERMIT in layer2-forwarding
受信側にレイヤ 2 中継を対象とする IPv6 フィルタを有効にします。

1.2.5 MAC ヘッダ・IP ヘッダ・TCP/UDP ヘッダで中継・廃棄をする設定

(1) MAC ヘッダ・IPv4 ヘッダ・TCP ヘッダをフロー検出条件とする設定

MAC ヘッダ・IPv4 ヘッダ・TCP ヘッダをフロー検出条件として、フレームを中継・廃棄指定する例を次に示します。

[設定のポイント]

フレーム受信時に送信元 MAC アドレス・送信元 IPv4 アドレス・TCP ヘッダによってフロー検出を行い、フィルタエントリに一致したフレームを中継します。フィルタエントリに一致しないすべてのフレームを廃棄します。

[コマンドによる設定]

1. (config)# advance access-list ADVANCE_ACL_A_PERMIT
advance access-list (ADVANCE_ACL_A_PERMIT) を作成します。本リストを作成することによって、Advance フィルタの動作モードに移行します。
2. (config-adv-acl)# permit mac-ip host 0012.e200.0001 any tcp 192.168.0.0
0.0.0.255 any eq telnet
送信元 MAC アドレス 0012.e200.0001, 送信元 IP アドレス 192.168.0.0/24 で telnet のパケットを中継する Advance フィルタを設定します。
3. (config-adv-acl)# exit
Advance 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。
4. (config)# interface vlan 10
VLAN10 のインタフェースモードに移行します。
5. (config-if)# advance access-group ADVANCE_ACL_A_PERMIT in
layer2-and-layer3-forwarding
受信側にレイヤ 2 中継およびレイヤ 3 中継を対象とする Advance フィルタを有効にします。

(2) MAC ヘッダ・IPv6 ヘッダ・UDP ヘッダをフロー検出条件とする設定

MAC ヘッダ・IPv6 ヘッダ・UDP ヘッダをフロー検出条件として、フレームを中継・廃棄指定する例を次に示します。

[設定のポイント]

フレーム受信時に送信元 MAC アドレス・送信元 IPv6 アドレス・UDP ヘッダによってフロー検出を行い、フィルタエントリに一致したフレームを中継します。フィルタエントリに一致しないすべてのフレームを廃棄します。

[コマンドによる設定]

1. (config)# **advance access-list ADVANCE_ACL_B_PERMIT**
advance access-list (ADVANCE_ACL_B_PERMIT) を作成します。本リストを作成することによって、Advance フィルタの動作モードに移行します。
2. (config-adv-acl)# **permit mac-ipv6 host 0012.e200.0001 any udp 2001:100::1/64 any eq ntp**
送信元 MAC アドレス 0012.e200.0001、送信元 IP アドレス 2001:100::1/64 の ntp パケットを中継する Advance フィルタを設定します。
3. (config-adv-acl)# **exit**
Advance 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。
4. (config)# **interface vlan 10**
VLAN10 のインタフェースモードに移行します。
5. (config-if)# **advance access-group ADVANCE_ACL_B_PERMIT in layer2-and-layer3-forwarding**
受信側にレイヤ 2 中継およびレイヤ 3 中継を対象とする Advance フィルタを有効にします。

1.2.6 複数インタフェースフィルタの設定

複数のイーサネットインタフェースにフィルタを指定する例を次に示します。

[設定のポイント]

config-if-range モードで複数のイーサネットインタフェースにフィルタを設定できます。

[コマンドによる設定]

1. (config)# **access-list 10 permit host 192.168.0.1**
ホスト 192.168.0.1 からだけフレームを中継する IPv4 アドレスフィルタを設定します。
2. (config)# **interface range gigabitethernet 1/1-4**
ポート 1/1-4 のインタフェースモードに移行します。
3. (config-if-range)# **ip access-group 10 in layer2-forwarding**
受信側にレイヤ 2 中継を対象とする IPv4 フィルタを有効にします。

1.3 オペレーション

show access-filter コマンドによって、設定した内容が反映されているかどうかを確認します。

1.3.1 運用コマンド一覧

フィルタで使用する運用コマンド一覧を次の表に示します。

表 1-10 運用コマンド一覧

コマンド名	説明
show access-filter	アクセスグループコマンド (mac access-group , ip access-group , ipv6 traffic-filter , advance access-group) で設定したアクセスリスト (mac access-list , access-list , ip access-list , ipv6 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 (mac access-group , ip access-group , ipv6 traffic-filter , advance access-group) で設定したアクセスリスト (mac access-list , access-list , ip access-list , ipv6 access-list , advance access-list) の統計情報をクリアします。

1.3.2 フィルタの確認

(1) イーサネットインタフェースに設定されたエントリの確認

イーサネットインタフェースにフィルタを設定した場合の動作確認の方法を次の図に示します。

図 1-3 イーサネットインタフェースにフィルタを設定した場合の動作確認

```
> show access-filter 1/1 IPX_DENY in
Date 2006/03/01 12:00:00 UTC
Using Port:1/1 in
Extended MAC access-list: IPX_DENY layer2-forwarding
remark "deny only ipx"
deny any any ipx
  matched packets      :          74699826
permit any any
  matched packets      :          264176
implicitly denied packets:          0
```

指定したポートのフィルタに「Extended MAC access-list」が表示されることを確認します。フロー検出条件に一致したフレームは matched packets で確認します。また、暗黙の廃棄に一致したフレームは implicitly denied packets で確認します。

(2) VLAN インタフェースに設定されたエントリの確認

VLAN インタフェースにフィルタを設定した場合の動作確認の方法を次の図に示します。

図 1-4 VLAN インタフェースにフィルタを設定した場合の動作確認

```
> show access-filter interface vlan 10 FLOOR_A_PERMIT in
Date 2006/03/01 12:00:00 UTC
Using Interface:vlan 10 in
Standard IP access-list: FLOOR_A_PERMIT layer3-forwarding
remark "permit only Floor-A"
permit 192.168.0.0 0.0.0.255 any
  matched packets      :          74699826
implicitly denied packets:          2698
```

指定した VLAN のフィルタに「Standard IP access-list」が表示されることを確認します。フロー検出条

件に一致したフレームは `matched packets` で確認します。また、暗黙の廃棄に一致したフレームは `implicit denied packets` で確認します。

2

アクセスリストロギング

この章では、アクセスリストロギングの解説と操作方法について説明します。

2.1 解説

2.2 コンフィグレーション

2.3 オペレーション

2.1 解説

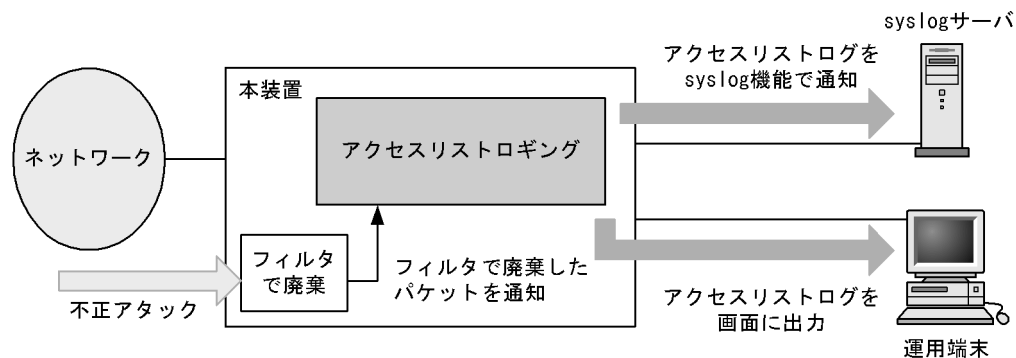
2.1.1 アクセスリストロギングの概要

アクセスリストロギングとは、フィルタで廃棄したパケットの情報とその統計情報を運用ログとして収集し、運用端末に出力したり、syslog サーバに通知したりする機能です。これによって、不正アクセスや不正パケットを監視したり、フィルタの設定誤りによる意図しないパケットの廃棄を確認したりできます。

アクセスリストロギングが通知するログをアクセスリストログと呼びます。また、フィルタで廃棄したパケットの情報とその統計情報をアクセスリストログ情報と呼びます。アクセスリストログでは、パケットの内容ごとに、廃棄したパケット数がカウントされます。

アクセスリストロギングの動作概要を次の図に示します。

図 2-1 アクセスリストロギングの動作概要



出力するアクセスリストログの例を次の図に示します。

図 2-2 出力するアクセスリストログの例

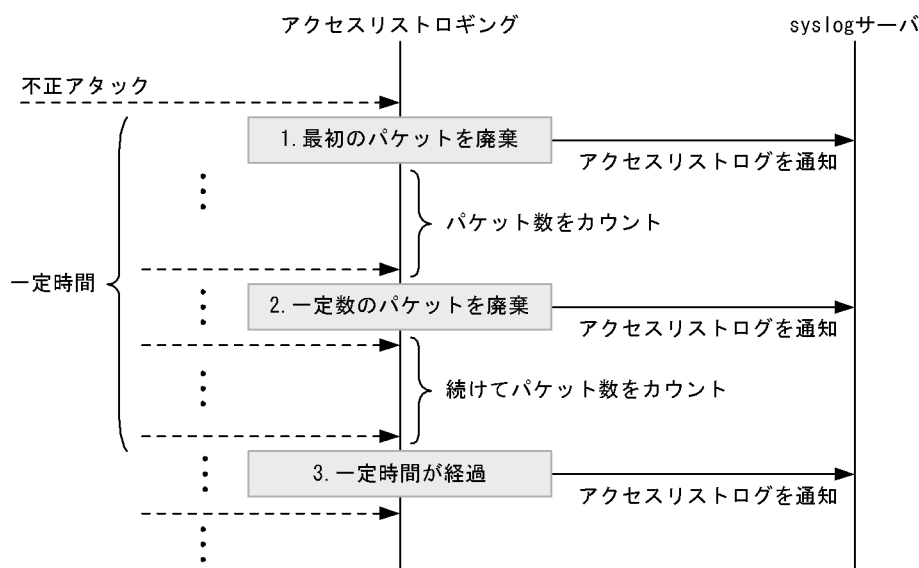
```
>
ACL 12/14 12:00:00 denied:IN:0012.e25a.9839(vlan10 Ethernet1/1) ->
0012.e25a.7840, 2 packets
ACL 12/14 12:00:00 denied:IN:0012.e25a.983a(vlan10 Ethernet1/1) ->
0012.e25a.7840, 1 packet
ACL 12/14 12:00:00 denied:IN:tcp 192.168.1.3(1024, vlan10 Ethernet1/1) ->
192.168.2.1(22), 5 packets
ACL 12/14 12:00:00 denied:OUT:tcp 2001:db8::1(1024, vlan10 Ethernet1/1) ->
2001:db8::2(22, vlan11 Ethernet3/1), 2 packets
>
```

アクセスリストログを通知する契機は次のとおりです。

- フィルタで最初のパケットを廃棄したとき
- パケットを廃棄してから一定時間が経過したとき
- 廃棄したパケット数が一定数に達したとき

フィルタでパケットを廃棄してからアクセスリストログを syslog サーバへ通知するまでの流れを次の図に示します。

図 2-3 アクセスリストログ通知の流れ



1. フィルタで最初のパケットを廃棄したときに通知します。
2. 同じ内容のパケットを一定数廃棄したときに通知します。
この機能をスレッシュホールド機能と呼びます。
3. 最初のパケットを廃棄してから、一定時間が経過したときに通知します。
この機能をログ出力インターバル機能と呼びます。

なお、一定時間が経過すると、通知したアクセスリストログ情報はクリアされます。

2.1.2 アクセスリストログの表示内容

アクセスリストロギングでは、フィルタで廃棄したパケット内のレイヤ 2、レイヤ 3 およびレイヤ 4 ヘッダを解析して、アクセスリストログに表示します。アクセスリストログの表示内容を次の表に示します。なお、アクセスリストログのフォーマットについては、マニュアル「メッセージ・ログレファレンス」を参照してください。

表 2-1 アクセスリストログの表示内容

分類	表示項目	内容
パケット内の情報	<source mac>	送信元 MAC アドレス
	<destination mac>	宛先 MAC アドレス
	<ethernet type>	イーサネットタイプ
	<protocol no.>	上位プロトコル番号
	<next header>	次ヘッダ番号
	<source ip address>	送信元 IPv4/IPv6 アドレス
	<destination ip address>	宛先 IPv4/IPv6 アドレス
	<source port>	送信元ポート番号 ¹
	<destination port>	宛先ポート番号 ¹
付与情報	<Time>	ログ出力時刻 ²
	<denied filter point>	フィルタで廃棄したポイント ³

2. アクセスリストロギング

分類	表示項目	内容
	<received interface>	表示パケットの受信インタフェース ⁴
	<send interface>	表示パケットの送信インタフェース ⁴
	<packets>	出力したログのうち、次の内容が同じフローのパケット数 <ul style="list-style-type: none"> • パケット内の情報 • フィルタで廃棄したポイント • 送受信インタフェース

注 1

上位プロトコルが TCP と UDP の場合だけ表示します。

注 2

運用コマンド show access-log flow では表示しません。

注 3

受信側インタフェース (IN), または送信側インタフェース (OUT) のどちらで廃棄したかを表示します。

注 4

送受信インタフェースには VLAN ID (vlan<vlan id>) およびイーサネットインタフェース (Ethernet<nif no.>/<port no.>) を表示します。なお、フィルタで廃棄したパケットの中継種別および <denied filter point> によって、表示内容が異なります。送受信インタフェースの表示内容を次の表に示します。

表 2-2 送受信インタフェースの表示内容

フィルタで廃棄したパケットの中継種別	<denied filter point>	表示項目	
		<received interface>の表示内容	<send interface>の表示内容
レイヤ 2 中継	IN	vlan<vlan id> と Ethernet<nif no.>/<port no.>	-
	OUT		vlan<vlan id> と Ethernet<nif no.>/<port no.>
レイヤ 3 中継	IN		-
	OUT		vlan<vlan id>
本装置宛	IN	-	
	OUT	-	

(凡例) - : 表示しない

フィルタで廃棄したパケット種別によって、表示するアクセスリストログの内容が異なります。アクセスリストログで表示する内容を、パケット種別ごとに次に示します。

表 2-3 アクセスリストログの表示内容 (非 IP パケット)

表示項目	VLAN Tag なし, または VLAN Tag1 段	VLAN Tag2 段以上
<source mac>		
<destination mac>		
<ethernet type>		-
<protocol no.>	-	-
<next header>	-	-
<source ip address>	-	-

表示項目	VLAN Tag なし, または VLAN Tag1 段	VLAN Tag2 段以上
<destination ip address>	-	-
<source port>	-	-
<destination port>	-	-
<denied filter point>		
<received interface>		
<send interface>		
<packets>		

(凡例) : 表示する - : 表示しない

表 2-4 アクセスリストログの表示内容 (IPv4 パケット)

表示項目	VLAN Tag なし, または VLAN Tag1 段					VLAN Tag2 段 以上
	IP オプションなし				IP オプ ション付 き	
	IP フラグメント以外		IP フラグメント			
	レイヤ 4 が TCP, UDP	レイヤ 4 な し, または レイヤ 4 が TCP, UDP 以外	レイヤ 4 が TCP, UDP	レイヤ 4 な し, または レイヤ 4 が TCP, UDP 以外		
<source mac>	-	-	-	-	-	
<destination mac>	-	-	-	-	-	
<ethernet type>	-	-	-	-	-	-
<protocol no.>						-
<next header>	-	-	-	-	-	-
<source ip address>						-
<destination ip address>						-
<source port>		-		-	-	-
<destination port>		-		-	-	-
<denied filter point>						
<received interface>						
<send interface>						
<packets>						

(凡例) : 表示する - : 表示しない

注

本装置で IP フラグメントする場合は, フラグメントする前のパケットの内容でアクセスリストログを表示します。

注

本装置で IP フラグメントする場合だけ表示します。本装置でフラグメントしない場合は表示しません。

表 2-5 アクセスリストログの表示内容 (IPv6 パケット)

表示項目	VLAN Tag なし, または VLAN Tag1 段			VLAN Tag 2 段以上
	IPv6 拡張ヘッダなし		IPv6 拡張ヘッダあり	
	レイヤ 4 が TCP, UDP	レイヤ 4 なし, または レイヤ 4 が TCP, UDP 以外		
<source mac>	-	-	-	
<destination mac>	-	-	-	
<ethernet type>	-	-	-	-
<protocol no.>	-	-	-	-
<next header>				-
<source ip address>				-
<destination ip address>				-
<source port>		-	-	-
<destination port>		-	-	-
<denied filter point>				
<received interface>				
<send interface>				
<packets>				

(凡例) : 表示する - : 表示しない

2.1.3 ログ出力インターバル機能

指定した時間間隔 (インターバル値) でアクセスリストログを出力する機能です。フィルタで最初のパケットを廃棄してアクセスリストログを出力してから, 時間を計り始めます。フィルタで廃棄してから指定した時間が経過するまでの間は, 複数のパケットをフィルタで廃棄しても, アクセスリストログを出力しません。指定した時間が経過すると, その間にフィルタで廃棄したパケット数も合わせてアクセスリストログを出力します。本機能を使用すると, 一定時間間隔で監視ができます。

なお, アクセスリストロギングの動作中に, 出力する時間間隔を変更した場合は, いったんアクセスリストログ情報をすべて削除して, 再度ログ出力インターバル機能による監視を開始します。

2.1.4 スレッシュホールド機能

フィルタで廃棄したパケット数の合計が, 指定したスレッシュホールド値 (パケット数) の N 倍に一致したときに, アクセスリストログを出力する機能です。本機能を使用すると, フィルタで廃棄したパケット数による監視ができます。

2.1.5 ソフトウェアパケット制御機能

フィルタで廃棄したパケットのうち, CPU へ転送するパケットの数を制限する機能です。本機能によって, 装置が高負荷になることを抑止します。CPU に転送するパケット数を次に示します。

(1) AX6700S の場合

フィルタで廃棄したパケットを BCU 内の CPU に転送する際, ソフトウェアパケット制御機能で設定した

パケット数に従って転送数を制御します。

CPU に転送するパケット数は、運用系 BSU の枚数によって異なります。運用系 BSU 枚数別の、CPU に転送するパケットの最大数を次の表に示します。

表 2-6 CPU に転送するパケットの最大数

運用系 BSU 枚数	CPU に転送するパケットの最大数
1 枚	設定値の約 2 倍
2 枚	設定値の約 4 倍
3 枚	設定値の約 6 倍

(2) AX6600S の場合

フィルタで廃棄したパケットを CSU 内の CPU に転送する際、ソフトウェアパケット制御機能で設定したパケット数に従って転送数を制御します。

CPU に転送するパケット数は、運用系 PSP の数によって異なります。運用系 PSP 数別の、CPU に転送するパケットの最大数を次の表に示します。

表 2-7 CPU に転送するパケットの最大数

運用系 PSP 数	CPU に転送するパケットの最大数
1	設定値
2	設定値の約 2 倍

(3) AX6300S の場合

フィルタで廃棄したパケットを MSU 内の CPU に転送する際、ソフトウェアパケット制御機能で設定したパケット数に従って転送数を制御します。

CPU に転送するパケットの最大数は、運用系 MSU が 1 枚だけなので、設定値と同じになります。

2.1.6 ログ出力の開始と停止について

syslog、運用ログ、および画面へのログ出力の開始と停止を指定できます。なお、アクセスリストロギングの動作開始時には、syslog および運用ログへのログ出力を開始しますが、画面へのログ出力は停止しています。

2.1.7 アクセスリストロギングの注意事項

- 暗黙の廃棄で検出したパケットはアクセスリストロギングの対象としません。
- アクセスリストロギングの収容数を超えた場合は、アクセスリストログ情報を新たに登録しません。このため、アクセスリストログを出力しません。
- アクセスリストロギングを使用した場合、マルチキャストのランデブーポイントで受信できる PIM-Register パケット数の上限値には、次の値が適用されます。
 - IPv4 の場合、コンフィグレーションコマンド `ip pim rate-limit register-receive` の指定値に関係なく、`ip pim rate-limit register-request` コマンドで設定した値
 - IPv6 の場合、コンフィグレーションコマンド `ipv6 pim rate-limit register-receive` の指定値に関係なく、`ipv6 pim rate-limit register-request` コマンドで設定した値

2. アクセスリストロギング

- アクセスリストロギングを使用している場合、次の MIB ではアクセスリストロギングの対象となったパケットはカウントされません。
 - ipInDiscards
 - ipOutDiscards
 - ipv6IfStatsInDiscards
 - ipv6IfStatsOutDiscards
- sFlow 統計を有効にしているポートに対してアクセスリストロギングを有効にした場合、アクセスリストロギングの対象となった廃棄パケットは VLAN 統計の廃棄パケット数にカウントされません。
- 系切替後およびアクセスリストロギングプログラムの再起動後、syslog および運用ログへのログ出力を開始します。このとき、画面へのログ出力は停止します。

2.2 コンフィグレーション

2.2.1 コンフィグレーションコマンド一覧

アクセスリストロギ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 2-8 コンフィグレーションコマンド一覧

コマンド名	説明
access-log enable	アクセスリストロギングを有効にします。
access-log interval	ログ出力インターバル機能のインターバル値を指定します。
access-log rate-limit	ソフトウェアパケット制御機能の CPU へ転送するパケット数を指定します。
access-log threshold	スレッシュホールド機能のスレッシュホールド値を指定します。
system hardware-mode	装置のハードウェアモードを設定します。

注

「コンフィグレーションコマンドレファレンス Vol.1 9. 装置の管理」を参照してください。

2.2.2 ハードウェアモードの設定

アクセスリストロギング対応ハードウェアモードに変更します。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。

[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。

2.2.3 アクセスリストロギングの設定

アクセスリストロギングを設定する例を次に示します。

[設定のポイント]

指定したアクセスリストで廃棄したパケットを、アクセスリストロギングの対象とします。

[コマンドによる設定]

1. `(config)# ip access-list extended ACLLOG_DENY`
`ip access-list (ACLLOG_DENY)` を作成します。本リストを作成することによって、IPv4 パケットフィルタの動作モードに移行します。
2. `(config-ext-nacl)# 10 deny ip any any action log`
IPv4 パケットをアクセスリストロギングの対象に設定します。
3. `(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。

2. アクセスリストロギング

4. `(config)# interface vlan 10`
VLAN10 のインタフェースモードに移行します。
5. `(config-if)# ip access-group ACLLOG_DENY in layer3-forwarding`
受信側にレイヤ 3 中継を対象とする IPv4 フィルタを有効にします。
6. `(config-if)# exit`
インタフェース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)# access-log enable`
アクセスリストロギングの動作を開始します。

2.2.4 syslog サーバへアクセスリストログを通知する設定

アクセスリストログを syslog サーバへ通知する設定例を次に示します。

[設定のポイント]

syslog サーバに送信する対象にアクセスリストログを追加します。これによって、アクセスリストロギングの対象フィルタで廃棄されたパケット情報が syslog サーバへ送信されます。

[コマンドによる設定]

1. `(config)# logging event kind acl`
syslog サーバに送信する対象としてアクセスリストログを設定します。
2. `(config)# ip access-list extended ACLLOG_DENY`
ip access-list (ACLLOG_DENY) を作成します。本リストを作成することによって、IPv4 パケットフィルタの動作モードに移行します。
3. `(config-ext-nacl)# 10 deny ip any any action log`
IPv4 パケットをアクセスリストロギングの対象に設定します。
4. `(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。
5. `(config)# interface vlan 10`
VLAN10 のインタフェースモードに移行します。
6. `(config-if)# ip access-group ACLLOG_DENY in layer3-forwarding`
受信側にレイヤ 3 中継を対象とする IPv4 フィルタを有効にします。
7. `(config-if)# exit`
インタフェース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。
8. `(config)# access-log threshold 100`
スレッシュホールド機能のスレッシュホールド値に 100 を設定します。
9. `(config)# access-log rate-limit 50`

ソフトウェアパケット制御機能のパケット数に 50 を設定します。

10. `(config)# access-log enable`

アクセスリストロギングの動作を開始します。

2.2.5 アクセスリストログ情報を長期間保持する設定

アクセスリストログ情報を長期間保持する設定例を次に示します。

[設定のポイント]

インターバル値 (ログ出力インターバル機能) を契機としたログの出力をしないように設定します。
ログの出力状態は、運用コマンド `show access-log` で確認してください。

[コマンドによる設定]

1. `(config)# ipv6 access-list ACLLOG_DENY`

ipv6 access-list (ACLLOG_DENY) を作成します。本リストを作成することによって、IPv6 パケットフィルタの動作モードに移行します。

2. `(config-ipv6-acl)# 10 deny ipv6 any any action log`

IPv6 パケットをアクセスリストロギングの対象に設定します。

3. `(config-ipv6-acl)# exit`

IPv6 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。

4. `(config)# interface vlan 10`

VLAN10 のインタフェースモードに移行します。

5. `(config-if)# ipv6 traffic-filter ACLLOG_DENY in layer3-forwarding`

受信側にレイヤ 3 中継を対象とする IPv6 フィルタを有効にします。

6. `(config-if)# exit`

インタフェース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)# access-log interval unlimit`

インターバル値を契機としたログの出力をしないように設定します。

8. `(config)# access-log enable`

アクセスリストロギングの動作を開始します。

2.3 オペレーション

2.3.1 運用コマンド一覧

アクセスリストロギングの運用コマンド一覧を次の表に示します。

表 2-9 運用コマンド一覧

コマンド名	説明
show access-log	アクセスリストロギングの情報を表示します。
clear access-log	アクセスリストロギングで取得した、フィルタで廃棄したパケットの統計情報をクリアします。
show access-log flow	アクセスリストログ情報を表示します。
clear access-log flow	アクセスリストログ情報をクリアします。
dump access-log	アクセスリストロギング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。
restart access-log	アクセスリストロギングを再起動します。
debug access-log	アクセスリストログの出力を開始します。
no debug access-log	アクセスリストログの出力を停止します。

2.3.2 アクセスリストロギング情報の確認

アクセスリストロギングの情報を確認するには、show access-log コマンドを実行してください。アクセスリストログの出力状態やアクセスリストログ情報数などが確認できます。

図 2-4 アクセスリストロギング情報の確認

```
> show access-log
Date 2009/12/14 12:00:00 UTC
Access list logging Information:
  rate-limit(pps)      :          100
  interval(minutes)   :           5
  threshold(packets)  :           -
  logging              :          enable    ...1
  display              :          disable   ...1
Access list logging Logged:
  Max                  :          2000     ...2
  Used                 :          1001     ...2
  NonIP                :           950
  IPv4                 :           0
  IPv6                 :           51
Access list logging Statistics:
  flow table full     :          17295
  rate-limit discard :          51615
>
```

1. アクセスリストログの出力が設定したとおりになっているか確認します。
2. アクセスリストログ情報数が最大収容数を超えていないか確認します。

2.3.3 アクセスリストログ情報の確認

アクセスリストロギングで保持しているアクセスリストログ情報を確認するには、show access-log flow コマンドを実行してください。廃棄したパケットの情報と廃棄したパケット数を確認できます。

図 2-5 アクセスリストログ情報の確認

```
> show access-log flow
Date 2009/12/14 12:00:00 UTC
ACL:denied:IN:0012.e25a.9839(vlan10 Ethernet1/1) -> 0012.e25a.7840, 2 packets
ACL:denied:IN:0012.e25a.983a(vlan10 Ethernet1/1) -> 0012.e25a.7840, 1 packet
ACL:denied:IN:tcp 192.168.1.3(1024, vlan10 Ethernet1/1) -> 192.168.2.1(22), 5
packets
ACL:denied:OUT:tcp 2001:db8::1(1024, vlan10 Ethernet1/1) -> 2001:db8::2(22,
vlan11 Ethernet3/1), 2 packets
>
```

2.3.4 ログ出力の開始と停止

(1) 画面へのログ出力開始

アクセスリストログを運用端末画面に出力する例を次の図に示します。ログ出力の開始を示すログが表示されます。

図 2-6 アクセスリストロギングの画面へのログ出力開始

```
>debug access-log display
monitor: start access list logging event-log monitor
>
```

(2) ログ出力停止

アクセスリストログ出力を停止する例を次の図に示します。ログ出力の停止を示すログが表示されます。

図 2-7 アクセスリストロギングのログ出力停止

```
>no debug access-log
monitor: stop access list logging event-log monitor
>
```


3

uRPF

uRPF はフィルタ機能の一種で、正しい相手からパケットが送信されたかだけを確認するため設定が容易です。この章では、uRPF 機能の解説と操作方法について説明します。

3.1 解説

3.2 コンフィグレーション

3.3 オペレーション

3.1 解説

uRPF (Unicast Reverse Path Forwarding) はフィルタ機能の一種です。通常のフィルタ機能が遮断したいトラフィックの種別をリスト形式で記述しなければならないのに対して、uRPF ではフィルタを実施したいインタフェースを指定するだけなので、設定が簡易であるという特徴があります。

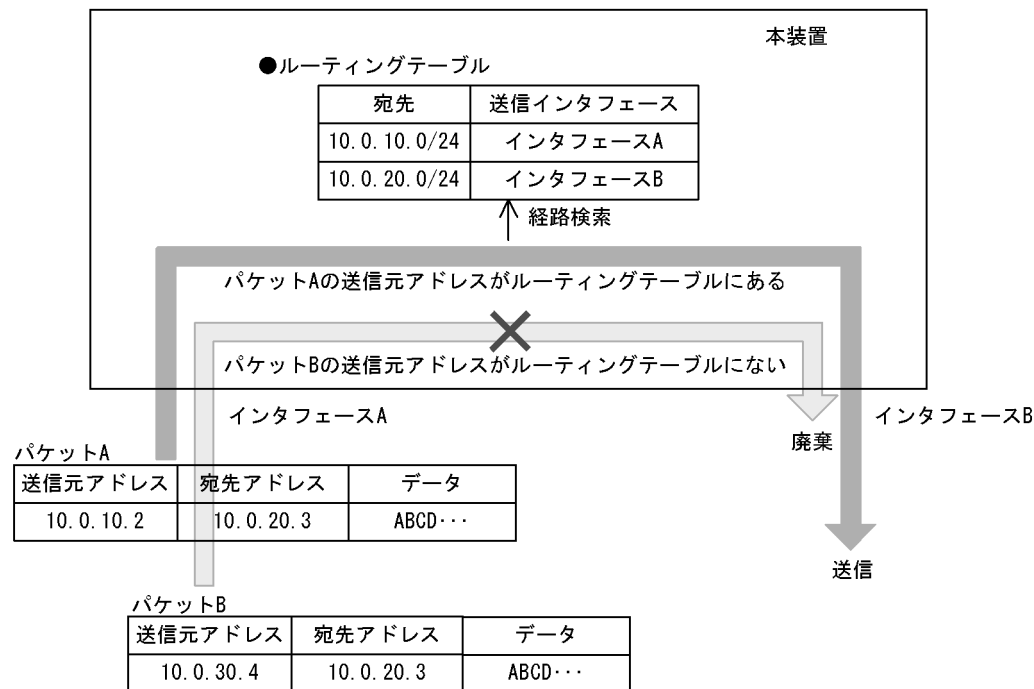
受信パケットの廃棄判定は、パケットの送信元アドレスが妥当かどうかを検証することで行われ、主に DoS 攻撃でよく見られる成りすましパケットの防御手段となります。

uRPF の廃棄対象となるアドレスは IPv4 アドレスおよび IPv6 アドレスです。

3.1.1 uRPF の概要

uRPF は、受信パケットの送信元アドレスを装置のルーティングテーブルから検索し、ルーティングテーブルになければパケットを廃棄します。uRPF の動作概要を次の図に示します。

図 3-1 uRPF の動作概要



上記の図では、パケット A 受信時に uRPF 機能が有効であれば、本装置はパケット A の送信元アドレス 10.0.10.2 をルーティングテーブルから検索します。ルーティングテーブルに 10.0.10.2 に一致する経路が存在するため、本装置はパケット A を正当なパケットと見なし、通常の経路検索による中継を行います。次項で説明している Strict モードではさらにインタフェースの妥当性も検証します。

パケット B 受信時は、パケット B の送信元アドレス 10.0.30.4 をルーティングテーブルから検索しますが、マッチする経路が存在しないため、パケット B は廃棄されます。

3.1.2 サポートモード

本装置の uRPF 機能でサポートしているモードを次に示します。本装置では、インタフェース単位にモードを指定でき、さらに IPv4 / IPv6 プロトコルごとに有効・無効を指定することもできます。

1. Strict モード

受信パケットの送信元アドレスがルーティングテーブルに存在し、かつ該当する経路で指定されている送信インタフェースが受信インタフェースと一致した場合だけ、パケットを受信可能とします。

2. Loose モード

受信パケットの送信元アドレスがルーティングテーブルに存在するかどうかだけで受信可・不可を判定し、インタフェースの妥当性は検証しません。

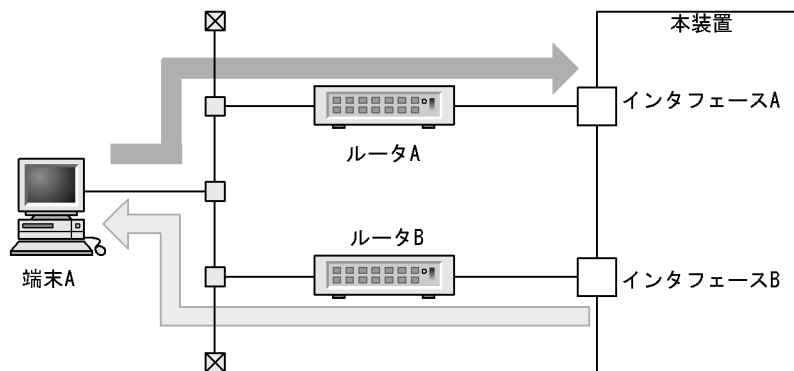
また、各モードで送信元アドレスの経路検索の際に、デフォルト経路を検索対象にするかどうかを設定できます。デフォルト経路検索対象設定は装置全体で有効になります。



3.1.3 uRPF 使用時の注意事項

(1) Strict モード使用時の注意

Strict モード使用時は、受信インタフェースと送信元アドレスの経路で指定した送信インタフェースが一致するかどうかを検証されます。したがって、次の図に示すように、本装置と隣接ルータ A および B 間で経路が非対称になるような場合、廃棄対象にはならないパケットも廃棄されることがあります。

図 3-2 非対称経路の例



(凡例)
 : 端末から本装置への経路
 : 本装置から端末への経路

上記の図では、本装置のルーティングテーブルに、端末 A 宛での経路として送信インタフェースはインタフェース B であることが登録されているため、ルータ B を経由して中継されます。端末側では、本装置宛てまたは本装置を経由する宛先の経路がルータ A を経由するように設定されているため、端末 A からのパケットは本装置のインタフェース A で受信されます。

本装置のインタフェース A で uRPF の Strict モードを設定した場合、ルーティングテーブルの検索結果であるインタフェース B 以外から受信するため、端末 A からのパケットは廃棄されます。

ただし、ロードバランスのためのマルチパスによって受信インタフェースと送信インタフェースが異なる場合は、出力対象のパスをすべて検証するため問題ありません。

(2) ロードバランス機能との併用について

本装置では uRPF とロードバランス機能を併用する際に、マルチパス最大数が 8 に制限されます。uRPF を設定する際、各種ルーティングプロトコルで 9 以上のマルチパス設定が存在すると設定できませんので、マルチパス設定を 8 以下に設定し直す必要があります。

マルチパス数の設定変更直後は、経路数が多い場合など、本装置のハードウェアルーティングテーブルにマルチパス経路が再設定されるのに時間が掛かることがあり、uRPF が誤動作するおそれがあります。マルチパス数を変更する必要がある場合は、装置を再起動することをお勧めします。

(3) フィルタ、QoS、ポリシーベースルーティング機能との同時使用について

本装置では、uRPF 機能とフィルタ、QoS、およびポリシーベースルーティング機能は同時に動作できません。パケットがフィルタ、QoS およびポリシーベースルーティングと、uRPF の両方の検証に該当する場合、廃棄のアクションが優先されます。したがって、フィルタ、QoS およびポリシーベースルーティングの検索結果が廃棄以外のアクションであっても、uRPF 検証で廃棄となった場合、そのパケットは廃棄されます。

統計情報は、機能ごとにカウントされます。uRPF およびフィルタを同時に使用した場合の統計情報を次の表に示します。

表 3-1 uRPF およびフィルタを同時に使用した場合の統計情報

フィルタによる パケット 検索結果	uRPF によるパケット検索結果			
	通過		廃棄	
通過	uRPF の廃棄カウンタ	×	uRPF の廃棄カウンタ	
	フィルタの通過カウンタ		フィルタの通過カウンタ	
	フィルタの廃棄カウンタ	×	フィルタの廃棄カウンタ	×
廃棄	uRPF の廃棄カウンタ	×	uRPF の廃棄カウンタ	
	フィルタの通過カウンタ	×	フィルタの通過カウンタ	×
	フィルタの廃棄カウンタ		フィルタの廃棄カウンタ	

(凡例) : カウントされます。 × : カウントされません。

注 IPv4 オプション付きパケットは、例外的に uRPF のカウンタだけがカウントされます。

3.2 コンフィグレーション

3.2.1 コンフィグレーションコマンド一覧

uRPF で使用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 3-2 コンフィグレーションコマンド一覧

コマンド名	説明
<code>ip urpf</code>	装置全体で uRPF を使用可能にします。
<code>ip verify unicast source reachable-via</code>	インタフェースで IPv4 の uRPF を使用します。
<code>ipv6 verify unicast source reachable-via</code>	インタフェースで IPv6 の uRPF を使用します。

3.2.2 装置全体での uRPF 設定

装置全体で uRPF を有効にするための設定例を次に示します。

[設定のポイント]

uRPF はインタフェース単位で設定しますが、その前に装置全体で uRPF を有効にする必要があります。装置全体の uRPF 設定がされていない場合、インタフェースで uRPF を設定しても無効になり装置には反映されません。また、本設定時には、各ルーティングプロトコルでマルチパス数が 8 以下に設定されている必要があります。

[コマンドによる設定]

1. `(config)# ip urpf`
装置全体で uRPF 機能を有効にします。

3.2.3 IPv4 の uRPF 設定

各インタフェースで IPv4 の uRPF を行うための設定例を次に示します。

[設定のポイント]

インタフェース単位で IPv4 の uRPF を有効にします。本設定前に装置全体で uRPF が有効になっている必要があります。また、IPv6 でも uRPF を有効にする場合は、インタフェースごとにモードを合わせる必要があります。

[コマンドによる設定]

1. `(config)# interface vlan 10`
VLAN10 のインタフェースモードに移行します。
2. `(config-if)# ip verify unicast source reachable-via rx`
VLAN10 に Strict モードの uRPF を設定します。既に IPv6 で uRPF が設定されている場合は、モードを合わせる必要があります。

3.2.4 IPv6 の uRPF 設定

各インタフェースで IPv6 の uRPF を行うための設定例を次に示します。

[設定のポイント]

インタフェース単位で IPv6 の uRPF を有効にします。本設定前に装置全体で uRPF が有効になっている必要があります。また、IPv4 でも uRPF を有効にする場合は、インタフェースごとにモードを合わせる必要があります。

[コマンドによる設定]

1. (config)# interface vlan 10

VLAN10 のインタフェースモードに移行します。

2. (config-if)# ipv6 verify unicast source reachable-via rx

VLAN10 に Strict モードの uRPF を設定します。既に IPv4 で uRPF が設定されている場合は、モードを合わせる必要があります。

3.3 オペレーション

uRPF で使用する運用コマンド一覧を次の表に示します。

表 3-3 運用コマンド一覧

コマンド名	説明
show ip-dual interface ¹ ²	IPv4/IPv6 両方の uRPF の設定状態およびインタフェース単位での廃棄統計情報を表示します。
clear counters urpf ¹ ²	IPv4/IPv6 両方の uRPF インタフェース廃棄統計情報のカウンタをクリアします。
show ip interface ¹	IPv4 の uRPF の設定状態およびインタフェース単位での廃棄統計情報を表示します。
clear counters ipv4 urpf ¹	IPv4 の uRPF インタフェース廃棄統計情報のカウンタをクリアします。
show netstat(netstat) ¹ ²	装置全体の uRPF 廃棄統計情報を表示します。
clear netstat ¹ ²	装置全体の uRPF 廃棄統計情報のカウンタをクリアします。
show ipv6 interface ²	IPv6 の uRPF の設定状態およびインタフェース単位での廃棄統計情報を表示します。
clear counters ipv6 urpf ²	IPv6 の uRPF インタフェース廃棄統計情報のカウンタをクリアします。

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。

3.3.1 uRPF 設定が有効かどうかの確認

インタフェースで uRPF 設定が有効かどうかを確認するには、show ip-dual interface コマンドを実行してください。

図 3-3 uRPF 設定状態の確認

```
> show ip-dual interface vlan 10
Date 2006/10/14 12:00:00 UTC
VLAN0010: flags=80e3<UP,BROADCAST,NOTRAILERS,RUNNING,NOARP,MULTICAST>
  mtu 1500
  inet 158.214.178.30/25 broadcast 158.214.178.127
  inet6 3ffe::1:1/64
  inet6 fe80::60:972e:1d4c%VLAN0010/64
  NIF1/Port1: UP media 100BASE-TX full(auto) 0012.e22e.1d4c
  NIF1/Port2: UP media 100BASE-TX full(auto) 0012.e22f.1d4f ChGr:5 (UP)
  Time-since-last-status-change: 78,11:22:33
  Last down at: 12/25 12:34:56
  uRPF(IPv4) : Strict Mode (Ignoring Default Route)
  uRPF(IPv6) : Disable
VLAN: 10
```

上記例では、IPv4 の uRPF が Strict モードで有効になっていて、IPv6 で uRPF は設定されていません。

3.3.2 装置全体での uRPF による廃棄パケット数確認

装置全体での uRPF による廃棄パケット数を確認するには、netstat コマンドを実行してください。次に

3. uRPF

示す例では IPv4 の uRPF 廃棄パケット数を表示していますが、IPv6 の uRPF 廃棄パケット数を表示するには、protocol パラメータに ip6 を指定します。

図 3-4 装置全体での uRPF による廃棄パケット数確認

```
> show netstat protocol ip (IPv6の場合はip6を指定します。)
Date 2006/03/24 16:10:17 UTC
ip:
    1934689 total packets received
    :
    <中略>
    :
    199 packets discarded due to uRPF
```

3.3.3 インタフェースごとの uRPF による廃棄パケット数確認

インタフェースごとの uRPF による廃棄パケット数を確認するには、show ip-dual interface urpf-discard コマンドを実行してください。

図 3-5 インタフェースごとの uRPF による廃棄パケット数確認

```
> show ip-dual interface urpf-discard vlan 2
Interface Name : VLAN002
Discard Packets due to uRPF(IPv4): 107(Pkts)
Discard Packets due to uRPF(IPv6): 107(Pkts)
```

4

QoS 制御の概要

QoS 制御は、帯域監視・マーカー・優先度決定・帯域制御によって通信品質を制御し、回線の帯域やキューのバッファ容量などの限られたネットワーク資源を有効に利用するための機能です。この章では、本装置の QoS 制御について説明します。

4.1 QoS 制御構造

4.2 QoS 制御共通のコンフィグレーション

4.3 QoS 制御共通のオペレーション

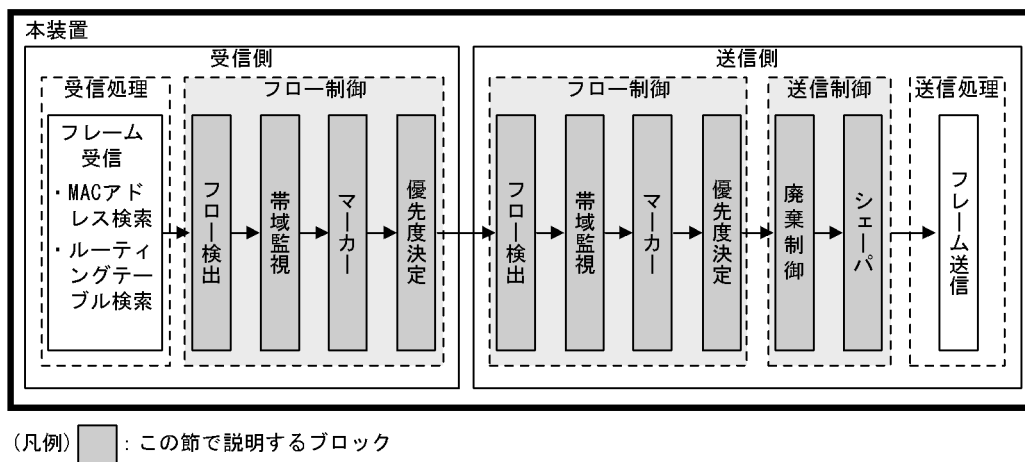
4.1 QoS 制御構造

ネットワークを利用したサービスの多様化に伴い、通信品質を保証しないベストエフォート型のトラフィックに加え、実時間型・帯域保証型のトラフィックが増加しています。本装置の QoS 制御を使用することによって、トラフィック種別に応じた通信品質を提供できます。

本装置の QoS 制御は、回線の帯域やキューのバッファ容量などの限られたネットワーク資源を有効に使用できます。アプリケーションごとに要求されるさまざまな通信品質を満たすために、QoS 制御を使用しネットワーク資源を適切に分配します。

本装置の QoS 制御の機能ブロックを次の図に示します。

図 4-1 本装置の QoS 制御の機能ブロック



図に示した QoS 制御の各機能ブロックの概要を次の表に示します。

表 4-1 QoS 制御の各機能ブロックの概要

機能部位		機能概要
受信処理部	フレーム受信	フレームを受信し、MAC アドレステーブル検索やルーティングテーブル検索を実施します。
フロー制御部	フロー検出	MAC ヘッダやプロトコル種別、IP アドレス、ポート番号などの条件に一致するフローを検出します。
	帯域監視	フローごとに帯域を監視して、帯域を超えたフローに対してペナルティを与えます。
	マーカー	IP ヘッダ内の DSCP や VLAN Tag のユーザ優先度を書き換える機能です。
	優先度決定	フローに対する優先度や、廃棄されやすさを示すキューイング優先度を決定します。
送信制御部	廃棄制御	パケットの優先度とキューの状態に応じて、該当フレームをキューイングするか廃棄するかを制御します。
	シェーパ	各キューからのフレームの出力順序および各ポートの出力帯域を制御します。
送信処理部	フレーム送信	シェーパによって制御されたフレームを送信します。

本装置の QoS 制御は、フロー制御によって決定します。

フロー制御は、優先度決定のほかに帯域監視やマーカを実施できます。フロー検出で検出したフローに対して、帯域監視、マーカ、優先度決定の各機能は同時に動作できます。

送信制御は、フロー制御によって決定した優先度に基づいて、廃棄制御やシェーパを実施します。

4.2 QoS 制御共通のコンフィグレーション

4.2.1 コンフィグレーションコマンド一覧

QoS 制御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 4-2 コンフィグレーションコマンド一覧

コマンド名	説明
advance qos-flow-group	イーサネットインタフェースまたは VLAN インタフェースに対して、Advance QoS フローリストを適用し、Advance 条件による QoS 制御を有効にします。
advance qos-flow-list	Advance 条件でフロー検出を行う Advance QoS フローリストを設定します。
advance qos-flow-list resequence	Advance QoS フローリストの条件適用順序のシーケンス番号を再設定します。
ip qos-flow-group	イーサネットインタフェースまたは VLAN インタフェースに対して、IPv4 QoS フローリストを適用し、IPv4 QoS 制御を有効にします。
ip qos-flow-list	IPv4 QoS フロー検出として動作する QoS フローリストを設定します。
ip qos-flow-list resequence	IPv4 QoS フローリストの条件適用順序のシーケンス番号を再設定します。
ipv6 qos-flow-group	イーサネットインタフェースまたは VLAN インタフェースに対して、IPv6 QoS フローリストを適用し、IPv6 QoS 制御を有効にします。
ipv6 qos-flow-list	IPv6 QoS フロー検出として動作する QoS フローリストを設定します。
ipv6 qos-flow-list resequence	IPv6 QoS フローリストの条件適用順序のシーケンス番号を再設定します。
llrlq1-burst	LLRLQ1 に対してバーストサイズを設定します。
llrlq2-burst	LLRLQ2 に対してバーストサイズを設定します。
mac qos-flow-group	イーサネットインタフェースまたは VLAN インタフェースに対して、MAC QoS フローリストを適用し、MAC QoS 制御を有効にします。
mac qos-flow-list	MAC QoS フロー検出として動作する QoS フローリストを設定します。
mac qos-flow-list resequence	MAC QoS フローリストの条件適用順序のシーケンス番号を再設定します。
mode	シェーパモードを設定します。階層化シェーパの帯域制御方式を決定します。
number-of-queue	階層化シェーパのユーザ当たりのキュー数を設定します。
predicted-tail-drop	早期検出テールドロップ機能の有効/無効を決定します。
qos-queue-group	イーサネットインタフェースに対して、QoS キューリスト情報を適用し、シェーパを有効にします。
qos-queue-list	QoS キューリスト情報にスケジューリングおよびキュー数指定を設定します。
remark	QoS の補足説明を記述します。
set-default-user-priority	出力されるフレームのユーザ優先度を 0 に書き換えます。
shaper auto-configuration	シェーパ自動設定機能を設定します。
shaper default-user	イーサネットインタフェースに階層化シェーパのデフォルトユーザを設定します。

コマンド名	説明
shaper llrlq1	イーサネットインタフェースに階層化シェーパの llrlq1 を設定します。
shaper llrlq2	イーサネットインタフェースに階層化シェーパの llrlq2 を設定します。
shaper nif	シェーパ NIF 情報を設定します。
shaper port buffer	イーサネットインタフェースに階層化シェーパのキューごとのバッファ容量を設定します。
shaper port rate-limit	イーサネットインタフェースに階層化シェーパのポート帯域制御を設定します。
shaper user	イーサネットインタフェースに階層化シェーパのユーザを設定します。
shaper user-list	階層化シェーパのユーザリストを作成します。
shaper vlan-user-map	VLAN ユーザマッピングを設定します。
shaper wgq-group rate-limit	WGQ のすべてのユーザに対する帯域制御をインタフェースに設定します。
traffic-shape rate	イーサネットインタフェースにレガシーシェーパのポート帯域制御を設定します。
upc-storm-control mode	帯域監視ストームコントロールモードを設定します。
fldm prefer ¹	フィルタ・QoS 制御のフローモード、フロー検出拡張モードを設定します。
flow mac mode ²	フィルタ・QoS 制御のフローモード、MAC モードを設定します。

注 1

「コンフィグレーションコマンドレファレンス Vol.1 9. 装置の管理」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 2. フローモード」を参照してください。

4.3 QoS 制御共通のオペレーション

4.3.1 運用コマンド一覧

QoS 制御共通の運用コマンド一覧を次の表に示します。

表 4-3 運用コマンド一覧

コマンド名	説明
show qos-flow	QoS フローグループコマンド (mac qos-flow-group , ip qos-flow-group , ipv6 qos-flow-group , advance qos-flow-group) で設定した QoS フローリスト (mac qos-flow-list , ip qos-flow-list , ipv6 qos-flow-list , advance qos-flow-list) の統計情報を表示します。
clear qos-flow	QoS フローグループコマンド (mac qos-flow-group , ip qos-flow-group , ipv6 qos-flow-group , advance qos-flow-group) で設定した QoS フローリスト (mac qos-flow-list , ip qos-flow-list , ipv6 qos-flow-list , advance qos-flow-list) の統計情報をクリアします。
show qos queueing	装置に設定されているすべての送受信キューの情報を表示します。
clear qos queueing	show qos queueing コマンドで表示するすべてのキュー統計を 0 クリアします。
show qos queueing distribution	指定したポートリストのディストリビューション送受信キューの情報を表示します。
clear qos queueing distribution	show qos queueing distribution コマンド指定で表示するすべてのキュー統計を 0 クリアします。
show qos queueing interface	指定したポートリストのポート送受信キュー情報を表示します。
clear qos queueing interface	show qos queueing interface コマンド指定で表示するすべてのキュー統計を 0 クリアします。
show qos queueing to-cpu	CPU への送信キューの情報を表示します。
clear qos queueing to-cpu	show qos queueing to-cpu コマンド指定で表示するすべてのキュー統計を 0 クリアします。
show shaper	装置に設定しているすべての階層化シェーパの統計情報を表示します。
clear shaper	装置に設定しているすべての階層化シェーパの統計情報を 0 クリアします。
show shaper <port list>	指定したポートリストの階層化シェーパの統計情報を表示します。
clear shaper <port list>	指定したポートリストの階層化シェーパの統計情報を 0 クリアします。

5

フロー制御

この章では本装置のフロー制御（フロー検出，帯域監視，マーカー，優先度決定）について説明します。

-
- 5.1 フロー検出解説
 - 5.2 フロー検出コンフィグレーション
 - 5.3 フロー検出のオペレーション
 - 5.4 帯域監視解説
 - 5.5 帯域監視のコンフィグレーション
 - 5.6 帯域監視のオペレーション
 - 5.7 マーカー解説
 - 5.8 マーカーのコンフィグレーション
 - 5.9 マーカーのオペレーション
 - 5.10 優先度決定の解説
 - 5.11 優先度決定コンフィグレーション
 - 5.12 優先度のオペレーション
-

5.1 フロー検出解説

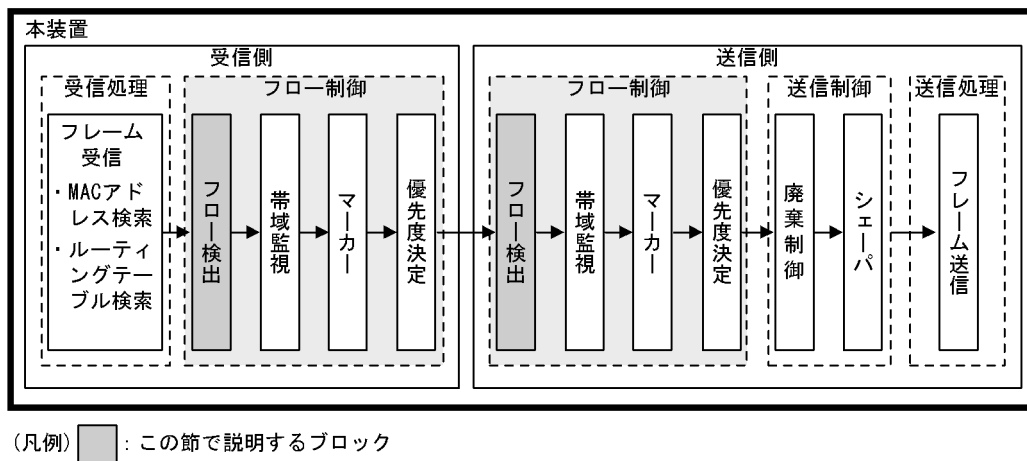
フロー検出とは、フレームの一連の流れであるフローを MAC ヘッダ、IP ヘッダ、TCP ヘッダなどの条件に基づいてフレームを検出する機能です。QoS フローリストで設定します。QoS フローリストの詳細は、「5.1.3 QoS フローリスト」を参照してください。

本装置では、イーサネットインタフェース・VLAN インタフェースで、イーサネット V2 形式および IEEE802.3 の SNAP/RFC1042 形式フレームのフロー検出ができます。インタフェースには、検出する中継種別ごとにレイヤ 2 中継のフロー検出、レイヤ 3 中継のフロー検出をそれぞれ設定してください。

フローモードのフロー検出拡張モードを設定した場合は、中継種別ごとのフロー検出に加えて、レイヤ 2 中継とレイヤ 3 中継の両方を対象にしたフロー検出を設定できます。

この節で説明するフロー検出の位置づけを次の図に示します。

図 5-1 フロー検出の位置づけ



5.1.1 フローモード

本装置では、フロー検出動作を決めるフローモードとして、MAC モードとフロー検出拡張モードを用意しています。MAC モードは VLAN 単位で設定し、フロー検出拡張モードは装置単位で設定します。

なお、MAC モードとフロー検出拡張モードは同時に設定できません。

(1) MAC モード

本装置では、レイヤ 2 中継する非 IP パケット、IP パケットを MAC ヘッダでフロー検出できるフローモードである MAC モードを用意しています。MAC モードは `flow mac mode` コマンドで指定します。

MAC モードは、VLAN インタフェースに設定した場合に有効となります。また、イーサネットインタフェースにフィルタ・QoS フロー検出を設定した場合は、該当するイーサネットインタフェースが属するすべての VLAN インタフェースに対して MAC モードを設定できません。

なお、MAC モードはフィルタ・QoS で共通の機能です。

(2) フロー検出拡張モード

本装置では、非 IP パケット、IP パケットのすべてをフロー検出対象とし、MAC ヘッダ、IP ヘッダ、レ

レイヤ 4 ヘッダの組み合わせ (Advance 条件) でフロー検出できるフロー検出拡張モードを用意しています。Advance 条件でフロー検出する場合、イーサネットインタフェースではレイヤ 2 中継フレームが、VLAN インタフェースではレイヤ 2 中継フレームとレイヤ 3 中継パケットの両方がフロー検出対象になります。フロー検出拡張モードは `fldm prefer` コマンドで指定します。

なお、フロー検出拡張モード設定ありから設定なしに変更する場合、すべての Advance 条件の設定を削除する必要があります。

(3) フローモードの動作比較

フローモードとフロー動作の関係を次の表に示します。

表 5-1 フローモードとフロー動作の関係

フローモード	対象となるフレーム	フロー動作
設定なし	レイヤ 2 中継する非 IP パケット	MAC アドレス、イーサネットタイプなどの MAC ヘッダでフレームを検出します。
	レイヤ 2 またはレイヤ 3 中継する IPv4、IPv6 パケット	IP ヘッダ、レイヤ 4 ヘッダでフレームを検出します。
MAC モード	レイヤ 2 中継するすべてのフレーム	MAC アドレス、イーサネットタイプなどの MAC ヘッダでフレームを検出します。
	レイヤ 3 中継する IPv4、IPv6 パケット	IP ヘッダ、レイヤ 4 ヘッダでフレームを検出します。
フロー検出拡張モード	レイヤ 2 中継する非 IP パケット	MAC アドレス、イーサネットタイプなどの MAC ヘッダでフレームを検出します。
	レイヤ 2 またはレイヤ 3 中継する IPv4、IPv6 パケット	MAC ヘッダ、IP ヘッダ、レイヤ 4 ヘッダでフレームを検出します。

5.1.2 フロー検出条件

フロー検出するためには、コンフィグレーションでフローを識別するための条件を指定します。フロー検出条件は大きく MAC 条件、IPv4 条件、IPv6 条件、およびフロー検出拡張モードで設定できる Advance 条件に分類されます。

- MAC 条件は、主に MAC アドレスなどの MAC ヘッダでフレームを検出します。
- IPv4 条件は、主に IPv4 アドレスなどの IPv4 ヘッダでフレームを検出します。
- IPv6 条件は、主に IPv6 アドレスなどの IPv6 ヘッダでフレームを検出します。
- Advance 条件は、MAC 条件と IPv4 条件、または MAC 条件と IPv6 条件の組み合わせでフレームを検出します。

フロー検出するインタフェースおよび中継種別ごとに、指定可能なフロー検出条件を次の表に示します。

表 5-2 指定可能なフロー検出条件

フロー検出条件	VLAN			イーサネット			
	レイヤ 2 中継指定		レイヤ 3 中継指定	レイヤ 2 中継およびレイヤ 3 中継両方指定	レイヤ 2 中継指定	レイヤ 3 中継指定	レイヤ 2 中継およびレイヤ 3 中継両方指定
	MAC モード 設定あり	MAC モード 設定なし					
MAC 条件			-	-		-	-
IPv4 条件	-			-		-	-
IPv6 条件	-			-		-	-
Advance 条件	-	-	-			-	-

(凡例) : 指定できる - : 指定できない

注

Advance 条件はフロー検出拡張モードを設定している場合に指定できます。

フロー検出条件の詳細な設定項目を次の表に示します。

表 5-3 指定可能なフロー検出条件の詳細項目

種別	設定項目	VLAN				イーサネット	
		レイヤ 2 中継指定		レイヤ 3 中継指定	レイヤ 2 中継およびレイヤ 3 中継両方指定		
		MAC モード 設定あり	MAC モード 設定なし				
MAC 条件	コンフィグレーション	VLAN ID ¹	-	-	-	-	
	MAC ヘッダ	送信元 MAC アドレス			-	-	
		宛先 MAC アドレス			-	-	
		イーサネットタイプ			-	-	
VLAN Tag ヘッダ ²	ユーザ優先度			-	-		
IPv4 条件	コンフィグレーション	VLAN ID ¹	-	-	-	-	
	VLAN Tag ヘッダ ²	ユーザ優先度	-			-	

種別	設定項目	VLAN				イーサネット		
		レイヤ 2 中継指定		レイヤ 3 中継指定	レイヤ 2 中継およびレイヤ 3 中継両方指定	レイヤ 2 中継指定		
		MAC モード 設定あり	MAC モード 設定なし					
IPv4 条件	IPv4 ヘッダ 3 4	上位プロトコル	-			-		
		送信元 IP アドレス	-			-		
		宛先 IP アドレス	-			-		
		ToS	-	-		-	-	
		DSCP	-			-		
		Precedence	-			-		
		フラグメントパケット識別 5	-			-		
	IPv4-TCP ヘッダ	送信元ポート番号	-			-		
		宛先ポート番号	-			-		
		TCP 制御フラグ 6	-	-		-	-	
	IPv4-UDP ヘッダ	送信元ポート番号	-			-		
		宛先ポート番号	-			-		
	IPv4-ICMP ヘッダ	ICMP タイプ値	-			-		
		ICMP コード値	-			-		
	IPv4-IGMP ヘッダ	IGMP コード値	-			-		
	IPv6 条件	コンフィグレーション	VLAN ID 1	-	-	-	-	
		VLAN Tag ヘッダ 2	ユーザ優先度	-			-	
IPv6 ヘッダ 3 7		上位プロトコル	-			-		
		送信元 IP アドレス 8	-			-		
		宛先 IP アドレス	-			-		
		Traffic Class	-	-		-	-	
		DSCP	-			-		
IPv6-TCP ヘッダ	送信元ポート番号	-			-			

5. フロー制御

種別	設定項目	VLAN				イーサネット	
		レイヤ 2 中継指定		レイヤ 3 中継指定	レイヤ 2 中継およびレイヤ 3 中継両方指定	レイヤ 2 中継指定	
		MAC モード 設定あり	MAC モード 設定なし				
	宛先ポート番号	-			-		
	TCP 制御フラグ ⁶	-	-		-	-	
	IPv6-UDP ヘッダ	送信元ポート番号	-			-	
		宛先ポート番号	-			-	
	IPv6-ICMP ヘッダ	ICMP タイプ	-			-	
		ICMP コード値	-			-	
Advance 条件	コンフィグレーション	VLAN ID ¹	-	-	-		
	MAC ヘッダ	送信元 MAC アドレス	-	-	-	9	
		宛先 MAC アドレス	-	-	-	9	
		イーサネットタイプ	-	-	-		
	VLAN Tag ヘッダ ²	ユーザ優先度	-	-	-		
		カスタマ Tag なしのパケット	-	-	-		
		カスタマ Tag の VLAN ID	-	-	-	10	10
		カスタマ Tag のユーザ優先度	-	-	-	10	10
	IPv4 ヘッダ ^{3 4}	上位プロトコル	-	-	-		
		送信元 IP アドレス	-	-	-		
		宛先 IP アドレス	-	-	-		
		ToS	-	-	-		
		DSCP	-	-	-		
		Precedence	-	-	-		
		フラグメントパケット識別 ⁵	-	-	-		
	IPv4-TCP ヘッダ	送信元ポート番号	-	-	-		
		宛先ポート番号	-	-	-		
		TCP 制御フラグ ⁶	-	-	-		

種別	設定項目	VLAN				イーサネット
		レイヤ 2 中継指定	レイヤ 3 中継指定	レイヤ 2 中継およびレイヤ 3 中継両方指定	レイヤ 2 中継指定	
						MAC モード 設定あり
IPv4-UDP ヘッダ	送信元ポート番号	-	-	-		
	宛先ポート番号	-	-	-		
IPv4-ICMP ヘッダ	ICMP タイプ値	-	-	-		
	ICMP コード値	-	-	-		
IPv4-IGMP ヘッダ	IGMP コード値	-	-	-		
IPv6 ヘッダ ^{3 7}	上位プロトコル	-	-	-		
	送信元 IP アドレス	-	-	-		
	宛先 IP アドレス	-	-	-		
	Traffic Class	-	-	-		
	DSCP	-	-	-		
IPv6-TCP ヘッダ	送信元ポート番号	-	-	-		
	宛先ポート番号	-	-	-		
	TCP 制御フラグ ⁶	-	-	-		
IPv6-UDP ヘッダ	送信元ポート番号	-	-	-		
	宛先ポート番号	-	-	-		
IPv6-ICMP ヘッダ	ICMP タイプ	-	-	-		
	ICMP コード値	-	-	-		

(凡例) : 指定できる : 指定できる (一部検出できない) - : 指定できない

注 1

本装置のフロー検出で検出できる VLAN ID は、VLAN コンフィグレーションで入力した VLAN に対して付与する値です。入力フレームまたは出力フレームの属する VLAN ID を検出します。複数の VLAN ID をフロー検出の対象とする場合は、VLAN リストで作成した VLAN リスト名称を指定してください。

注 2

5. フロー制御

VLAN Tag ヘッダの指定についての補足を次に示します。なお、カスタマ Tag とは 2 段目の VLAN Tag を指します。

ユーザ優先度

1 段目の VLAN Tag のユーザ優先度です。VLAN Tag なしのパケットは検出しません。

カスタマ Tag なしのパケット

2 段目の VLAN Tag が無いパケットです。VLAN Tag が 2 段以上あるパケットは検出しません。

カスタマ Tag の VLAN ID

2 段目の VLAN Tag の VLAN ID です。VLAN Tag が 1 段以下のパケットは検出しません。

カスタマ Tag のユーザ優先度

2 段目の VLAN Tag のユーザ優先度です。VLAN Tag が 1 段以下のパケットは検出しません。

(i) VLAN Tag 1段のフォーマット

MAC-DA	MAC-SA	1段目の VLAN Tag	Ether Type	Data	FCS
--------	--------	------------------	---------------	------	-----

(ii) VLAN Tag 2段のフォーマット

MAC-DA	MAC-SA	1段目の VLAN Tag	2段目の VLAN Tag	Ether Type	Data	FCS
--------	--------	------------------	------------------	---------------	------	-----

注 3

IP アドレスに own-address または own パラメータを指定することで、フロー検出を設定したインタフェースの IP アドレスが自動で検出できます。IPv4 アドレスの場合は、own-address および own を指定したインタフェースがマルチホームのときはプライマリ IPv4 アドレスが対象になります。IPv6 アドレスの場合は、own-address および own を指定したインタフェースがマルチホームでないときはフロー検出条件に指定できます。

注 4

ToS フィールドの指定についての補足を次に示します。

ToS : ToS フィールドの 3 ビット～ 6 ビットの値です。

Precedence : ToS フィールドの上位 3 ビットの値です。

Bit0 Bit1 Bit2 Bit3 Bit4 Bit5 Bit6 Bit7

Precedence	ToS	-
------------	-----	---

DSCP : ToS フィールドの上位 6 ビットの値です。

Bit0 Bit1 Bit2 Bit3 Bit4 Bit5 Bit6 Bit7

DSCP	-
------	---

注 5

QoS フローリストのパラメータである fragments パラメータを指定した場合は、IP ヘッダだけをフロー検出条件として指定できます。

注 6

ack/fin/psh/rst/syn/urg フラグが 1 または 0 のパケットを検出します。また、ack または rst フラグが 1 のパケットも検出できます。

注 7

トラフィッククラスフィールドの指定についての補足を次に示します。

トラフィッククラス : トラフィッククラスフィールドの値です。

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
トラフィッククラス							

DSCP : トラフィッククラスフィールドの上位 6 ビットの値です。

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP						-	

注 8

上位 64bit だけ指定できます。

注 9

送信側インタフェースでレイヤ 3 中継パケットの MAC アドレスを指定しても、送信時の MAC アドレスは検出できません。指定した場合、送信時の MAC アドレスではなく受信時の MAC アドレスを検出します。

注 10

送信側インタフェースでは、送信時のカスタム Tag (2 段目の VLAN Tag) を検出できません。指定した場合、送信時のカスタム Tag ではなく受信時のカスタム Tag を検出します。送信側インタフェースでのフロー検出を次の表に示します。

表 5-4 送信側インタフェースでのカスタム Tag の VLAN ID およびユーザ優先度のフロー検出

フレーム中継時の VLAN Tag		送信側インタフェースでのフロー検出	
フレーム 受信時	フレーム 送信時	カスタム Tag の VLAN ID	カスタム Tag のユーザ優先度
なし	なし	-	-
	1 段	-	-
1 段	なし	-	-
	1 段	-	-
	2 段	0 として検出	0 として検出
2 段	1 段	-	-
	2 段	受信時の 2 段目の VLAN Tag	受信時の 2 段目の VLAN Tag
	3 段	受信時の 2 段目の VLAN Tag	受信時の 2 段目の VLAN Tag
上記以外		受信時の 2 段目の VLAN Tag	受信時の 2 段目の VLAN Tag

(凡例) - : 検出できない

5.1.3 QoS フローリスト

QoS のフロー検出を実施するためにはコンフィグレーションで QoS フローリストを設定します。フロー検出条件に応じて設定する QoS フローリストが異なります。また、フロー検出条件ごとに検出可能なフレーム種別が異なります。フロー検出条件と対応する QoS フローリスト、および検出可能なフレーム種別の関係を次の表に示します。

表 5-5 フロー検出条件と対応する QoS フローリスト，検出可能なフレーム種別の関係

設定可能なフロー検出条件	対応する QoS フローリスト	検出可能なフレーム種別								
		フローモードなし			MAC モード			フロー検出拡張モード		
		非 IP	IPv4	IPv6	非 IP	IPv4	IPv6	非 IP	IPv4	IPv6
MAC 条件	mac qos-flow-list		-	-					-	-
IPv4 条件 1	ip qos-flow-list	-		-	- 2	- 2	- 2	-		-
IPv6 条件 1	ipv6 qos-flow-list	-	-		- 2	- 2	- 2	-	-	
Advance 条件	advance qos-flow-list	- 3	- 3	- 3	- 2	- 2	- 2			

(凡例) : 検出できる - : 検出できない

注 1

layer2-forwarding を指定している場合，本装置宛での IP パケットは検出できません。

注 2

MAC モードを設定している VLAN インタフェースでは，IPv4 条件，IPv6 条件，および Advance 条件を適用できません。

注 3

フローモードなしの場合，Advance 条件をインタフェースに適用できません。

QoS フローリストのインタフェースへの適用は，QoS フローグループコマンドで実施します。適用順序は，QoS フローリストのパラメータであるシーケンス番号によって決定します。

(1) イーサネットインタフェースと VLAN インタフェース同時に設定した場合の動作

イーサネットインタフェースと，該当するイーサネットインタフェースが属する VLAN インタフェースに対して QoS エントリを設定し，該当するイーサネットインタフェースからの送受信フレームに対して QoS フロー検出を実施した場合は，イーサネットインタフェース上の QoS エントリを優先します。

(2) 同一インタフェースに複数のフロー検出条件を同時に設定した場合の動作

同一インタフェースに複数のフロー検出条件を設定して，該当インタフェースの送受信フレームに対して QoS フロー検出を実施した場合は，次の順番でフレームを検出します。

1. MAC 条件
2. IPv4 条件
3. IPv6 条件
4. Advance 条件

例えば，MAC 条件でフロー検出したフレームは，Advance 条件ではフロー検出されません。また，統計情報もカウントされません。

5.1.4 フロー検出使用時の注意事項

(1) 本装置が自発的に送信するパケット / フレームに対する QoS フロー検出

本装置が自発的に送信するフレームは、QoS フロー検出できません。

(2) IPv4 オプション付きパケットに対する QoS フロー検出

レイヤ 2 中継する IPv4 オプション付きパケットを QoS フロー検出する場合は、フロー検出条件に MAC ヘッダ、IPv4 ヘッダを指定してください。TCP/UDP/ICMP/IGMP ヘッダをフロー検出条件に指定しても、指定したフロー検出条件に従った QoS フロー検出をしません。

また、レイヤ 3 中継する IPv4 オプション付きパケットは QoS フロー検出しません。

(3) 拡張ヘッダのある IPv6 パケットに対する QoS フロー検出

拡張ヘッダのある IPv6 パケットを QoS フロー検出する場合は、フロー検出条件に MAC ヘッダ、IPv6 ヘッダを指定してください。TCP/UDP/ICMP ヘッダをフロー検出条件に指定しても、QoS フロー検出しません。

(4) IPv4 フラグメントパケットに対する QoS フロー検出

IPv4 フラグメントパケットに対して 2 番目以降のフラグメントパケットは TCP/UDP/ICMP/IGMP ヘッダがフレーム内にありません。フラグメントパケットを受信した際の QoS フロー検出を次の表に示します。

表 5-6 IPv4 フラグメントパケットと QoS フロー検出の関係

フロー検出条件	フロー検出条件とパケットの一致 / 不一致	先頭パケット	2 番目以降のパケット
IPv4 ヘッダだけ	IPv4 ヘッダ一致	一致したエントリの動作	一致したエントリの動作
	IPv4 ヘッダ不一致	次のエントリを検索	次のエントリを検索
IPv4 ヘッダ +TCP/UDP/ICMP/IGMP ヘッダ	IPv4 ヘッダ一致,TCP/UDP/ICMP/IGMP ヘッダ一致	一致したエントリの動作	-
	IPv4 ヘッダ一致,TCP/UDP/ICMP/IGMP ヘッダ不一致	次のエントリを検索	次のエントリを検索
	IPv4 ヘッダ不一致,TCP/UDP/ICMP/IGMP ヘッダ不一致	次のエントリを検索	次のエントリを検索

(凡例)

- : TCP/UDP/ICMP/IGMP ヘッダがパケットに無いため、常に TCP/UDP/ICMP/IGMP ヘッダ不一致として扱うので該当しない

注

QoS フローリストのパラメータである fragments パラメータを指定することで、2 番目以降のフラグメントパケットだけを検出できます。

(5) IPv6 フラグメントパケットに対する QoS フロー検出

IPv6 フラグメントパケットの 2 番目以降のフラグメントパケットは TCP/UDP/ICMP ヘッダがパケット内にありません。IPv6 フラグメントパケットを受信した際の QoS フロー検出を次の表に示します。

表 5-7 IPv6 フラグメントパケットと QoS フロー検出の関係

フロー検出条件	フロー検出条件とパケットの一致 / 不一致	先頭パケット	2 番目以降のパケット
IPv6 ヘッダだけ	IPv6 ヘッダ一致	一致したエントリの動作	一致したエントリの動作
	IPv6 ヘッダ不一致	次のエントリを検索	次のエントリを検索
IPv6 ヘッダ +TCP/UDP/ ICMP ヘッダ	IPv6 ヘッダ一致 ,TCP/ UDP/ICMP ヘッダ一致	次のエントリを検出	-
	IPv6 ヘッダ一致 ,TCP/ UDP/ICMP ヘッダ不一致	次のエントリを検索	次のエントリを検出
	IPv6 ヘッダ不一致 ,TCP/ UDP/ICMP ヘッダ不一致	次のエントリを検索	次のエントリを検索

(凡例) - : TCP/UDP/ICMP/IGMP ヘッダがパケットに無いため該当しない

注

QoS フローリストのパラメータである ipv6 パラメータを指定した場合だけ、有効な QoS エントリです。

(6) マルチキャストフレーム・ブロードキャストフレームに対する QoS フロー検出

マルチキャストフレーム・ブロードキャストフレームは、レイヤ 2 中継・レイヤ 3 中継ともに実施されます。マルチキャストフレーム・ブロードキャストフレームを QoS フロー検出する場合は、該当するインタフェースに対して次のどちらかを適用してください。

- レイヤ 2 中継指定の QoS フローリストおよびレイヤ 3 中継指定の QoS フローリスト
- Advance 条件で、レイヤ 2 中継およびレイヤ 3 中継両方指定の QoS フローリスト
この場合、統計情報は 2 回カウントされます。

(7) VLAN Tag 付きフレームに対する QoS フロー検出

本装置では、2 段までの VLAN Tag があるフレームについて、IPv4 ヘッダ・IPv6 ヘッダをフロー検出条件とした QoS フロー検出ができます。3 段以上の VLAN Tag があるフレームを QoS フロー検出する場合は、MAC ヘッダをフロー検出条件とした QoS フローリストを適用してください。

(8) QoS エントリ変更時の動作

本装置では、インタフェースに適用済みの QoS エントリを変更すると、変更が反映されるまでの間、検出の対象となるフレームが検出されなくなります。そのため、一時的にほかの QoS エントリで検出される場合があります。

(9) VLAN インタフェースの送信側での統計情報

本装置でフラッディングされるパケットまたは宛先 MAC アドレスがマルチキャストアドレスのパケットをレイヤ 2 中継する場合、次に示す三つの条件をすべて満たすと、VLAN インタフェースの送信側に設定した QoS フローリストの統計情報が実際の値より 65536 の倍数分少なくなることがあります。この統計情報とは、運用コマンド show qos-flow および MIB の統計情報の両方を指します。

なお、フロー検出動作には影響ありません。

- イーサネットインタフェースまたは VLAN インタフェースの受信側に設定した QoS フローリストに、レイヤ 2 中継パケットが一致した場合
- VLAN インタフェースの送信側に設定した QoS フローリストにレイヤ 2 中継パケットが一致し、一致

する前の統計情報が「(65536 の倍数) - 2」の場合

- パケットをレイヤ 2 中継する VLAN インタフェースに、三つ以上のイーサネットインタフェースが所属している場合

5.2 フロー検出コンフィグレーション

5.2.1 フローモードの設定

(1) MAC モードの設定

QoS 制御の MAC モードを指定する例を示します。

[設定のポイント]

MAC モードは、装置の基本的な動作条件を決定するため、最初に設定します。

[コマンドによる設定]

1. `(config)# interface vlan 10`
VLAN10 のインタフェースモードに移行します。
2. `(config-if)# flow mac mode`
flow mac mode を有効にします。

[注意事項]

イーサネットインタフェースにフィルタ・QoS フロー検出を設定した場合は、該当するイーサネットインタフェースが属するすべての VLAN インタフェースに対して MAC モードを設定できません。MAC モードを設定した VLAN 配下のイーサネットインタフェースに対してフィルタ・QoS フロー検出を設定できません。MAC モードを設定しない場合は、イーサネットインタフェース・VLAN インタフェース共に、フィルタ・QoS フロー検出を設定できます。

(2) フロー検出拡張モードの設定

QoS 制御のフロー検出拡張モードを指定する例を次に示します。

[設定のポイント]

フロー検出拡張モードは、装置の基本的な動作条件を決定するため、最初に設定します。

[コマンドによる設定]

1. `(config)# fldm prefer default standard-advance`
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、フロー系テーブル容量を standard-advance に設定します。コンフィグレーションの変更を確認して 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。

[注意事項]

すべての VLAN に MAC モードが設定されていない場合は、フロー検出拡張モードに変更できます。また、すべてのインタフェースに Advance 条件のアクセスリストおよび QoS フローリストが設定されていない場合は、フロー検出拡張モード設定なしに変更できます。

5.2.2 複数インタフェースの QoS 制御の指定

複数のイーサネットインタフェースに QoS 制御を指定する例を示します。

[設定のポイント]

config-if-range モードで QoS 制御を有効に設定することで、複数のイーサネットインタフェースに QoS 制御を設定できます。

[コマンドによる設定]

1. **(config)# ip qos-flow-list QOS-LIST1**
IPv4 QoS フローリスト (QOS-LIST1) を作成します。本リストを作成することによって、IPv4 QoS フローリストモードに移行します。
2. **(config-ip-qos)# qos ip any host 192.168.100.10 action priority-class 6**
192.168.100.10 の IP アドレスを宛先とし、出力優先度 = 6 の QoS フローリストを設定します。
3. **(config-ip-qos)# exit**
IPv4 QoS フローリストモードからグローバルコンフィギュレーションモードに戻ります。
4. **(config)# interface range gigabitethernet 1/1-4**
ポート 1/1-4 のインタフェースモードに移行します。
5. **(config-if-range)# ip qos-flow-group QOS-LIST1 out layer2-forwarding**
送信側にレイヤ 2 中継を対象とする IPv4 QoS フローリストを有効にします。

5.3 フロー検出のオペレーション

show qos-flow コマンドによって、設定した内容が反映されているかどうかを確認します。

5.3.1 IPv4 パケットをフロー検出条件とした QoS 制御の動作確認

IPv4 パケットをフロー検出条件とした QoS 制御の動作確認の方法を次の図に示します。

図 5-2 IPv4 パケットをフロー検出条件とした QoS 制御の動作確認

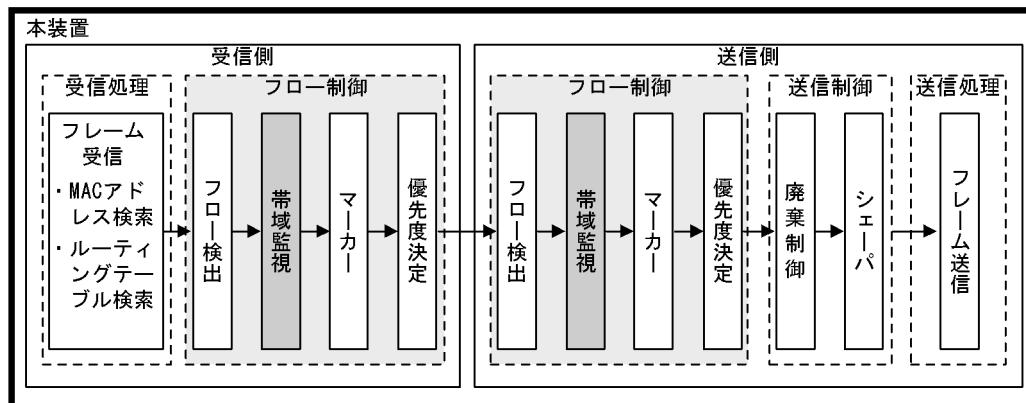
```
> show qos-flow 1/1 QOS-LIST1 out
Date 2006/03/01 12:00:00 UTC
Using Port:1/1 out
IP qos-flow-list:QOS-LIST1 layer2-forwarding
  ip any host 192.168.100.10 action priority-class 6
  matched packets          :          74699826
```


指定したポートの QoS 制御に「IP qos-flow-list」が表示されることを確認します。また、フロー検出条件に一致したフレームは matched packets で確認します。

5.4 帯域監視解説

帯域監視は、フロー検出で検出したフローの帯域を監視する機能です。この節で説明する帯域監視の位置づけを次の図に示します。

図 5-3 帯域監視の位置づけ



(凡例)  : この節で説明するブロック

5.4.1 帯域監視

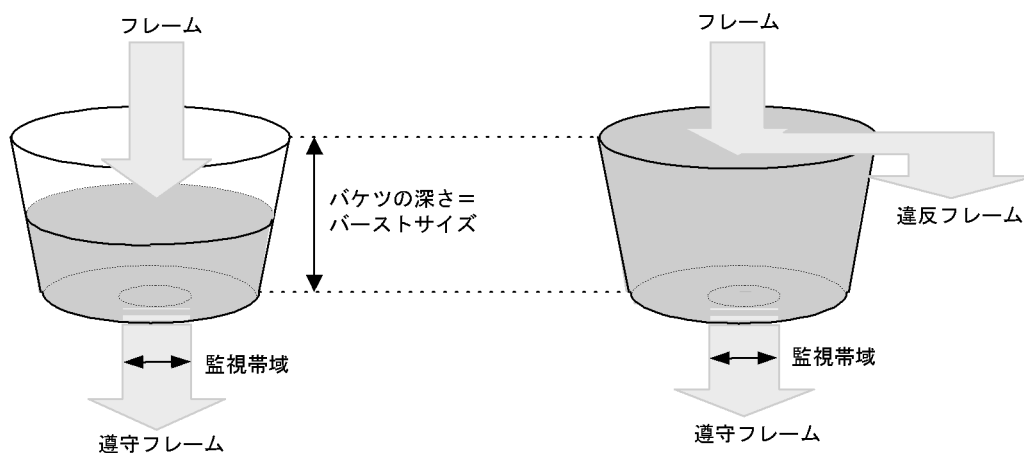
フロー検出で検出したフレームのフレーム長（フレーム間ギャップ から FCS まで）を基に帯域を監視する機能です。指定した監視帯域内として中継するフレームを「遵守フレーム」、監視帯域以上としてペナルティを科すフレームを「違反フレーム」と呼びます。

注 フレーム間ギャップは、12byte とします。

フロー検出で検出したフレームが監視帯域を遵守しているか、または違反しているかの判定には、水の入った穴の開いたバケツをモデルとする、Leaky Bucket アルゴリズムを用いています。

Leaky Bucket アルゴリズムのモデルを次の図に示します。

図 5-4 Leaky Bucket アルゴリズムのモデル



バケツからは監視帯域分の水が流れ、フレーム送受信時にはフレーム間ギャップから FCS までのサイズの

水が注ぎ込まれます。水が注ぎ込まれる際にパケットがあふれていなければ、遵守フレームとして中継されます（上図の左側の例）。水が注ぎ込まれる際にパケットがあふれている場合は、フロー検出で検出したフレームを違反フレームとしてペナルティを科します（上図の右側の例）。水が一時的に大量に注ぎこまれたときに許容できる量、すなわちパケットの深さがバーストサイズに対応します。

バーストサイズのデフォルトは 3000byte ですが、より帯域の揺らぎが大きいトラフィックの遵守パケットを中継する際には、バーストサイズを大きく設定し使用してください。

なお、バーストサイズは、フロー検出で検出されたフレームのフレーム長より大きな値を指定してください。バーストサイズが注入されるフレーム長より小さい値を指定した場合は、設定した帯域以下で違反となる場合があります。

本機能は、最低帯域監視と最大帯域制御から成ります。最低帯域監視は、違反フレームに対してマーカーや優先度決定によって優先度や DSCP を書き換え、ペナルティを科します。最大帯域制御は違反フレームを廃棄します。最低帯域監視と最大帯域制御で使用できるペナルティの種類を次の表に示します。

表 5-8 最低帯域監視と最大帯域制御で使用できるペナルティの種類

違反フレームに対するペナルティ	帯域監視種別	
	最低帯域監視	最大帯域制御
廃棄	-	
キューイング優先度変更		-
DSCP 書き換え		-
ユーザ優先度書き換え		-

（凡例） : 使用可能なペナルティ - : 使用不可能なペナルティ

本機能と、マーカー、優先度決定を同時に実施することができますが、最低帯域監視に違反したフレームは、違反フレームに対するペナルティを優先します。

5.4.2 帯域監視ストームコントロールモード

本装置では、帯域監視とストームコントロール機能を同時に実施する帯域監視ストームコントロールモードを用意しています。使い方に合わせて選択してください。

帯域監視ストームコントロールモードの動作概要を次の表に示します。

表 5-9 帯域監視ストームコントロールモードの動作概要

帯域監視 ストームコントロールモード	動作概要
upc-in-and-storm-control	帯域監視とストームコントロール機能を同時に実施したい場合に指定します。
upc-in-in	受信インタフェースで、最大帯域制御と最低帯域監視を同時に実施したい場合に指定します。
upc-in-out	送信インタフェースで、帯域監視を実施したい場合に指定します。

帯域監視ストームコントロールモードは、コンフィグレーションコマンド `upc-storm-control mode` で指定します。帯域監視ストームコントロールモードのデフォルトは、`upc-in-and-storm-control` です。

帯域監視ストームコントロールモードと動作の関係を次の表に示します。

表 5-10 帯域監視ストームコントロールモードと動作の関係【AX6700S】

帯域監視ストームコントロールモード	指定可能な動作			
	帯域監視			ストームコントロール機能
	受信インタフェース		送信インタフェース	
	最大帯域制御または、最低帯域監視を指定	最大帯域制御と、最低帯域監視を同時に指定	最大帯域制御または、最低帯域監視を指定	
upc-in-and-storm-control		-	-	
upc-in-in			-	-

(凡例) : 指定できる - : 指定できない

注

イーサネットインタフェースのレイヤ 2 中継に対して指定できます。

表 5-11 帯域監視ストームコントロールモードと動作の関係【AX6600S】

帯域監視ストームコントロールモード	指定可能な動作			
	帯域監視			ストームコントロール機能
	受信インタフェース		送信インタフェース	
	最大帯域制御または、最低帯域監視を指定	最大帯域制御と、最低帯域監視を同時に指定	最大帯域制御または、最低帯域監視を指定	
upc-in-and-storm-control	1	-	-	
upc-in-in	1	1	-	-
upc-in-out ²		-		-

(凡例) : 指定できる - : 指定できない

注 1

イーサネットインタフェースのレイヤ 2 中継に対して指定できます。VLAN インタフェースに対しては、redundancy max-ppsp コマンドで、稼働させる PSP 数に 1 を設定しているときに指定できます。

注 2

upc-in-out は、redundancy max-ppsp コマンドで、稼働させる PSP 数に 1 を設定しているときに指定できます。

表 5-12 帯域監視ストームコントロールモードと動作の関係【AX6300S】

帯域監視ストームコントロールモード	指定可能な動作			
	帯域監視			ストームコントロール機能
	受信インタフェース		送信インタフェース	
	最大帯域制御または、最低帯域監視を指定	最大帯域制御と、最低帯域監視を同時に指定	最大帯域制御または、最低帯域監視を指定	
upc-in-and-storm-control		-	-	
upc-in-in			-	-
upc-in-out		-		-

(凡例) : 指定できる - : 指定できない

ストームコントロール機能の詳細は、「25 ストームコントロール」を参照してください。

5.4.3 帯域監視使用時の注意事項

(1) 帯域監視機能とほかの機能を同時に使用したときに優先する動作

帯域監視機能とマーカー、優先度決定およびデフォルトユーザ優先度書き換えを同時に使用した場合は、次の順で動作を優先しフレームを送信します。デフォルトユーザ優先度書き換えについては、「6.4.5 デフォルトユーザ優先度書き換え」を参照してください。

1. デフォルトユーザ優先度書き換え（ユーザ優先度だけ）
2. 送信インタフェースに設定した、最低帯域監視に違反したフレームに対するペナルティ
3. 送信インタフェースに設定した、優先度決定またはマーカー
4. 受信インタフェースに設定した、最低帯域監視に違反したフレームに対するペナルティ
5. 受信インタフェースに設定した、優先度決定またはマーカー

(2) フローで指定した監視帯域と出力回線・出力キューの関係

複数のフローで帯域監視機能を使用している場合は、各 QoS フローエントリで指定した監視帯域値の合計が、出力イーサネットインタフェースまたは送信キューの帯域値以内となるように、各監視帯域値を調整してください。

(3) 帯域監視機能を使用しないフローとの混在

帯域監視機能を使用しないフローと使用するフローが同じ回線またはキューに出力されないようにしてください。

(4) プロトコル制御パケットの帯域監視

本装置では、本装置宛てのプロトコル制御フレームも帯域監視対象になります。したがって、本装置宛てのプロトコル制御フレームも最大帯域制御違反として廃棄される場合があります。そのため、本装置宛てのプロトコル制御フレームを考慮した最大帯域を確保する必要があります。

(5) TCP フレームに対する最大帯域制御の使用

最大帯域制御を使用した場合は、TCP のスロースタートが繰り返されデータ転送速度が極端に遅くなる場

合があります。

上記動作を防ぐために、最低帯域監視を使用して、「フレームが廃棄されやすくなるようにキューイング優先度を下げる」の動作を実施するようにしてください。本設定によって、契約帯域を超えてもすぐに廃棄されなくて、出力回線が混んできたときだけに廃棄されるようになります。

(6) バーストサイズの設定

最大帯域制御および最低帯域監視のどちらか、または両方を使用している場合、装置内での帯域揺らぎの影響で、遵守パケットを違反パケットとして扱うことがあります。

この場合、最大帯域制御および最低帯域監視のバーストサイズを 12000 バイト以上に設定することで、装置内での帯域揺らぎによる影響をなくせます。

(7) マルチキャストフレーム・ブロードキャストフレームに対する帯域監視

マルチキャストフレーム・ブロードキャストフレームは、レイヤ 2 中継・レイヤ 3 中継ともに実施されます。そのため、Advance 条件でレイヤ 2 中継およびレイヤ 3 中継両方指定の QoS フローリストを適用した場合、帯域監視でのマルチキャストフレーム・ブロードキャストフレームは 1 フレームで 2 フレーム分となります。

(8) 帯域監視機能と指定可能なインタフェース【AX6700S】

帯域監視を使用したフローは、受信側のイーサネットインタフェースに指定できます。

(9) 帯域監視機能に制限のある送信インタフェース【AX6600S】【AX6300S】

- ポート 1/1 のイーサネットインタフェースでは、送信側のレイヤ 2 中継フレームに対して帯域監視機能を動作させないでください。該当フレームに対して帯域監視機能を動作させた場合、実際に指定した帯域より小さい値で帯域監視機能が動作します。
- uRPF の Strict モードが動作している VLAN インタフェースでは、送信側のレイヤ 3 中継パケットに対して帯域監視機能を動作させないでください。該当パケットに対して帯域監視機能を動作させた場合、実際に指定した帯域より小さい値で帯域監視機能が動作します。

(10) 送信側 VLAN インタフェースの帯域監視対象パケットおよびフレーム【AX6600S】【AX6300S】

VLAN インタフェースの送信側で帯域監視機能を動作させた場合、本装置でレイヤ 3 中継するパケットおよびレイヤ 2 中継するフレームのうち、次に示すパケット/フレームも帯域監視対象とします。

次に示す状態ではなかったために廃棄されるパケット/フレーム

- 運用コマンド show port で、ポート状態が運用中（正常動作中）
- 運用コマンド show channel-group で、チャンネルグループ状態がデータパケット送受信可能状態
- 運用コマンド show spanning-tree で、ポート状態が転送状態
- 運用コマンド show axrp で、リングポート状態がフォワーディング状態

本装置でフラグメントする前のパケット

ARP/NDP の未解決によって本装置に一時的に滞留するパケット

注 違反パケット/フレームに対してペナルティを科しません。

5.5 帯域監視のコンフィグレーション

5.5.1 帯域監視ストームコントロールモードの設定

[設定のポイント]

帯域監視ストームコントロールモードは、装置の基本的な動作条件を決定するため、最初に設定します。

[コマンドによる設定]

1. (config)# upc-storm-control mode upc-in-in
帯域監視ストームコントロールモードの upc-in-in を設定します。

5.5.2 最大帯域制御の設定

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出を行い、最大帯域制御を行う帯域監視を設定します。

[コマンドによる設定]

1. (config)# ip qos-flow-list QOS-LIST1
IPv4 QoS フローリスト (QOS-LIST1) を作成します。本リストを作成することによって、IPv4 QoS フローリストモードに移行します。
2. (config-ip-qos)# qos ip any host 192.168.100.10 action max-rate 5M
max-rate-burst 3000
宛先 IP アドレスが 192.168.100.10 のフローに対し、最大帯域制御の監視帯域 = 5Mbit/s、最大帯域制御のバーストサイズ = 3000byte の IPv4 QoS フローリストを設定します。
3. (config-ip-qos)# exit
IPv4 QoS フローリスト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。
4. (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。
5. (config-if)# ip qos-flow-group QOS-LIST1 in layer2-forwarding
受信側にレイヤ 2 中継を対象とする IPv4 QoS フローリスト (QOS-LIST1) を有効にします。

5.5.3 最低帯域監視違反時のキューイング優先度の設定

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出を行い、最低帯域監視を行うことを設定します。最低帯域監視を違反したフレームに対しては、キューイング優先度の変更を行う設定をします。

[コマンドによる設定]

1. (config)# ip qos-flow-list QOS-LIST2

IPv4 QoS フローリスト (QOS-LIST2) を作成します。本リストを作成することによって、IPv4 QoS フローリストモードに移行します。

2. (config-ip-qos)# qos ip any host 192.168.110.10 action min-rate 1M
min-rate-burst 3000 penalty-discard-class 1
宛先 IP アドレスが 192.168.110.10 のフローに対し、最低監視帯域 =1Mbit/s、最低監視帯域のバーストサイズ =3000byte、最低帯域監視での違反フレームのキューイング優先度 =1 の IPv4 QoS フローリストを設定します。
3. (config-ip-qos)# exit
IPv4 QoS フローリスト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。
4. (config)# interface gigabitethernet 1/3
ポート 1/3 のインタフェースモードに移行します。
5. (config-if)# ip qos-flow-group QOS-LIST2 out layer2-forwarding
送信側にレイヤ 2 中継を対象とする IPv4 QoS フローリスト (QOS-LIST2) を有効にします。

5.5.4 最低帯域監視違反時の DSCP 書き換えの設定

特定のフローに対して最低帯域監視 (違反フレームは DSCP の書き換え) を実施する場合に設定します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出を行い、最低帯域監視 (min-rate) を行う帯域監視を設定します。最低監視帯域を違反したフレームに対しては、DSCP 値の変更を行う設定をします。

[コマンドによる設定]

1. (config)# ip qos-flow-list QOS-LIST3
IPv4 QoS フローリスト (QOS-LIST3) を作成します。本リストを作成することによって、IPv4 QoS フローリストモードに移行します。
2. (config-ip-qos)# qos ip any host 192.168.120.10 action min-rate 1M
min-rate-burst 3000 penalty-dscp 8
宛先 IP アドレスが 192.168.120.10 のフローに対し、最低監視帯域 =1Mbit/s、最低監視帯域のバーストサイズ =3000byte、最低帯域監視での違反フレームの DSCP 値 =8 の IPv4 QoS フローリストを設定します。
3. (config-ip-qos)# exit
IPv4 QoS フローリスト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。
4. (config)# interface vlan 10
VLAN10 のインタフェースモードに移行します。
5. (config-if)# ip qos-flow-group QOS-LIST3 in layer3-forwarding
受信側にレイヤ 3 中継を対象とする IPv4 QoS フローリスト (QOS-LIST3) を有効にします。

5.5.5 最大帯域制御と最低帯域監視の組み合わせの設定

特定のフローに対して最大帯域制御と最低帯域監視（違反フレームは DSCP の書き換え）を実施したい場合に設定します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出を行い、最大帯域制御と最低帯域監視を行う帯域監視を設定します。最低帯域監視を違反したフレームに対しては、DSCP 値の変更を行う設定をします。

[コマンドによる設定]

1. (config)# ip qos-flow-list QOS-LIST4
IPv4 QoS フローリスト (QOS-LIST4) を作成します。本リストを作成することによって、IPv4 QoS フローリストモードに移行します。
2. (config-ip-qos)# qos ip any host 192.168.130.10 action max-rate 5M
max-rate-burst 6000 min-rate 1M min-rate-burst 3000 penalty-dscp 8
宛先 IP アドレスが 192.168.130.10 のフローに対し、最大帯域制御の監視帯域 = 5Mbit/s、最大帯域制御のバーストサイズ = 6000byte、最低監視帯域 = 1Mbit/s、最低監視帯域のバーストサイズ = 3000byte、最低帯域監視での違反フレームの DSCP 値 = 8 の IPv4 QoS フローリストを設定します。
3. (config-ip-qos)# exit
IPv4 QoS フローリストモードからグローバルコンフィギュレーションモードに戻ります。
4. (config)# interface vlan 20
VLAN20 のインタフェースモードに移行します。
5. (config-if)# ip qos-flow-group QOS-LIST4 in layer3-forwarding
受信側にレイヤ 2 中継を対象とする IPv4 QoS フローリスト (QOS-LIST4) を有効にします。

5.6 帯域監視のオペレーション

show qos-flow コマンドによって、設定した内容が反映されているかどうかを確認します。

5.6.1 最大帯域制御の確認

最大帯域制御の確認方法を次の図に示します。

図 5-5 最大帯域制御の確認

```
> show qos-flow 1/1 QOS-LIST1 in
Date 2006/09/01 12:00:00 UTC
Using Port:1/1 in
IP qos-flow-list:QOS-LIST1 layer2-forwarding
  ip any host 192.168.100.10 action max-rate 5M max-rate-burst 3000
  matched packets
    (max-rate over) :          7
    (max-rate under):        28
```

QOS-LIST1 のリスト情報に「最大帯域制御の監視帯域 (max-rate 5M)」、「最大帯域制御のバーストサイズ (max-rate-burst 3000)」が表示されることを確認します。また、違反フレームは matched packets (max-rate over)、遵守フレームは matched packets (max-rate under) で確認します。

5.6.2 最低帯域監視違反時のキューイング優先度の確認

最低帯域監視違反時のキューイング優先度の確認方法を次の図に示します。

図 5-6 最低帯域監視違反時のキューイング優先度の確認

```
> show qos-flow 1/3 QOS-LIST2 out
Date 2006/09/01 12:00:00 UTC
Using Port:1/3 out
IP qos-flow-list:QOS-LIST2 layer2-forwarding
  ip any host 192.168.110.10 action min-rate 1M min-rate-burst 3000
  penalty-discard-class 1
  matched packets
    (min-rate over) :          9826
    (min-rate under):       74699826
```

QOS-LIST2 のリスト情報に「最低監視帯域 (min-rate 1M)」、「最低監視帯域のバーストサイズ (min-rate-burst 3000)」、「違反フレームのキューイング優先度 (penalty-discard-class 1)」が表示されることを確認します。また、違反フレームは matched packets (min-rate over)、遵守フレームは matched packets (min-rate under) で確認します。

5.6.3 最低監視帯域違反時の DSCP 書き換えの確認

最低監視帯域違反時の DSCP 書き換えの確認方法を次の図に示します。

図 5-7 最低監視帯域違反時の DSCP 書き換えの確認

```
> show qos-flow vlan 10 QOS-LIST3 in
Date 2006/09/01 12:00:00 UTC
Using Interface:vlan 10 in
IP qos-flow-list:QOS-LIST3 layer3-forwarding
  ip any host 192.168.120.10 action min-rate 1M min-rate-burst 3000
```

```

penalty-dscp CS1
  matched packets
    (min-rate over) :          28
    (min-rate under):          7

```

QOS-LIST3 のリスト情報に「最低監視帯域 (min-rate 1M)」、「最低監視帯域のバーストサイズ (min-rate-burst 3000)」、「違反フレームの DSCP 値 (penalty-dscp CS1)」が表示されることを確認します。また、違反フレームは matched packets (min-rate over)、遵守フレームは matched packets (min-rate under) で確認します。

5.6.4 最大帯域制御と最低帯域監視の組み合わせの確認

最大帯域制御と最低帯域監視の組み合わせの確認方法を次の図に示します。

図 5-8 最大帯域制御と最低帯域監視の組み合わせの確認

```

> show qos-flow vlan 20 QOS-LIST4 in
Date 2006/09/01 12:00:00 UTC
Using Interface:vlan 20 in
IP qos-flow-list:QOS-LIST4 layer3-forwarding
  ip any host 192.168.130.10 action max-rate 5M max-rate-burst 6000 min-rate
  1M min-rate-burst 3000 penalty-dscp CS1
    matched packets
      (max-rate over) :          28
      (min-rate over) :          58214
      (min-rate under):          74699826

```

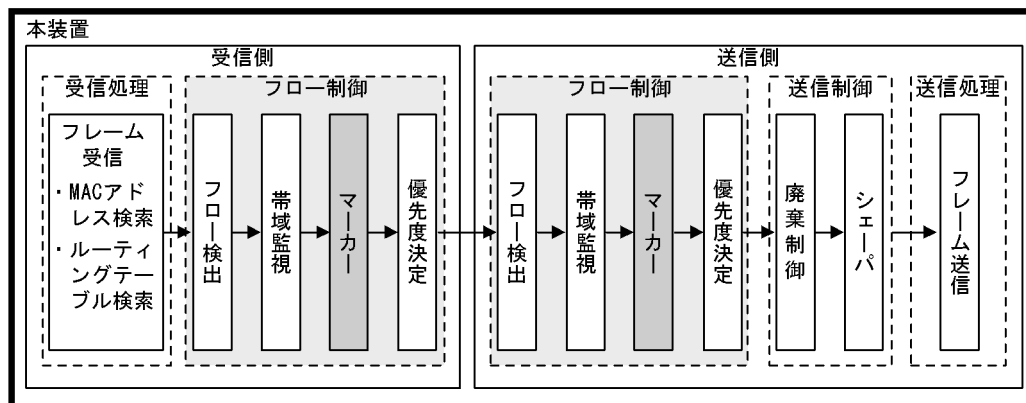
QOS-LIST4 のリスト情報に「最大帯域制御の監視帯域 (max-rate 5M)」、「最大帯域制御のバーストサイズ (max-rate-burst 6000)」、「最低監視帯域 (min-rate 1M)」、「最低監視帯域のバーストサイズ (min-rate-burst 3000)」、「違反フレームの DSCP 値 (penalty-dscp CS1)」が表示されることを確認します。

最大帯域制御の違反フレームは matched packets (max-rate over) で確認します。最低帯域監視の違反フレームは matched packets (min-rate over)、最低帯域監視の遵守フレームは matched packets (min-rate under) で確認します。

5.7 マーカー解説

マーカーは、フロー検出で検出したフレームの VLAN Tag 内のユーザ優先度および IP ヘッダ内の DSCP を書き換える機能です。この節で説明するマーカーの位置づけを次の図に示します。

図 5-9 マーカーの位置づけ

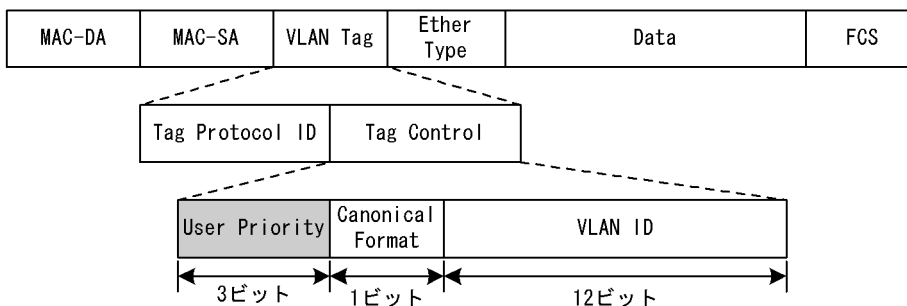


(凡例) : この節で説明するブロック

5.7.1 ユーザ優先度書き換え

フロー検出で検出したフレームの VLAN Tag 内にあるユーザ優先度 (User Priority) を書き換える機能です。ユーザ優先度は、次の図に示す Tag Control フィールドの先頭 3 ビットを指します。

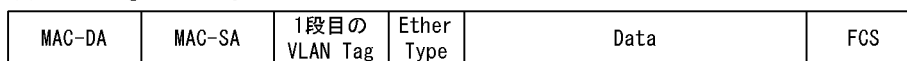
図 5-10 VLAN Tag のヘッダフォーマット



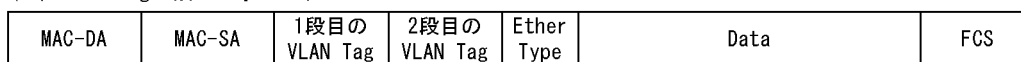
VLAN トンネル使用時のフレームに対してユーザ優先度書き換えを実施する場合は、対象となる VLAN トンネルのフレームフォーマットを次の図に示します。

図 5-11 VLAN トンネルのフレームフォーマットの概略図

(i) VLAN Tag 1段のフォーマット



(ii) VLAN Tag 2段のフォーマット



また、VLAN トンネルとユーザ優先度書き換え機能が同時実施される場合の動作について、次の表に示し

ます。

表 5-13 VLAN トンネルとユーザ優先度書き換え機能の競合動作

中継の種類		ユーザ優先度書き換え対象の VLAN Tag
受信時の VLAN Tag 数	送信時の VLAN Tag 数	
Tag なし	1	1 段目の VLAN Tag
1	1	1 段目の VLAN Tag
1	2	1 段目の VLAN Tag
1	Tag なし	書き換え不可
2	1	1 段目の VLAN Tag
2	2	1 段目の VLAN Tag

本装置がレイヤ 3 中継をする場合は、ユーザ優先度の書き換えを使用しないで受信した VLAN から、別の VLAN へ VLAN Tag フレームを中継すると、出力するフレームのユーザ優先度はデフォルトの 0 になります。

ユーザ優先度書き換え機能とデフォルトユーザ優先度書き換え機能を同時に使用した場合は、デフォルトユーザ優先度書き換え機能の動作に従ってユーザ優先度を決定します。デフォルトユーザ優先度書き換えについては、「6.4.5 デフォルトユーザ優先度書き換え」を参照してください。

5.7.2 DSCP 書き換え

IPv4 ヘッダの TOS フィールドまたは IPv6 ヘッダのトラフィッククラスフィールドの上位 6 ビットである DSCP 値を書き換える機能です。TOS フィールドのフォーマットおよびトラフィッククラスフィールドのフォーマットの図を次に示します。

図 5-12 TOS フィールドのフォーマット

<IPv4ヘッダフォーマット>

Ver	HLEN	Type Of Service	Total Length	
Identification			Flags	Fragment Offset
Time To Live	Protocol		Header Checksum	
Source IP Address				
Destination IP Address				

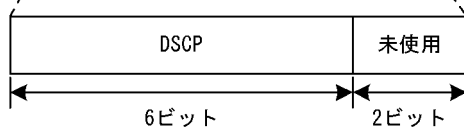
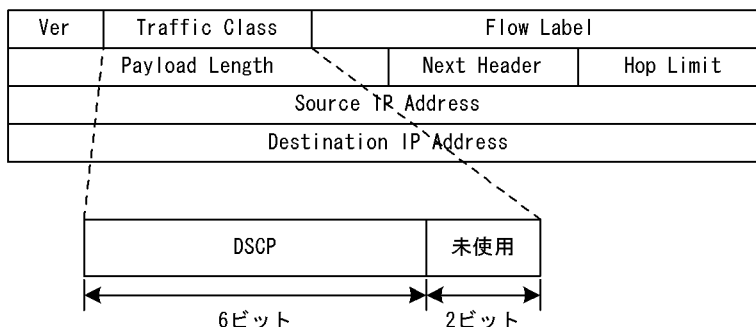


図 5-13 トラフィッククラスフィールドのフォーマット

<IPv6ヘッダフォーマット>



検出したフローの TOS フィールドまたはトラフィッククラスフィールドの上位 6 ビットを書き換えます。

5.7.3 マーカー使用時の注意事項

(1) 受信インタフェースおよび送信インタフェースにマーカーを指定したときの動作

送受信インタフェースにマーカーを実施するフロー検出を設定し、送受信インタフェースそれぞれに一致した場合は、送信側インタフェースのマーカーを適用し、フレームを送信します。

(2) マーカーできないフレーム

マーカーで書き換えができないフレームを次に示します。

本装置が自発的に送信するパケット / フレーム ¹

本装置でレイヤ 3 中継するパケット / フレームのうち次のパケット / フレーム

- IPv4 オプション付きのパケット ²
- 本装置でフラグメントして送信するフレーム ³
- IPv6 拡張ヘッダ (Hop by Hop) 付きのパケット ³
- ARP/NDP の未解決によって本装置に一時的に滞留し送信するフレーム ³

注 1 本装置が自発的に送信するパケット / フレームは、QoS フロー検出することができません。

注 2 IPv4 オプション付きのパケットは、QoS フロー検出することができません。

注 3 送信側インタフェースでは、QoS フロー検出することができません。

5.8 マーカーのコンフィグレーション

5.8.1 ユーザ優先度書き換えの設定

特定のフローに対してユーザ優先度を書き換える場合に設定します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出を行い、ユーザ優先度の書き換えを設定します。

[コマンドによる設定]

1. `(config)# ip qos-flow-list QOS-LIST1`
IPv4 QoS フローリスト (QOS-LIST1) を作成します。本リストを作成することによって、IPv4 QoS フローリストモードに移行します。
2. `(config-ip-qos)# qos ip any host 192.168.100.10 action replace-user-priority 6`
192.168.100.10 の IP アドレスを宛先とし、ユーザ優先度を 6 に書き換える IPv4 QoS フローリストを設定します。
3. `(config-ip-qos)# exit`
IPv4 QoS フローリスト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。
4. `(config)# interface vlan 10`
VLAN10 のインタフェースモードに移行します。
5. `(config-if)# ip qos-flow-group QOS-LIST1 out layer3-forwarding`
送信側にレイヤ 3 中継を対象とする IPv4 QoS フローリスト (QOS-LIST1) を有効にします。

5.8.2 DSCP 書き換えの設定

特定のフローに対して DSCP を書き換える場合に設定します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出を行い、DSCP 値の書き換えを設定します。

[コマンドによる設定]

1. `(config)# ip qos-flow-list QOS-LIST2`
IPv4 QoS フローリスト (QOS-LIST2) を作成します。本リストを作成することによって、IPv4 QoS フローリストモードに移行します。
2. `(config-ip-qos)# qos ip any host 192.168.100.10 action replace-dscp 63`
192.168.100.10 の IP アドレスを宛先とし、DSCP 値を 63 に書き換える IPv4 QoS フローリストを設定します。
3. `(config-ip-qos)# exit`
IPv4 QoS フローリスト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。

4. **(config)# interface vlan 20**

VLAN20 のインタフェースモードに移行します。

5. **(config-if)# ip qos-flow-group QOS-LIST2 in layer3-forwarding**

受信側にレイヤ 3 中継を対象とする IPv4 QoS フローリスト (QOS-LIST2) を有効にします。

5.9 マーカーのオペレーション

show qos-flow コマンドによって、設定した内容が反映されているかどうかを確認します。

5.9.1 ユーザ優先度書き換えの確認

ユーザ優先度書き換えの確認方法を次の図に示します。

図 5-14 ユーザ優先度書き換えの確認

```
> show qos-flow vlan 10 QOS-LIST1 out
Date 2006/03/01 12:00:00 UTC
Using Port: vlan 10 out
IP qos-flow-list:QOS-LIST1 layer3-forwarding
  ip any host 192.168.100.10 action replace-user-priority 6
  matched packets           :           74699826
```

QOS-LIST1 のリスト情報に「replace-user-priority 6」が表示されることを確認します。また、フロー検出条件に一致したフレームは matched packets で確認します。

5.9.2 DSCP 書き換えの確認

DSCP 書き換えの確認方法を次の図に示します。

図 5-15 DSCP 書き換えの確認

```
> show qos-flow vlan 10 QOS-LIST2 in
Date 2006/03/01 12:00:00 UTC
Using Port: vlan 10 in
IP qos-flow-list:QOS-LIST2 layer3-forwarding
  ip any host 192.168.100.10 action replace-dscp 63
  matched packets           :           0
```

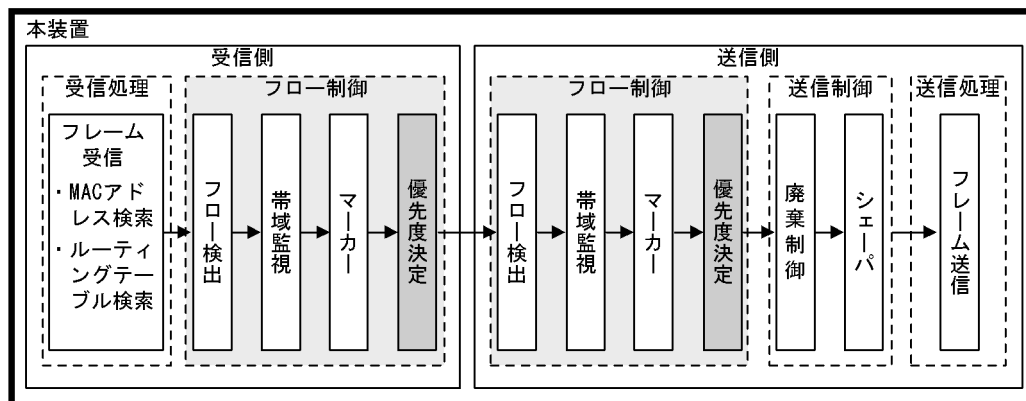
QOS-LIST2 のリスト情報に「replace-dscp 63」が表示されることを確認します。また、フロー検出条件に一致したフレームは matched packets で確認します。

5.10 優先度決定の解説

優先度決定は、本装置が中継するフレームおよび本装置が自発的に送信するフレームの優先度を決定する機能です。本機能には、検出したフロー単位で使用する出力優先度とキューイング優先度の直接指定、DSCP マッピング、階層化シェーパのユーザ指定、および NIF 単位で使用する VLAN ユーザマッピングの四つの機能があります。VLAN ユーザマッピングは送信側だけの機能です。

この節で説明する優先度決定の位置づけを次の図に示します。

図 5-16 優先度決定の位置づけ



(凡例) : この節で説明するブロック

優先度決定の各機能は、送信制御のシェーパの種類によって有効/無効が決まります。優先度決定とシェーパの対応を次の表に示します。フレームが送信される NIF のシェーパの種類を考慮して優先度決定を使用してください。

表 5-14 優先度決定とシェーパの対応

優先度決定の機能	設定単位	送信制御のシェーパの種類	
		レガシーシェーパ	階層化シェーパ
出力優先度とキューイング優先度の直接指定	フロー		
DSCP マッピング	フロー		
階層化シェーパのユーザ指定	フロー	-	
VLAN ユーザマッピング	NIF	-	

(凡例) : 有効 - : 無効

5.10.1 出力優先度とキューイング優先度の直接指定

検出したフローに対して、出力優先度およびキューイング優先度を直接指定する機能です。出力優先度は、フレームをどのキューにキューイングするかを示します。キューイング優先度は、キューイングする際の廃棄されやすさの度合いを示します。出力優先度は数字が大きいほど優先度が高く、キューイング優先度は数字が大きいほど廃棄されにくいことを示します。

出力優先度とキューイング優先度の指定範囲を次の表に示します。

表 5-15 出力優先度とキューイング優先度の指定範囲

項目	指定範囲
出力優先度	1 ~ 8
キューイング優先度	1 ~ 4

出力優先度と送信キューのマッピングの関係を次の表に示します。

表 5-16 出力優先度と送信キューの関係

出力優先度	送信時のキュー番号			
	8 キュー	4 キュー	2 キュー	1 キュー
1	1	1	1	1
2	2			
3	3	2		
4	4			
5	5	3	2	
6	6			
7	7	4		
8	8			

キューイング優先度と送信時の廃棄クラスの関係を示します。

表 5-17 キューイング優先度と送信時の廃棄クラスの関係

キューイング優先度	送信時の廃棄クラス
	4 クラス
1	1
2	2
3	3
4	4

注

送受信どちらのインターフェースに設定した場合も、ポート送信キューおよびディストリビューション送信キューに反映されます。ポート送信およびディストリビューション送信キューについては、「6.1.1 レガシーシェーパの概要」を参照してください。

5.10.2 DSCP マッピング

DSCP マッピングは、フレームの DSCP 値に応じて出力優先度とキューイング優先度を固定的に決定する機能です。DSCP 値は、TOS フィールドまたはトラフィッククラスフィールドの上位 6bit を意味します。

DSCP 値に対応する出力優先度とキューイング優先度を次の表に示します。

表 5-18 DSCP 値に対応する出力優先度とキューイング優先度

DSCP 値	出力優先度	キューイング優先度
0 ~ 7	1	4

DSCP 値	出力優先度	キューイング優先度
8 ~ 9	2	1
10 ~ 11		4
12 ~ 13		3
14 ~ 15		2
16 ~ 17	3	1
18 ~ 19		4
20 ~ 21		3
22 ~ 23		2
24 ~ 25	4	1
26 ~ 27		4
28 ~ 29		3
30 ~ 31		2
32 ~ 33	5	1
34 ~ 35		4
36 ~ 37		3
38 ~ 39		2
40 ~ 47	6	1
48 ~ 55	7	1
56 ~ 63	8	1

5.10.3 階層化シェーパのユーザ指定

検出したフローに対して、階層化シェーパのユーザを指定する機能です。指定するユーザはコンフィグレーションの階層化シェーパ情報と一致するように設定してください。

本機能を使用するためには、あらかじめコンフィグレーションの階層化シェーパ情報で、シェーパ自動設定機能またはシェーパモードのどちらかを設定する必要があります。どちらも設定しない場合は本機能を使用できません。ユーザ指定のために必要な階層化シェーパ情報を次の表に示します。

表 5-19 ユーザ指定のために必要な階層化シェーパ情報

ユーザ指定したフロー検出のインタフェース		ユーザ指定のために必要な階層化シェーパ情報
		シェーパモード、キュー数
受信側	イーサネット	装置内の NIF のうち、シェーパモードを設定した各 NIF のシェーパモード、キュー数をすべて同じ設定にしてください。
	VLAN	
送信側	イーサネット	該当イーサネットポートを含む NIF にシェーパモードを設定してください。
	VLAN	該当 VLAN に属するポートの NIF のうち、シェーパモードを設定した各 NIF のシェーパモード、キュー数をすべて同じ設定にしてください。

フレーム送信時の NIF が階層化シェーパ機能をサポートしていない場合、指定したユーザは無視されません。なお、出力優先度とキューイング優先度は適用されます。

フローで指定できるユーザの範囲を次の表に示します。ユーザの範囲は、シェーパ自動設定機能の設定情

報, または NIF ごとの階層化シェーパ情報によって決まります。

表 5-20 フローで指定できるユーザの範囲 (シェーパ自動設定機能のシェーパモード別)

モデル	シェーパ自動設定機能のシェーパモード	フローで指定できるユーザの範囲
AX6700S シリーズ共通	RGQ, WGQ	1 ~ 511
AX6600S シリーズ共通	LLPQ	1 ~ 255
AX6300S シリーズ共通	RGQ	1 ~ 255

注

範囲の上限は, シェーパ自動設定機能で設定したユーザ数 - 1 になります。例えば, シェーパ自動設定機能でユーザ数を 10 に設定した場合, フローで指定できるユーザの範囲は 1 ~ 9 になります。なお, シェーパ自動設定機能のユーザ数を 1 に設定した場合は, フローでユーザを指定できません。

表 5-21 フローで指定できるユーザの範囲 (NIF ごとの階層化シェーパ情報別)

モデル	NIF ごとの階層化シェーパ情報		フローで指定できるユーザの範囲
	モード	キュー数	
AX6700S シリーズ共通	RGQ, WGQ	8	1 ~ 511
AX6600S シリーズ共通		4	1 ~ 1023
	LLPQ1, LLPQ2	8	1 ~ 255
		4	1 ~ 511
	LLPQ4	8	1 ~ 255
AX6300S シリーズ共通	RGQ	8	1 ~ 255
		4	1 ~ 511

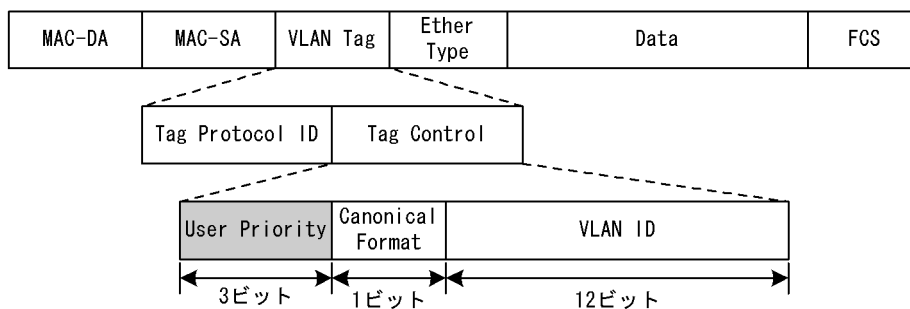
注

階層化シェーパのシェーパモードで LLRLQ オプションモードを設定している場合は, ユーザとして llrlq1 および llrlq2 を指定できます。この場合, ユーザ 1 および 2 は指定できません。

5.10.4 VLAN ユーザマッピング

VLAN ユーザマッピングは, 送信パケットの VLAN Tag 内にある VLAN ID とユーザ優先度 (User Priority) から階層化シェーパのユーザ ID と出力優先度を固定的に決定する機能です。VLAN Tag のヘッダフォーマットを次の図に示します

図 5-17 VLAN Tag のヘッダフォーマット



本機能を使用した場合、フロー検出によるユーザ ID と出力優先度の決定は無視されます。VLAN ID とユーザ ID のマッピングを次の表に示します。

表 5-22 VLAN ID とユーザ ID のマッピング

VLAN ID	マッピングされるユーザ	備考
Tag なし	デフォルトユーザ	-
0 ~ 4095	VLAN ID と一致するユーザ ID のユーザ	<ul style="list-style-type: none"> デフォルト VLAN (VLAN ID 0) はデフォルトユーザにマッピングされます。 LLRLQ オプションモード使用時は、VLAN ID 1 は LLRLQ1 に、VLAN ID 2 は LLRLQ2 に対応します。

(凡例) - : なし

注 2 段以上の VLAN Tag 付きフレームでは、1 段目の VLAN Tag を参照します。

ユーザ優先度と出力優先度のマッピングを次の表に示します。

表 5-23 ユーザ優先度と出力優先度のマッピング

ユーザ優先度	出力優先度
Tag なし	8
0	3
1	1
2	2
3	4
4	5
5	6
6	7
7	8

5.10.5 優先度決定のデフォルト動作

優先度決定が設定されていない場合は、次の表に示すデフォルト値で動作します。

表 5-24 優先度決定のデフォルト値

フレーム種別	デフォルト値		
	階層化シェーパのユーザ	出力優先度	キューイング優先度
フロー検出に一致して明示的に優先度を指定していない、かつ VLAN ユーザマッピングを使用していないフレーム	デフォルトユーザ	4	4
フロー検出に一致しない、かつ VLAN ユーザマッピングを使用していないフレーム	デフォルトユーザ	4	4

注

デフォルトユーザは、階層化シェーパのユーザの一つです。なお、優先度決定でデフォルトユーザを指定することはできません。

なお、次に示すフレームは、フロー制御の優先度決定の有無にかかわらず、固定的に優先度を決定します。

ただし、VLAN ユーザマッピングを使用した場合は、VLAN ユーザマッピングの動作に従います。

VLAN ユーザマッピング以外の優先度決定で変更できないフレームを次の表に示します。

表 5-25 VLAN ユーザマッピング以外の優先度決定で変更できないフレーム一覧

フレーム種別	固定的に決定される優先度		
	階層化シェーパの ユーザ	出力優先度	キューイング 優先度
本装置が自発的に送信するパケット/フレーム	1 ¹	8	4
本装置でレイヤ 3 中継するパケットのうち次のパケット <ul style="list-style-type: none"> • IPv4 オプション付きのパケット • 本装置でフラグメントし送信するパケット • IPv6 拡張ヘッダ (Hop by Hop) 付きのパケット • ARP/NDP の未解決によって本装置に一時的に滞留し送信するパケット 	デフォルトユーザ ²	4	4

注 1

階層化シェーパのシェーパモードで LLRLQ オプションモードを設定している場合は、LLRLQ1 になります。

注 2

デフォルトユーザは、階層化シェーパのユーザの一つです。

5.10.6 優先度決定使用時の注意事項

(1) 優先度決定での動作の優先順位

(a) 出力優先度とキューイング優先度の決定での優先順位

出力優先度とキューイング優先度は、直接指定、DSCP マッピング、または VLAN ユーザマッピングのどれかの動作で決定します。優先度を決定する場合の優先順位を次に示します。優先順位が高いのは、数字が小さい方です。

1. 装置に設定した、VLAN ユーザマッピング (送信側の NIF が階層化シェーパ機能をサポートしている場合)
2. 送信インタフェースに設定した、出力優先度とキューイング優先度の直接指定、または DSCP マッピング
3. 受信インタフェースに設定した、出力優先度とキューイング優先度の直接指定、または DSCP マッピング

(b) 階層化シェーパのユーザの決定での優先順位

階層化シェーパのユーザは、ユーザ指定または VLAN ユーザマッピングのどちらかの動作で決定します。ユーザを決定する場合の優先順位を次に示します。優先順位が高いのは、数字が小さい方です。

1. 装置に設定した、VLAN ユーザマッピング
2. 送信インタフェースに設定した、階層化シェーパのユーザ指定
3. 受信インタフェースに設定した、階層化シェーパのユーザ指定

(2) DSCP 書き換えと DSCP マッピングを同時に指定した場合の動作

受信インタフェースに DSCP 書き換えを実施するフロー検出、送信インタフェースに DSCP マッピング

を実施するフロー検出を設定し、送受信インタフェースそれぞれに一致した場合は、DSCP 書き換え後の DSCP 値に従って出力優先度とキューイング優先度を決定します。

(3) 直接指定と DSCP マッピングの動作

一つの受信または送信インタフェースに対して、直接指定と DSCP マッピングは同時に実施できません。

(4) NH1G-16S, NH1G-48T での優先度決定について【AX6300S】

本 NIF では、優先度決定はサポートしていません。

(5) 階層化シェーパで設定されていないユーザ宛てフレームについて

フレーム送信時の NIF が階層化シェーパ機能をサポートしていても、優先度決定で決定されたユーザが階層化シェーパで設定されていない場合、送信制御のシェーパでフレームが廃棄されます。

(6) VLAN ユーザマッピングのサポート NIF

階層化シェーパ機能をサポートしている NIF でサポートしています。

「6.10.2 階層化シェーパ機能サポート NIF」を参照してください。

(7) VLAN ユーザマッピングと VLAN 拡張機能の Tag 変換を併用した場合の動作

Tag 変換によって変換された VLAN ID と一致するユーザ ID にマッピングされます。

(8) フロー検出拡張モードでの DSCP マッピング

advance qos-flow-list をインタフェースに適用した場合、その QoS エントリは非 IP パケットおよび IP パケットの両方をフロー検出の対象にします。しかし、動作に DSCP マッピングを設定した QoS エントリは、IP パケットだけをフロー検出の対象にします。そのため、非 IP パケットはフロー検出の対象外となり、統計情報はカウントされません。

5.11 優先度決定コンフィグレーション

5.11.1 出力優先度の設定

特定のフローに対して出力優先度を設定します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出を行い、出力優先度を設定します。

[コマンドによる設定]

1. `(config)# ip qos-flow-list QOS-LIST1`
IPv4 QoS フローリスト (QOS-LIST1) を作成します。本リストを作成することによって、IPv4 QoS フローリストモードに移行します。
2. `(config-ip-qos)# qos ip any host 192.168.100.10 action priority-class 6`
192.168.100.10 の IP アドレスを宛先とし、出力優先度 = 6 の IPv4 QoS フローリストを設定します。
3. `(config-ip-qos)# exit`
IPv4 QoS フローリスト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。
4. `(config)# interface vlan 10`
VLAN10 のインタフェースモードに移行します。
5. `(config-if)# ip qos-flow-group QOS-LIST1 out layer2-forwarding`
送信側にレイヤ 2 中継を対象とする IPv4 QoS フローリスト (QOS-LIST1) を有効にします。

5.11.2 DSCP マッピングの設定

特定のフローに対して DSCP マッピングによって出力優先度を設定します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出を行い、DSCP マッピングによって出力優先度を設定します。

[コマンドによる設定]

1. `(config)# ip qos-flow-list QOS-LIST1`
IPv4 QoS フローリスト (QOS-LIST1) を作成します。本リストを作成することによって、IPv4 QoS フローリストモードに移行します。
2. `(config-ip-qos)# qos ip any host 192.168.100.10 action dscp-map`
192.168.100.10 の IP アドレスを宛先とし、DSCP マッピングによって出力優先度を決定するフローリストを設定します。
3. `(config-ip-qos)# exit`
IPv4 QoS フローリスト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。
4. `(config)# interface vlan 20`

VLAN20 のインタフェースモードに移行します。

5. (config-if)# ip qos-flow-group QOS-LIST1 out layer3-forwarding
送信側にレイヤ 3 中継を対象とする IPv4 QoS フローリスト (QOS-LIST1) を有効にします。

5.11.3 フローに対するユーザの設定

特定のフローに対してユーザを設定します。

階層化シェーパでユーザを設定します。フローに対するユーザでは、階層化シェーパで設定したユーザと同じユーザを設定します。

(1) 階層化シェーパのユーザ設定

[設定のポイント]

ユーザ帯域制御、スケジューリングを設定したユーザリストを作成し、ポート 1/8 に対して設定します。

[コマンドによる設定]

1. (config)# shaper user-list USER-LIST1 1 peak-rate 10M min-rate 5M weight 1 pq
ユーザリスト (USER-LIST1) を作成します。最大帯域 10Mbps, 最低帯域 5Mbps, 重み 1, スケジューリング (PQ) を設定します。
2. (config)# interface gigabitethernet 1/8
ポート 1/8 のインタフェースモードに移行します。
3. (config-if)# shaper user 10 list USER-LIST1
ユーザ ID 10 にユーザリスト (USER-LIST1) を指定し、ユーザ ID 10 を有効にします。

(2) フロー制御の優先度決定でのユーザ指定

[設定のポイント]

フレーム送信時に宛先 IP アドレスによってフロー検出を行い、階層化シェーパ情報で有効にしたユーザを指定します。

[コマンドによる設定]

1. (config)# ip qos-flow-list QOS-LIST1
IPv4 QoS フローリスト (QOS-LIST1) を作成します。本リストを作成することによって、IPv4 QoS フローリストモードに移行します。
2. (config-ip-qos)# qos ip any host 192.168.100.10 action user 10
192.168.100.10 の IP アドレスを宛先とし、ユーザ ID 10 の IPv4 QoS フローリストを設定します。
3. (config-ip-qos)# exit
IPv4 QoS フローリストモードからグローバルコンフィギュレーションモードに戻ります。
4. (config)# interface gigabitethernet 1/8
ポート 1/8 のインタフェースモードに移行します。

5. フロー制御

5. (config-if)# ip qos-flow-group QOS-LIST1 out layer2-forwarding

送信側にレイヤ 2 中継を対象とする IPv4 QoS フローリスト (QOS-LIST1) を有効にします。

5.11.4 VLAN ユーザマッピングの設定

VLAN ユーザマッピングを設定します。

[設定のポイント]

VLAN ユーザマッピングをサポートしているすべての NIF では、VLAN Tag のヘッダ情報に基づきユーザ ID と出力優先度が決まります。

[コマンドによる設定]

1. (config)# shaper vlan-user-map

VLAN ユーザマッピングを設定します。

5.12 優先度のオペレーション

5.12.1 優先度の確認

回線にトラフィック（宛先 IP アドレスが 192.168.100.10 のフレーム）を注入している状態で、show qos queueing interface コマンドによってキューイングされているキュー番号を確認します。対象のイーサネットインタフェースは、ポート 1/11 です。

図 5-18 優先度の確認

```
> show qos queueing interface 1/11 outbound
Date 2007/11/01 12:00:00 UTC
NIF1/Port11 (outbound)
Max_Queue=8, Rate=100Mbit/s, Schedule_mode=pq
Queue1: Qlen=0, Peak_Qlen=0, Limit_Qlen=255, Drop_mode=tail_drop
  discard      send_pkt      discard_pkt      send_byte
  1             0             0             0
  2             0             0             0
  3             0             0             0
  4             0             0             0
  total        0             0             0
      :
Queue6: Qlen=0, Peak_Qlen=2, Limit_Qlen=255, Drop_mode=tail_drop
  discard      send_pkt      discard_pkt      send_byte
  1             2564          0             125.5M
  2             0             0             0
  3             0             0             0
  4             0             0             0
  total        2564          0             125.5M
      :
Queue8: Qlen=0, Peak_Qlen=0, Limit_Qlen=255, Drop_mode=tail_drop
  discard      send_pkt      discard_pkt      send_byte
  1             0             0             0
  2             0             0             0
  3             0             0             0
  4             0             0             0
  total        0             0             0
>
```

Queue6 の Qlen の値がカウントされていることを確認します。

なお、この表示例は、NIF 種別の NK1G-24S または NH1G-24S の例です。

5.12.2 階層化シェーパのユーザの確認

回線にトラフィック（宛先 IP アドレスが 192.168.100.10 のフレーム）を注入している状態で、show shaper コマンドによってキューイングされている階層化シェーパのユーザを確認します。対象のイーサネットインタフェースは、ポート 1/8 です。

図 5-19 ユーザの確認

```

> show shaper 1/8 user 10
Date 2008/06/24 12:00:00 UTC
NIF 1/Port 8, Shaper_mode:RGQ
Set_default_user_priority:disable
Predicted_tail_drop:enable, Vlan_user_map:disable
Port Rate_limit=1000000kbit/s

User:ID=10, USER-LIST1
Schedule_mode=pq
Peak_rate=10Mbit/s, Min_rate=5Mbit/s, Weight=1
Queue      send_pkt      discard_pkt  Queue_length
1           0              0           0/ 0/ 120
2           0              0           0/ 0/ 120
3           0              0           0/ 0/ 100
4           0              0           0/ 0/ 100
5           0              0           0/ 0/ 80
6           23091811       0           1/ 63/ 80
7           0              0           0/ 0/ 50
8           0              0           0/ 0/ 50
total      23091811       0           0/ 0/ -
>

```

User ID 10 の send_pkt の値がカウントされていることを確認します。

なお、この表示例は、NIF 種別の NK1GS-8M の例です。

5.12.3 VLAN ユーザマッピングの確認

show shaper all コマンドによって VLAN ユーザマッピングが有効になっている NIF を確認します。

図 5-20 VLAN ユーザマッピングの確認

```

> show shaper all
Date 2008/06/24 12:00:00 UTC
NIF 1/Port 1, Shaper_mode:RGQ
Set_default_user_priority:disable
Predicted_tail_drop:disable, Vlan_user_map:enable
Port Rate_limit=1Gbit/s
Buffer
QoS1= 194/ 1812/ 2000 QoS2= 82/ 1784/ 2000
QoS3= 74/ 1582/ 1500 QoS4= 71/ 1422/ 1500
QoS5= 68/ 1398/ 1500 QoS6= 61/ 1284/ 1500
QoS7= 51/ 1231/ 1000 QoS8= 41/ 1098/ 1000
:
:
>

```

NIF1 に対して VLAN ユーザマッピングが有効になっていることを確認します。

6

送信制御

この章では本装置の送信制御（シェーパおよび廃棄制御）について説明します。

-
- 6.1 レガシーシェーパ解説

 - 6.2 レガシーシェーパのコンフィグレーション

 - 6.3 レガシーシェーパのオペレーション

 - 6.4 階層化シェーパの解説

 - 6.5 階層化シェーパのコンフィグレーション

 - 6.6 階層化シェーパのオペレーション

 - 6.7 廃棄制御解説

 - 6.8 廃棄制御のコンフィグレーション

 - 6.9 廃棄制御のオペレーション

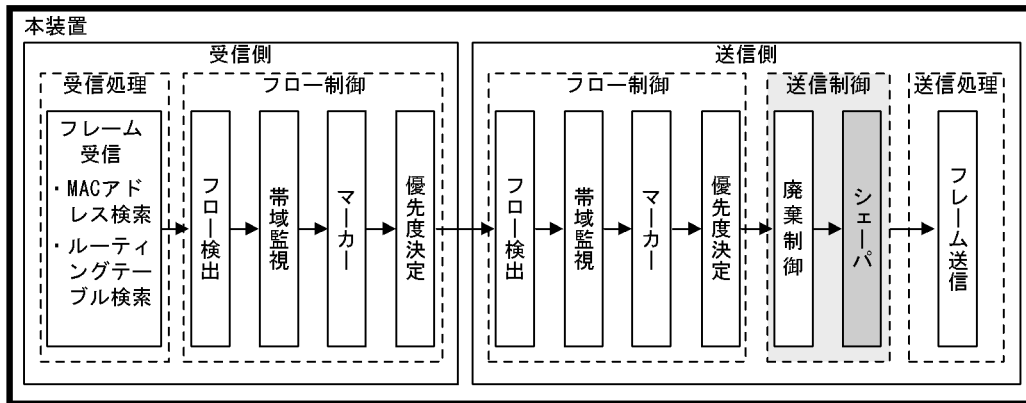
 - 6.10 NIF 種別と送信制御機能との対応
-


6.1 レガシーシェーパ解説

6.1.1 レガシーシェーパの概要

シェーパは、各キューからのフレームの出力順序、および各ポートの出力帯域を制御する機能です。この節で説明するシェーパの位置づけを次の図に示します。

図 6-1 シェーパの位置づけ

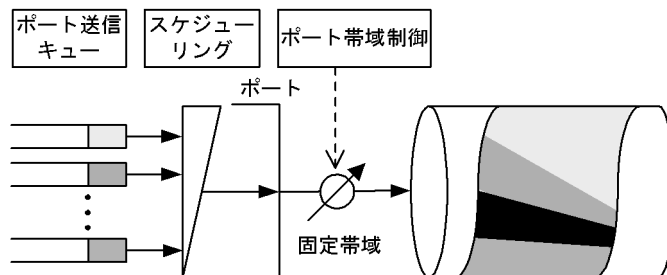


(凡例)  : この節で説明するブロック

レガシーシェーパには NIF 種別に応じて、ポート送信キューを備えたレガシーシェーパと、ポート送信キューおよびディストリビューション送信キューを備えたレガシーシェーパの 2 種類があります。ディストリビューション送信キューを搭載する NIF 種別については、「6.10 NIF 種別と送信制御機能との対応」を参照してください。レガシーシェーパの機能は、どのキューにあるフレームを次に送信するかを決めるスケジューリングおよびイーサネットインタフェースの帯域をシェーピングするポート帯域制御から構成されます。

レガシーシェーパの概念を次の図に示します。

図 6-2 レガシーシェーパ (ポート送信キューを搭載) の概念




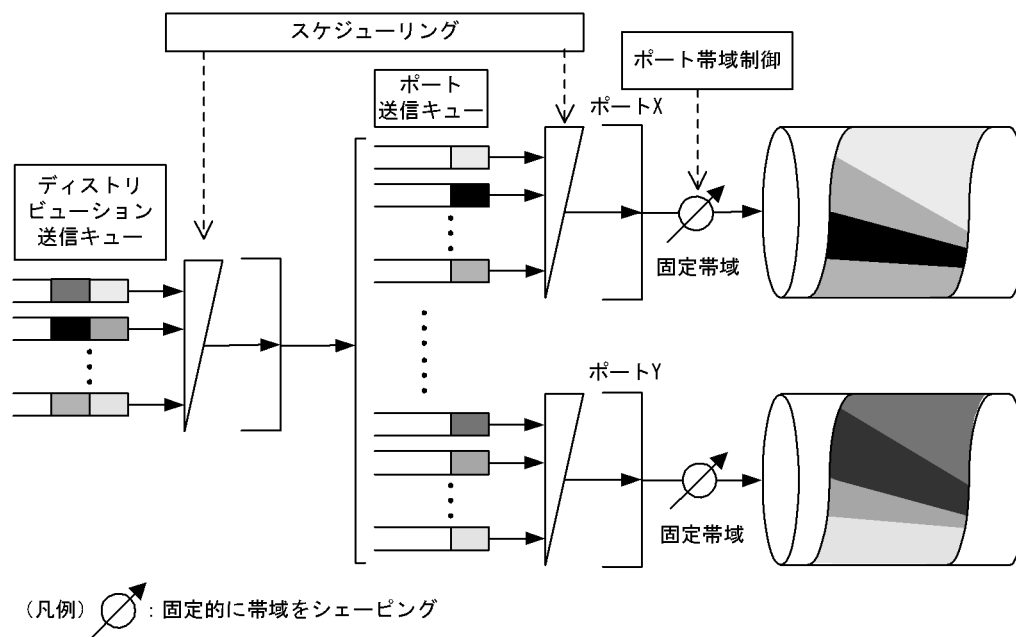
(凡例)  : 固定的に帯域をシェーピング

図 6-3 レガシーシェーパ (ポート送信キューおよびディストリビューション送信キューを搭載) の概念



ディストリビューション送信キューのスケジューリングによって、ディストリビューション送信キューにキューイングされたフレームを、ポートXからポートYのポート送信キューに分配します。

6.1.2 スケジューリング

スケジューリングは、各キューに積まれたフレームをどのような順序で送信するかを制御する機能です。本装置では、次に示すスケジューリング機能があります。スケジューリングの動作説明および仕様を次の表に示します。

表 6-1 スケジューリングの動作説明

スケジューリング種別	概念図	動作説明	適用例
PQ	<p>Q#8 Q#7 Q#6 Q#5 Q#4 Q#3 Q#2 Q#1</p> <p>高 低</p>	完全優先制御。複数のキューにフレームがキューイングされている場合、優先度の高いキューから常にフレームを送出します。	トラフィック優先順を完全に遵守する場合
RR	<p>Q#8 Q#7 Q#6 Q#5 Q#4 Q#3 Q#2 Q#1</p>	ラウンドロビン。複数のキューにフレームが存在する場合、順番にキューを見ながら1フレームずつ送出します。フレーム長によらず、フレーム数が均等になる制御を行います。	フレーム数を元に全トラフィックを均等とする場合

スケジューリング種別	概念図	動作説明	適用例
4PQ + 4WFQ		4 最優先キュー + 4 重み付き帯域均等制御。キュー 8, 7, 6, 5(左図 Q#8, Q#7, Q#6, Q#5) までを完全優先制御で行います。キュー 8 から 5 にフレームが存在しない場合、予め設定した帯域の比 (w:x:y:z) に応じてキュー 4, 3, 2, 1(左図 Q#4, Q#3, Q#2, Q#1) からフレームを送出します。	PQ に優先順を完全に遵守するトラフィック WFQ に PQ の余剰帯域を用いて、帯域の比を適用するトラフィック
2PQ+4WFQ+2BEQ		2 最優先キュー + 4 重み付き帯域均等制御 + 2Best Effort。キュー 8, 7(左図 Q#8, Q#7) を完全優先制御で行います。キュー 8, 7 にフレームが存在しない場合、予め設定した帯域の比 (w:x:y:z) に応じてキュー 6, 5, 4, 3(左図 Q#6, Q#5, Q#4, Q#3) からフレームを送出します。キュー 8 から 3 までにフレームが存在しない場合、キュー 2, 1(左図 Q#2, Q#1) で完全優先制御を行います。	PQ に優先順を完全に遵守するトラフィック WFQ に PQ の余剰帯域を用いて、帯域の比を適用するトラフィック BEQ に PQ, WFQ の余剰帯域を用いるトラフィック
4WFQ+4BEQ		4 重み付き帯域均等制御 + 4Best Effort。キュー 8, 7, 6, 5(左図 Q#8, Q#7, Q#6, Q#5) で予め設定した帯域の比 (w:x:y:z) に応じてフレームを送出します。キュー 8 から 5 にフレームが存在しない場合、キュー 4, 3, 2, 1(左図 Q#4, Q#3, Q#2, Q#1) で完全優先制御を行います。	WFQ に帯域の比を適用したトラフィック BEQ に WFQ の余剰帯域を用いるトラフィック

表 6-2 スケジューリングの仕様

項目		仕様	内容
キュー数	PQ RR	1,2,4,8 キュー	NIF 種別によって、1, 2, 4, 8 キューのキュー数を指定できます。キュー数を変更することで、キュー長を拡張できます。キュー数を変更すると該当ポートが再起動します。NIF 種別との対応については、「6.10 NIF 種別と送信制御機能との対応」を参照してください。
	4PQ+4WFQ 2PQ+4WFQ+2BEQ 4WFQ+4BEQ	8 キュー	8 キュー固定。
4WFQ の 重み	4PQ+4WFQ 2PQ+4WFQ+2BEQ 4WFQ+4BEQ	1 ~ 100%	4WFQ の重みとして帯域の比 (w:x:y:z) を次の条件を満たすように設定してください。 w x y z かつ w+x+y+z=100

(1) ポート送信キューのスケジューリング

ポート送信キューのスケジューリングは NIF 種別により選択可能な種類が異なります。NIF 種別との対応については、「6.10 NIF 種別と送信制御機能との対応」を参照してください。廃棄制御はテールドロップで動作します。テールドロップの詳細については、「6.7.1 廃棄制御」を参照してください。

(2) ディストリビューション送信キューのスケジューリング

ディストリビューション送信キューのスケジューリングは PQ 固定、キュー数を 8 固定、廃棄制御をテ-

ルドロップで動作します。テールドロップの詳細については、「6.7.1 廃棄制御」を参照してください。

ディストリビューション送信キューにキューイングされたフレームは、優先度の高いキューからポート送信キューへキューイングされます。このため、ディストリビューション送信キューに滞留が発生すると、ポート送信キューのスケジューリング動作でPQ以外を選択していてもPQの優先順で送信されます。

6.1.3 キュー数指定

キュー数指定は、ポート送信キューのキュー数を変更することによってキュー長を拡張する機能です。キュー長とは、一つのキューにキューイングできるフレーム数のことです。通常の8キューから4キュー、2キュー、1キューに変更すると、1キューに割り当てるキュー長を拡張できます。

キュー数指定によるキュー長の変化を次の表に示します。

表 6-3 ポート送信キューのキュー数指定時のキュー長【AX6700S】【AX6600S】

NIF 種別	キュー数ごとのキュー長			
	8 キュー時	4 キュー時	2 キュー時	1 キュー時
NK1G-24T	256	512	1024	2048
NK1G-24S	256	512	1024	2048
NK1GS-8M	512	-	-	-
NK10G-4RX	512	1024	2048	4096
NK10G-8RX	512	1024	2048	4096

(凡例) - : キュー数が指定できないため対象外

表 6-4 ポート送信キューのキュー数指定時のキュー長【AX6300S】

NIF 種別	キュー数ごとのキュー長			
	8 キュー時	4 キュー時	2 キュー時	1 キュー時
NH1G-16S	256	-	-	-
NH1G-24T	256	512	1024	2048
NH1G-24S	256	512	1024	2048
NH1G-48T	256	-	-	-
NH1GS-6M	2048	-	-	-
NH10G-1RX	2048	-	-	-
NH10G-4RX	512	1024	2048	4096
NH10G-8RX	512	1024	2048	4096

(凡例) - : キュー数が指定できないため対象外

6.1.4 ポート帯域制御

ポート帯域制御は、スケジューリングを実施したあとに該当ポートに指定した送信帯域にシェーピングする機能です。この制御を使用して、広域イーサネットサービスへ接続できます。

例えば、ポート帯域が1Gbit/sでISPとの契約帯域が400Mbit/sの場合、ポート帯域制御機能を使用してあらかじめ帯域を400Mbit/s以下に抑えてフレームを送信することができます。

6. 送信制御

ポート帯域制御は NIF 種別により設定可否が異なります。NIF 種別との対応については、「6.10 NIF 種別と送信制御機能との対応」を参照してください。

回線種別に対するポート帯域制御の帯域範囲と設定単位を次の表に示します。

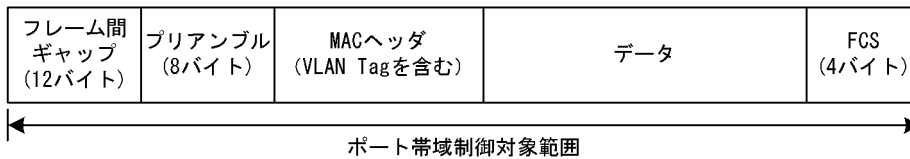
表 6-5 ポート帯域制御の仕様

回線速度 (オートネゴシエーション結果も含む)	設定範囲	刻み値
10Gbit/s	1G ~ 10Gbit/s	1Gbit/s
	100M ~ 1Gbit/s	100Mbit/s
1Gbit/s	1Gbit/s	1Gbit/s
	10M ~ 1Gbit/s	10Mbit/s
100Mbit/s	1M ~ 100Mbit/s	1Mbit/s
10Mbit/s	1M ~ 10Mbit/s	1Mbit/s
	300K ~ 10Mbit/s	100Kbit/s

注 全二重モードの場合だけポート帯域制御が動作します

ポート帯域制御の対象となるフレームの範囲は、フレーム間ギャップから FCS までです。ポート帯域制御の対象範囲を次の図に示します。

図 6-4 ポート帯域制御の対象範囲



6.2 レガシーシェーパのコンフィグレーション

6.2.1 スケジューリングの設定

[設定のポイント]

スケジューリングを設定した QoS キューリスト情報を作成し、該当するポートに設定します。

[コマンドによる設定]

1. (config)# qos-queue-list QLIST-PQ pq
QoS キューリスト情報 (QLIST-PQ) にスケジューリング (PQ) を設定します。
2. (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。
3. (config-if)# qos-queue-group QLIST-PQ
QoS キューインタフェース情報に QoS キューリスト名称を指定し、QoS キューリスト情報を有効にします。

6.2.2 キュー数指定の設定

[設定のポイント]

キュー数指定を設定した QoS キューリスト情報を作成し、該当するポートに設定します。なお、キュー数指定ができるスケジューリングは、PQ (完全優先制御) または RR (ラウンドロビン) です。

[コマンドによる設定]

1. (config)# qos-queue-list QLIST-PQ-QNUM4 pq number_of_queue_4
QoS キューリスト名称 (QLIST-PQ-QNUM4) のスケジューリングを pq, キュー数 4 に設定します。
2. (config)# interface gigabitethernet 1/11
ポート 1/11 のインタフェースモードに移行します。
3. (config-if)# qos-queue-group QLIST-PQ-QNUM4
QoS キューインタフェース情報に QoS キューリスト名称を指定し、QoS キューリスト情報を有効にします。

6.2.3 ポート帯域制御の設定

該当するポートの出力帯域を、実回線の帯域より低くする場合に設定します。

[設定のポイント]

該当するポート (100Mbit/s) に対し、ポート帯域制御による帯域の設定 (20Mbit/s) を行います。

[コマンドによる設定]

1. (config)# interface gigabitethernet 1/13

6. 送信制御

ポート 1/13 のインタフェースモードに移行します。

2. `(config-if)# speed 100`

`(config-if)# duplex full`

該当するポートの回線速度を 100Mbit/s に設定します。

3. `(config-if)# traffic-shape rate 20M`

ポート帯域を 20Mbit/s に設定します。

6.3 レガシーシェーパのオペレーション

show qos queueing interface コマンドによって、イーサネットインタフェースに設定したレガシーシェーパの内容を確認します。

6.3.1 スケジューリングの確認

スケジューリングの確認方法を次の図に示します。

図 6-5 スケジューリングの確認

```
> show qos queueing interface 1/1 outbound

Date 2006/08/01 12:00:00 UTC
NIF1/Port1 (outbound)
Max_Queue=8, Rate=100Mbit/s, Schedule_mode=pq ... 1
Queue1: Qlen=0, Peak_Qlen=0, Limit_Qlen=255, Drop_mode=tail_drop
  discard      send_pkt      discard_pkt      send_byte
  1             2248             0                 452.0k
  2             0              0                 0
  3             0              0                 0
  4             0              0                 0
  total        2248             0                 452.0k
      :
      :
Queue8: Qlen=0, Peak_Qlen=0, Limit_Qlen=255, Drop_mode=tail_drop
  discard      send_pkt      discard_pkt      send_byte
  1             0              0                 0
  2            1528             0                231.0k
  3             0              0                 0
  4             0              0                 0
  total        1528             0                231.0k
```

1. Schedule_mode パラメータの内容が、設定したスケジューリング（この例では、pq）になっていることを確認します。

なお、この表示例は、NIF 種別の NK1G-24S または NH1G-24S の例です。

6.3.2 キュー数指定の確認

キュー数指定の確認方法を次の図に示します。

図 6-6 キュー数指定の確認

```
> show qos queueing interface 1/11 outbound

Date 2006/08/01 12:00:00 UTC
NIF1/Port11 (outbound)
Max_Queue=4, Rate=100Mbit/s, Schedule_mode=pq ... 1
Queue1: Qlen=0, Peak_Qlen=0, Limit_Qlen=255, Drop_mode=tail_drop
discard      send_pkt      discard_pkt      send_byte
1             6225                0                125.5M
2             0                   0                0
3             0                   0                0
4             0                   0                0
total        6225                0                125.5M
:
:
Queue4: Qlen=0, Peak_Qlen=0, Limit_Qlen=255, Drop_mode=tail_drop
discard      send_pkt      discard_pkt      send_byte
1             0                0                0
2            1575                0                145.0k
3             0                0                0
4             0                0                0
total        1575                0                145.0k
```

1. Max_Queue パラメータの内容が、指定したキュー数（この例では、4）になっていることを確認します。

なお、この表示例は、NIF 種別の NK1G-24S または NH1G-24S の例です。

6.3.3 ポート帯域制御の確認

ポート帯域制御の確認方法を次の図に示します。

図 6-7 ポート帯域制御の確認

```
> show qos queueing interface 1/13 outbound

Date 2006/08/01 12:00:00 UTC
NIF1/Port13 (outbound)
Max_Queue=8, Rate=20Mbit/s, Schedule_mode=pq ... 1
Queue1: Qlen=0, Peak_Qlen=0, Limit_Qlen=255, Drop_mode=tail_drop
discard      send_pkt      discard_pkt      send_byte
1            2248                0                452.0k
2             0                0                0
3             0                0                0
4             0                0                0
total        2248                0                452.0k
:
:
Queue8: Qlen=0, Peak_Qlen=0, Limit_Qlen=255, Drop_mode=tail_drop
discard      send_pkt      discard_pkt      send_byte
1             0                0                0
2            1528                0                231.0k
3             0                0                0
4             0                0                0
total        1528                0                231.0k
```

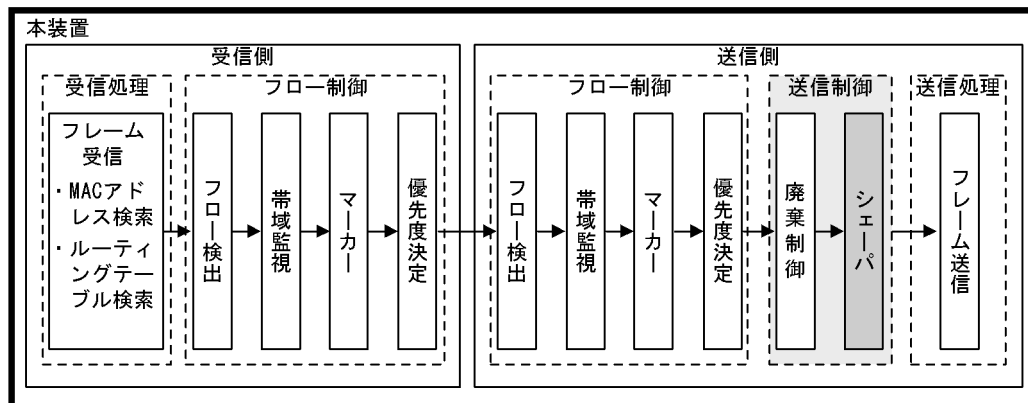
1. Rate パラメータの内容が、指定した帯域値（この例では、20Mbit/s）になっていることを確認します。

なお、この表示例は、NIF 種別の NK1G-24S または NH1G-24S の例です。

6.4 階層化シェーパの解説

シェーパは、各キューからのフレームの出力順序、および各ポートの出力帯域を制御する機能です。この節で説明するシェーパの位置づけを次の図に示します。

図 6-8 シェーパの位置づけ



(凡例) : この節で説明するブロック

階層化シェーパとは、次の二つの制御を同時に行う機能です。

- インタフェースから出力するトラフィックを絞りながら、そのトラフィックをユーザごとに帯域制御をする。
- 音声やデータなどのユーザパケットに応じた優先制御をする。

これによって、ユーザごとの帯域を守りながら、音声パケットなどを通常パケットよりも優先的に送信して、低い遅延率を実現できます。

階層化シェーパは、レガシーシェーパのディストリビューション送信キュー、ポート送信キューに加えて、多数のユーザキューを備えています。ポート送信キューは、レガシーシェーパと異なり、NIF ごとに一つのキュー制御となります。ユーザキューは複数のユーザキューをまとめたユーザという制御単位のキュー制御となります。

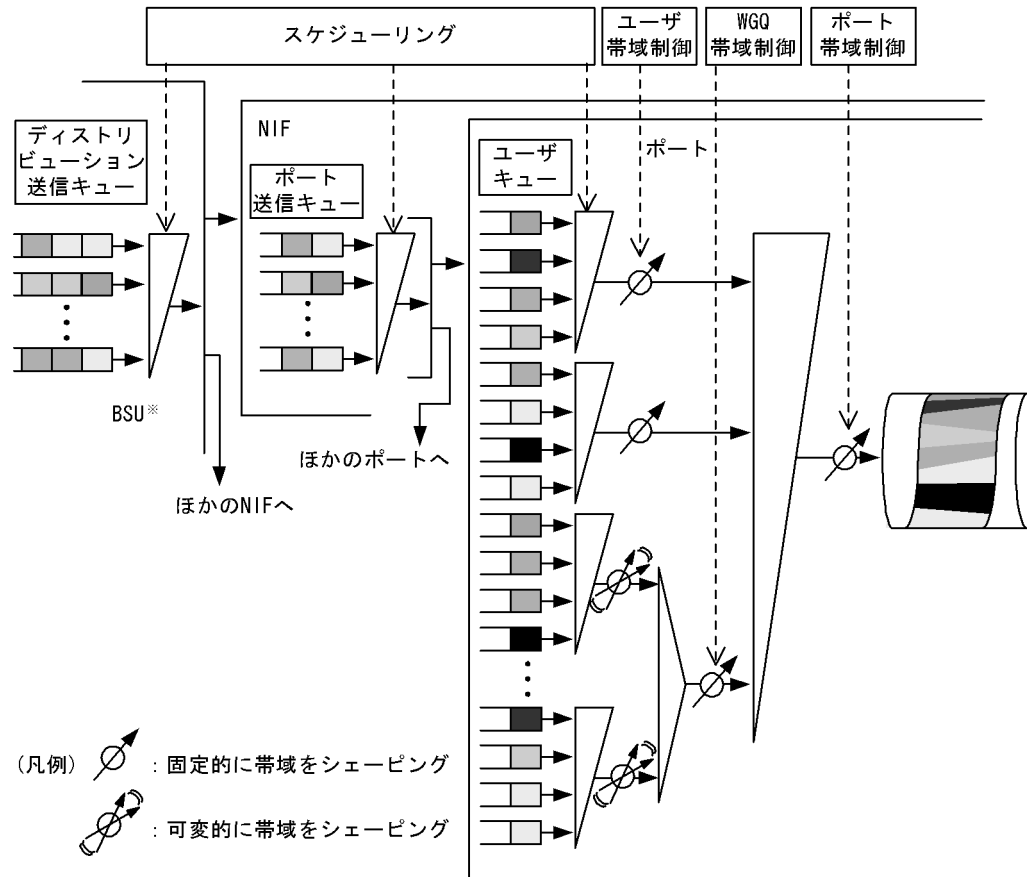
階層化シェーパは、トラフィックに適した帯域制御方式をシェーパモードで決定し、次に示す三つの機能で実現します。

- ユーザのユーザキューごとのフレームの送信順を制御するスケジューリング
- ユーザから送信されるフレーム量を制御するユーザ帯域制御
- 1 ポートのすべてのユーザから送信されるフレーム量を制御するポート帯域制御

階層化シェーパを使用できる NIF 種別については、「6.10 NIF 種別と送信制御機能との対応」を参照してください。また、階層化シェーパにはこれらの機能を簡単に設定するためのシェーパ自動設定機能があります。

階層化シェーパの概念を次の図に示します。

図 6-9 階層化シェーパの概念



注※ AX6700Sの場合BSU, AX6600Sの場合CSU, AX6300Sの場合MSUです。

6.4.1 シェーパモード

シェーパモードを設定することで、NIFごとにユーザキューの帯域制御方式が決まり、シェーパ機能が有効になります。シェーパモードを設定するときは、同時にユーザ帯域制御を設定してください。シェーパ機能が有効になったNIFのポートにユーザ帯域制御を設定していない場合、該当ポートからフレームが送信されません。ユーザ帯域制御については、「6.4.3 階層化シェーパの帯域制御」を参照してください。

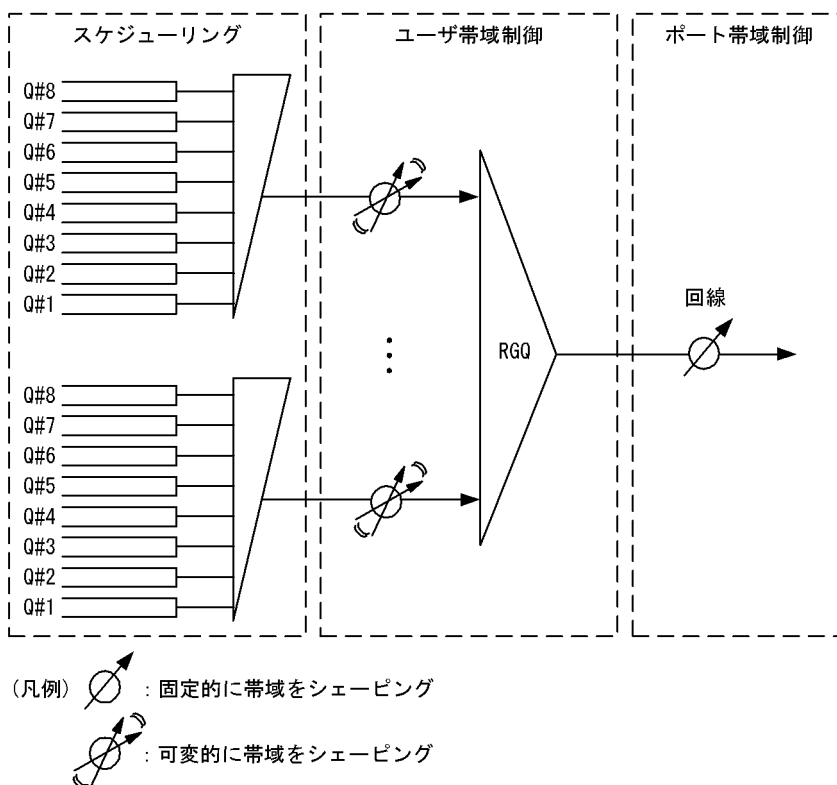
シェーパモードには、RGQ、WGQ、LLPQ1、LLPQ2、およびLLPQ4の五つのモードとLLRLQオプションモードがあります。LLRLQオプションモードは、五つのモードと併用します。指定できるシェーパモードはNIF種別によって異なります。また、シェーパモードを変更すると該当NIFが再起動します。NIF種別との対応については、「6.10 NIF種別と送信制御機能との対応」を参照してください。次にそれぞれのモードについて説明します。

(1) RGQ

RGQはユーザごとの最低帯域を保証するモードです。余剰帯域がある場合は最大帯域まで使用できます。ユーザ間で出力優先度は均等です。各ユーザには設定した最低帯域が分配されます。分配後に余剰帯域がある場合は、ユーザごとの重みによって余剰帯域が分配されます。

また、ユーザの最大帯域と最低帯域を同じ値に設定した場合、固定帯域として動作します。RGQの概念を次の図に示します。

図 6-10 RGQ の概念



RGQ の帯域の計算例を次の表に示します。この表ではポート帯域制御によって回線帯域を 900Mbit/s にシェーピングする場合を想定します。

表 6-6 RGQ の帯域の計算例

ユーザ	入力帯域 (Mbit/s)	最低帯域 (Mbit/s)	最大帯域 (Mbit/s)	重み	余剰帯域 (Mbit/s) ¹	送信帯域 (Mbit/s) ²
ユーザ 1	500	200	800	3	150	350
ユーザ 2	350	200	800	2	100	300
ユーザ 3	250	200	800	1	50	250

注 1

$$\begin{aligned} \text{回線内の余剰帯域} &= \text{回線帯域} - \text{各ユーザの最低帯域の合計} \\ &= 900 - (200 + 200 + 200) = 300 \text{ (Mbit/s)} \end{aligned}$$

$$\text{ユーザ 1 の余剰帯域} = 300 \times (3 \div (3 + 2 + 1)) = 150 \text{ (Mbit/s)}$$

$$\text{ユーザ 2 の余剰帯域} = 300 \times (2 \div (3 + 2 + 1)) = 100 \text{ (Mbit/s)}$$

$$\text{ユーザ 3 の余剰帯域} = 300 \times (1 \div (3 + 2 + 1)) = 50 \text{ (Mbit/s)}$$

注 2

$$\begin{aligned} \text{各ユーザの送信帯域 (最大帯域以下)} \\ &= \text{各ユーザの最低帯域} + \text{各ユーザに分配された余剰帯域} \end{aligned}$$

$$\text{ユーザ 1 の送信帯域} = 200 + 150 = 350 \text{ (Mbit/s)}$$

$$\text{ユーザ 2 の送信帯域} = 200 + 100 = 300 \text{ (Mbit/s)}$$

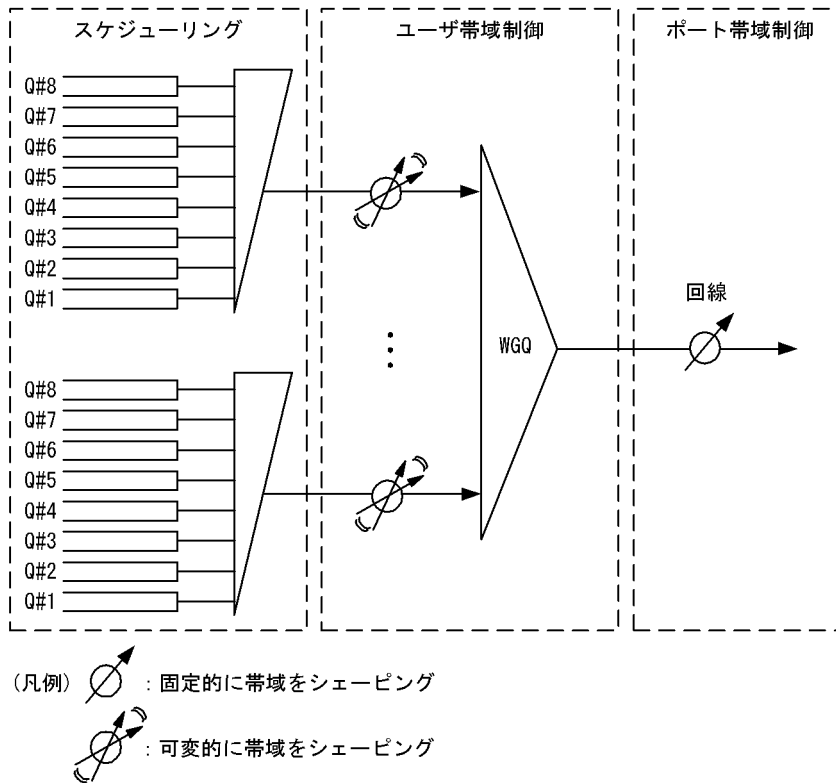
$$\text{ユーザ 3 の送信帯域} = 200 + 50 = 250 \text{ (Mbit/s)}$$

(2) WGQ

WGQ はユーザ間での帯域比率を保証するモードです。ユーザ間で出力優先度は均等です。各ユーザには設定した重みによって帯域が分配されます。

WGQ の概念を次の図に示します。

図 6-11 WGQ の概念



WGQ の帯域の計算例を次の表に示します。この表ではポート帯域制御によって回線帯域を 900Mbit/s にシェーピングする場合を想定します。

表 6-7 WGQ の帯域の計算例

ユーザ	入力帯域 (Mbit/s)	重み	送信帯域 (Mbit/s)
ユーザ 1	500	3	450
ユーザ 2	350	2	300
ユーザ 3	250	1	150

注

ユーザ 1 の送信帯域 = $900 \times (3 \div (3 + 2 + 1)) = 450$ (Mbit/s)

ユーザ 2 の送信帯域 = $300 \times (2 \div (3 + 2 + 1)) = 300$ (Mbit/s)

ユーザ 3 の送信帯域 = $300 \times (1 \div (3 + 2 + 1)) = 150$ (Mbit/s)

(3) LLPQ

LLPQ1, LLPQ2, および LLPQ4 の 3 モードは LLPQ 方式で帯域制御します。LLPQ は RGQ と同様にユーザごとの最低帯域を保証し、余剰帯域がある場合は最大帯域まで使用できます。RGQ との違いは、す

すべてのユーザのユーザキューより優先的に出力できる低遅延キューを備え、その低遅延キューに対して帯域を制限できる LLPQ 帯域制御を備えている点です。これによって、あるユーザの優先する必要があるデータが、別ユーザの通常データで遅延するのを防ぎます。なお、ユーザ間の低遅延キューの出力優先度は均等です。低遅延キュー以外のユーザキューについても同様です。

LLPQ 帯域は該当ユーザの最大帯域まで設定できます。ただし、ユーザごとの最低帯域を常に保証するには、回線内のすべてのユーザで LLPQ 帯域を最低帯域以下に設定する必要があります。また、すべてのユーザの低遅延キューは、低遅延キュー以外のユーザキューより優先的に帯域が割り当てられます。

低遅延キューに対して入力帯域がある場合、LLPQ 帯域を上限として入力分の帯域が低遅延キューに割り当てられます。

低遅延キューに割り当てた帯域が最低帯域以下の場合、最低帯域から低遅延キューに割り当てた帯域を引いた帯域がユーザキューに割り当てられます。分配後に余剰帯域がある場合は、ユーザごとの重みに従って余剰帯域がユーザキューに分配されます。

LLPQ 帯域に最低帯域以上を設定した場合、優先度の高いデータを広帯域で使用できます。また、パスト性を持つトラフィックも低遅延で送信できます。

最低帯域が保証されない例を次の表に示します。なお、ポート帯域制御および各ユーザの最大帯域は 1Gbit/s とします。低遅延キューに対する各ユーザの入力帯域は、ユーザ 1 が 700Mbit/s、ユーザ 2 がなしです。ユーザキューに対する各ユーザの入力帯域は、ユーザ 1 がなし、ユーザ 2 が 700Mbit/s です。

表 6-8 最低帯域が保証されない例

ユーザ	低遅延キューに対する 入力帯域 (Mbit/s)	通常キューに対する 入力帯域 (Mbit/s)	LLPQ 帯域の 設定値 (Mbit/s)	最低帯域の設 定値 (Mbit/s)	送信帯域 (Mbit/s)
ユーザ 1	700	-	600	500	600
ユーザ 2	-	700			400

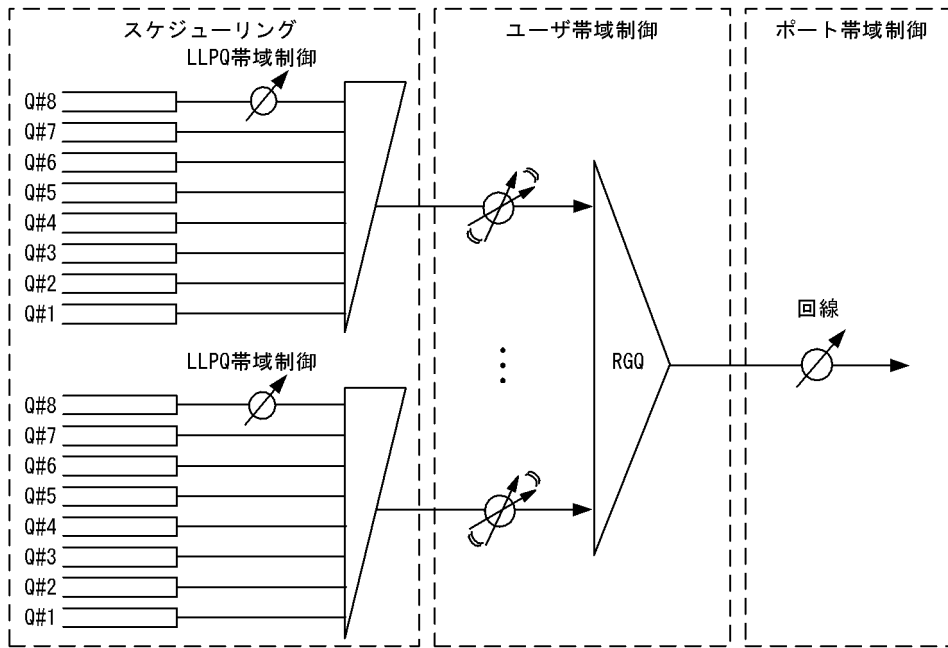
(凡例) - : なし


この場合、LLPQ 帯域が 600Mbit/s なので、入力帯域のあるユーザ 1 に 600Mbit/s を割り当てます。ユーザ 1 は低遅延キューに最低帯域を超える 600Mbit/s を割り当てているため、ユーザキューに割り当てる帯域がありません。ユーザ 2 は低遅延キューに割り当てた帯域がないため、最低帯域の 500Mbit/s をユーザキューに割り当てようとしています。しかし、未使用の帯域が 400Mbit/s しかないため、ユーザキューに対して割り当てられる帯域は 400Mbit/s です。このため、ユーザ 2 の送信帯域は、設定した最低帯域以下の 400Mbit/s になります。


なお、LLPQ1、LLPQ2、および LLPQ4 のシェーパモード名の数値は、低遅延キューの数を示しています。同時に、スケジューリング種別で、低遅延キュー数以上の PQ 数がある種別を選択することを意味します。例えば、LLPQ4 は各ユーザの出力優先度の高いユーザキューの四つが低遅延キューになるモードで、スケジューリングとして PQ が四つ以上ある PQ または 4PQ+4WFQ を選択できます。

LLPQ1、LLPQ2、LLPQ4 の各概念を次の図に示します。

図 6-12 LLPQ1 の概念

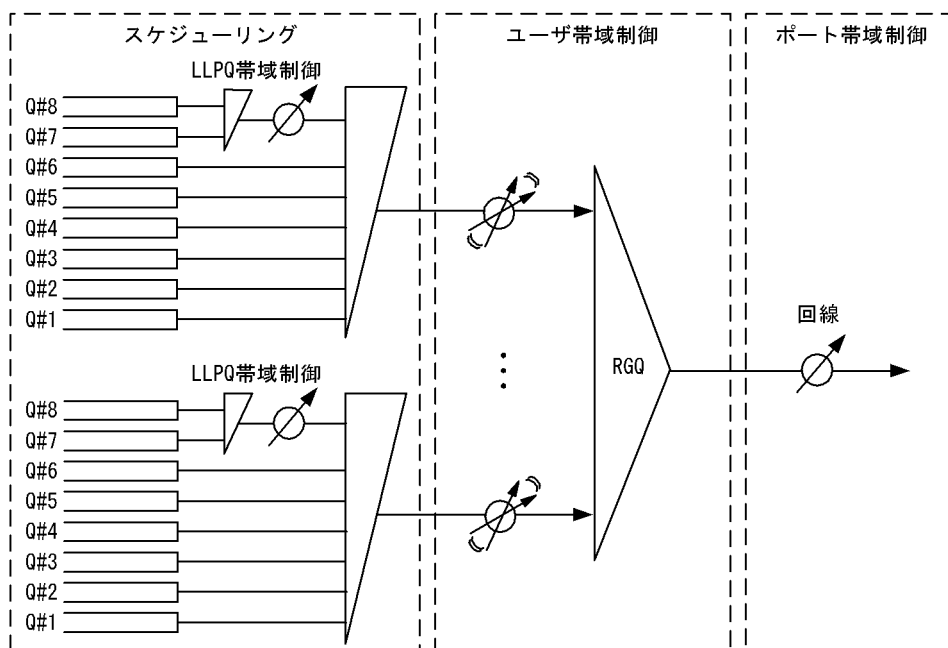



(凡例)  : 固定的に帯域をシェーピング


 : 可変的に帯域をシェーピング

注 Q#8が低遅延キューとなります。Q#1~7はユーザキューです。

図 6-13 LLPQ2 の概念

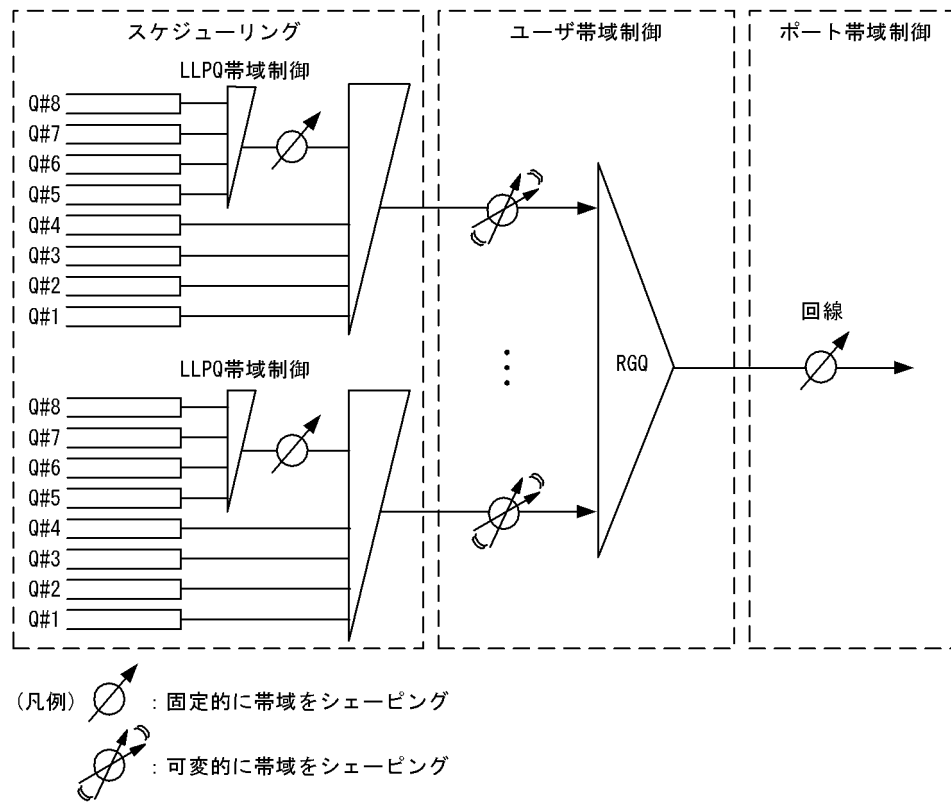


(凡例)  : 固定的に帯域をシェーピング

 : 可変的に帯域をシェーピング

注 Q#7およびQ#8が低遅延キューとなります。Q#1～6はユーザキューです。

図 6-14 LLPQ4 の概念



注 Q#5~8が低遅延キューとなります。Q#1~4はユーザキューです。

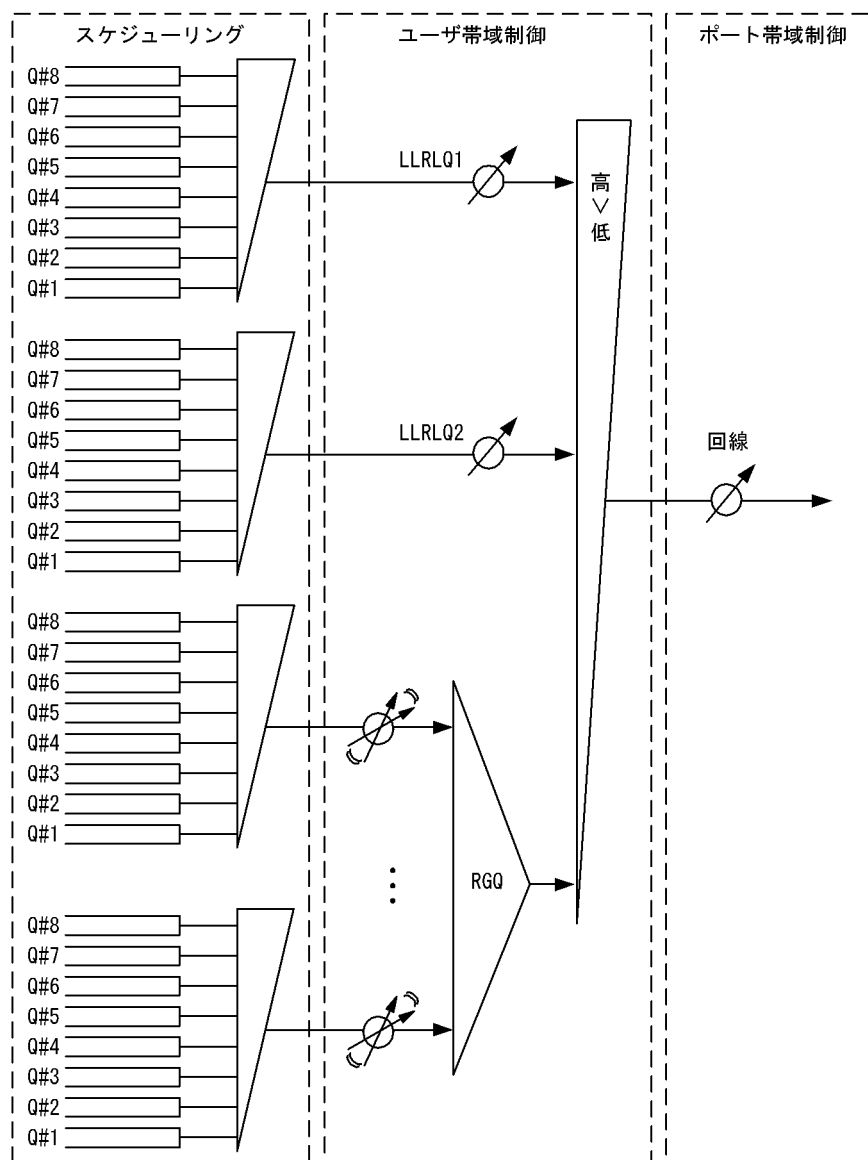
(4) LLRLQ


LLRLQ は、RGQ、WGQ、LLPQ1、LLPQ2、および LLPQ4 の各シェーパーモードにオプションとして指定できるモードです。LLRLQ オプションモードを指定した場合、基本のシェーパーモードの帯域制御とは異なる独立した最優先出力の 2 ユーザ (LLRLQ1、LLRLQ2) を使用できます。


LLRLQ1 および LLRLQ2 には、それぞれに設定した最大帯域が割り当てられます。基本のシェーパーモードのユーザには LLRLQ1 および LLRLQ2 が使用していない帯域が、各モードの帯域分配方法に基づいて割り当てられます。

LLRLQ オプション付き RGQ の概念を次の図に示します。

図 6-15 LLRLQ オプション付き RGQ の概念



(凡例)  : 固定的に帯域をシェーピング

 : 可変的に帯域をシェーピング

LLRLQ オプション付き RGQ の帯域の計算例を次の表に示します。この表ではポート帯域制御によって回線帯域を 900Mbit/s にシェーピングする場合を想定します。

表 6-9 LLRLQ オプション付き RGQ の帯域の計算例

ユーザ	入力帯域 (Mbit/s)	最低帯域 (Mbit/s)	最大帯域 (Mbit/s)	重み	未使用帯域 (Mbit/s) ¹	余剰帯域 (Mbit/s) ²	送信帯域 (Mbit/s)
LLRLQ1	100	-	200	-	-	-	100 ³
LLRLQ2	200	-	150	-		-	150 ³
RGQ ユーザ 1	650	200	700	2	650	200	400 ⁴

6. 送信制御

ユーザ	入力帯域 (Mbit/s)	最低帯域 (Mbit/s)	最大帯域 (Mbit/s)	重み	未使用帯域 (Mbit/s) ¹	余剰帯域 (Mbit/s) ²	送信帯域 (Mbit/s)
ユーザ 2	400	150	700	1		100	250 ⁴

注 1

RGQ ユーザに割り当てられる未使用帯域
 = 回線帯域 - (LLRLQ1 の送信帯域 + LLRLQ2 の送信帯域)
 = 900 - 100 - 150 = 650 (Mbit/s)

注 2

RGQ ユーザの余剰帯域
 = RGQ ユーザに割り当てられる未使用帯域 - 各ユーザの最低帯域の合計値
 = 650 - (200 + 150) = 300 (Mbit/s)
 RGQ ユーザ 1 の余剰帯域 = 300 × (2 ÷ (2 + 1)) = 200 (Mbit/s)
 RGQ ユーザ 2 の余剰帯域 = 300 × (1 ÷ (2 + 1)) = 100 (Mbit/s)

注 3

LLRLQ1 および LLRLQ2 の送信帯域は次のどちらかの値です。
 入力帯域 最大帯域の場合：入力帯域
 入力帯域 > 最大帯域の場合：最大帯域

注 4

RGQ と同様です。

6.4.2 階層化シェーパのスケジューリング

(1) スケジューリングの動作説明

スケジューリングは、各キューに積まれたフレームをどのような順序で送信するかを制御する機能です。階層化シェーパでは制御するキュー数を NIF 単位で設定します。キュー数は 8 キューと 4 キューが選択でき、それぞれ使用できるスケジューリングが異なります。また、キュー数を変更すると該当 NIF が再起動します。キュー数ごとのスケジューリングの動作説明と、VLLQ および WFQ の重みの仕様を次の表に示します。

表 6-10 8 キュー時のスケジューリングの動作説明

スケジューリング種別	概念図	動作説明	適用例
PQ		完全優先制御。複数のキューにフレームがキューイングされている場合、優先度の高いキューから常にフレームを送信します。	トラフィック優先順を完全に遵守する場合

スケジューリング種別	概念図	動作説明	適用例
2PQ+VLLQ+4WFQ+BEQ (3PQ+4WFQ+BEQ)		<p>2 最優先キュー + 可変低遅延キュー + 4 重み付き帯域均等制御 + 2Best Effort。キュー 8, 7 (左図 Q#8, Q#7) を完全優先制御で行います。キュー 8, 7 にフレームが存在しない場合、キュー 6 (左図 Q#6) にあらかじめ設定した比率分の帯域を割り当てフレームを送信します。さらに、キュー 6 の余剰帯域をあらかじめ設定した帯域の比 ($w:x:y:z$) に応じてキュー 5, 4, 3, 2 (左図 Q#5, Q#4, Q#3, Q#2) からフレームを送信します。キュー 8, 7 と 5 から 2 までにフレームが存在しない場合、キュー 1 (左図 Q#1) で完全優先制御を行います。VLLQ の比率を 100% とした場合は 3PQ+4WFQ+BEQ で動作します。</p>	<p>PQ に優先順を完全に遵守させたいトラフィック、VLLQ に PQ の余剰帯域に対して設定した割合を使用し優先的に出力したいトラフィック、WFQ に PQ、VLLQ の余剰帯域を設定した割合で使用し、均等な優先度で出力したいトラフィック、BEQ に PQ、VLLQ、WFQ の余剰帯域がある場合に出力するトラフィック</p>
4PQ+4WFQ		<p>4 最優先キュー + 4 重み付き帯域均等制御。キュー 8, 7, 6, 5 (左図 Q#8, Q#7, Q#6, Q#5) までを完全優先制御で行います。キュー 8 から 5 にフレームが存在しない場合、あらかじめ設定した帯域の比 ($w:x:y:z$) に応じてキュー 4, 3, 2, 1 (左図 Q#4, Q#3, Q#2, Q#1) からフレームを送信します。</p>	<p>PQ に優先順を完全に遵守するトラフィック、WFQ に PQ の余剰帯域を使用して、帯域の比を適用するトラフィック</p>
2PQ+4WFQ+2BEQ		<p>2 最優先キュー + 4 重み付き帯域均等制御 + 2Best Effort。キュー 8, 7 (左図 Q#8, Q#7) を完全優先制御で行います。キュー 8, 7 にフレームが存在しない場合、あらかじめ設定した帯域の比 ($w:x:y:z$) に応じてキュー 6, 5, 4, 3 (左図 Q#6, Q#5, Q#4, Q#3) からフレームを送信します。キュー 8 から 3 までにフレームが存在しない場合、キュー 2, 1 (左図 Q#2, Q#1) で完全優先制御を行います。</p>	<p>PQ に優先順を完全に遵守するトラフィック、WFQ に PQ の余剰帯域を使用して、帯域の比を適用するトラフィック、BEQ に PQ、WFQ の余剰帯域を使用するトラフィック</p>

表 6-11 4 キュー時のスケジューリングの動作説明

スケジューリング種別	概念図	動作説明	適用例
PQ		<p>完全優先制御。複数のキューにフレームがキューイングされている場合、優先度の高いキューから常にフレームを送信します。</p>	<p>トラフィック優先順を完全に遵守する場合</p>

スケジューリング種別	概念図	動作説明	適用例
VLLQ+3WFQ (PQ+3WFQ)		<p>可変低遅延キュー + 3重み付き帯域均等制御。キュー 4 (左図 Q#4) にあらかじめ設定した比率分の帯域を割り当てフレームを送信します。キュー 4 の余剰帯域をあらかじめ設定した帯域の比 (x:y:z) に応じてキュー 3, 2, 1 (左図 Q#3, Q#2, Q#1) からフレームを送信します。VLLQ の比率を 100%とした場合は PQ+3WFQ で動作します。</p>	<p>VLLQ にユーザ帯域に対して設定した割合の帯域を使用し優先的に出力したいトラフィック、WFQ に VLLQ の余剰帯域を設定した割合で使用し、均等な優先度で出力させたいトラフィック</p>
4WFQ		<p>設定した帯域の比 (w:x:y:z) に応じてキュー 4, 3, 2, 1 (左図 Q#4, Q#3, Q#2, Q#1) からフレームを送信します。</p>	<p>トラフィックごとに設定した割合で帯域を使用し、均等な優先度で出力したい場合</p>
PQ+VLLQ+2WFQ (2PQ+2WFQ)		<p>最優先キュー + 可変低遅延キュー + 2重み付き帯域均等制御。キュー 4 (左図 Q#4) を完全優先制御で行います。キュー 4 にフレームが存在しない場合、キュー 3 (左図 Q#3) にあらかじめ設定した比率分の帯域を割り当てフレームを送信します。さらに、キュー 3 の余剰帯域をあらかじめ設定した帯域の比 (x:y) に応じてキュー 2, 1 (左図 Q#2, Q#1) からフレームを送信します。VLLQ の比率を 100%とした場合は 2PQ+2WFQ で動作します。</p>	<p>PQ に優先順を完全に遵守させたいトラフィック、VLLQ に PQ の余剰帯域に対して設定した割合を使用し優先的に出力したいトラフィック、WFQ に PQ, VLLQ の余剰帯域を設定した割合で使用し、均等な優先度で出力したいトラフィック</p>

表 6-12 VLLQ および WFQ の重みの仕様

項目	仕様	内容
VLLQ の重み	5 ~ 100%	5 刻みで設定できます。100%を設定した場合、VLLQ は PQ として動作します。
WFQ の重み	1 ~ 100%	<p>帯域の比としての重みの設定です。各 WFQ の値が次の条件を満たすように設定してください。</p> <ul style="list-style-type: none"> キュー番号の小さいキューの重み値が、キュー番号の大きいキューの重み値を超えないこと 各 WFQ の重み値の合計が 100 以下になること <p>例：VLLQ+3WFQ の場合 $x \quad y \quad z$, かつ $x + y + z = 100$</p>

(2) シェーパモードとスケジューリング

シェーパモードごとに設定できるスケジューリングが異なります。各シェーパモードで設定できるスケジューリングを次の表に示します。なお、LLPQ4 モードは 8 キュー制御でだけ使用できます。

表 6-13 8 キュー時のシェーパモードで設定できるスケジューリング

スケジューリング	シェーパモード					
	RGQ	WGQ	LLPQ1	LLPQ2	LLPQ4	LLRLQ
PQ						
2PQ+VLLQ+4WFQ+BEQ					-	

スケジューリング	シェーパモード					
	RGQ	WGQ	LLPQ1	LLPQ2	LLPQ4	LLRLQ
2PQ+4WFQ+2BEQ					-	
4PQ+4WFQ						

(凡例) : 設定できる - : 設定できない

注 LLRLQ1, LLRLQ2 に対してのスケジューリングを指しています。

表 6-14 4 キュー時のシェーパモードで設定できるスケジューリング

スケジューリング	シェーパモード				
	RGQ	WGQ	LLPQ1	LLPQ2	LLRLQ ¹
PQ					
VLLQ+3WFQ			2	-	
4WFQ			-	-	
PQ+VLLQ+2WFQ				2	

(凡例) : 設定できる - : 設定できない

注 1 LLRLQ1, LLRLQ2 に対してのスケジューリングを指しています。

注 2 VLLQ の重みを 100% に設定してください。

(3) キュー種別とスケジューリング

階層化シェーパはキュー種別によって指定できるスケジューリングが異なります。次にキュー種別ごとのスケジューリングについて説明します。

(a) ユーザキューのスケジューリング

ユーザキューのスケジューリングは NIF ごとに設定したシェーパモードとキュー数で異なります。また、すべてのスケジューリングで廃棄制御はテールドロップで動作します。テールドロップの詳細については、「6.7.1 廃棄制御」を参照してください。

(b) ポート送信キューのスケジューリング

ポート送信キューのスケジューリングは PQ 固定、キュー数は NIF ごとの設定で異なります。廃棄制御はテールドロップで動作します。テールドロップの詳細については、「6.7.1 廃棄制御」を参照してください。

(c) ディストリビューション送信キューのスケジューリング

ディストリビューション送信キューのスケジューリングは PQ 固定、キュー数は 8 固定です。廃棄制御はテールドロップで動作します。テールドロップの詳細については、「6.7.1 廃棄制御」を参照してください。

6.4.3 階層化シェーパの帯域制御

階層化シェーパには、ユーザ帯域制御、WGQ 帯域制御、およびポート帯域制御があります。

(1) ユーザ帯域制御

ユーザ帯域制御は、ユーザ内のすべてのユーザキューの送信帯域をシェーピングする機能です。ユーザ帯

域制御の方式は、ユーザ種別や該当ユーザの所属している NIF のシェーパモードによって異なります。ユーザの種別、ユーザ帯域制御の設定条件、およびユーザ帯域制御値の仕様を次の表に示します。

表 6-15 ユーザの種別

ユーザ種別	回線当たりのユーザ数	内容
LLRLQ1 ¹	1	帯域の割り当て、出力優先度共にポート内で最優先のユーザ。
LLRLQ2	1	LLRLQ1 の次に優先度の高いユーザ。
ユーザ ^{1 2}	最大 1023	通常のユーザ。ユーザ間の帯域分配、出力優先度はシェーパモードによって異なります。
デフォルトユーザ	1	フロー検出条件で検出されないフレームおよび優先度によるユーザキューの指定をしていないフレームがキューイングされるユーザ。

注 1

LLRLQ1 またはユーザ ID1 のユーザには、本装置が自発的に送信するフレームがキューイングされます。

注 2

装置種別で最大値が異なります。詳細は、マニュアル「コンフィグレーションガイド Vol.1 3.2 AX6700S の収容条件【AX6700S】」、「コンフィグレーションガイド Vol.1 3.4 AX6600S の収容条件【AX6600S】」または「コンフィグレーションガイド Vol.1 3.6 AX6300S の収容条件【AX6300S】」のフィルタ・QoS の階層化シェーパを参照してください。

表 6-16 ユーザ帯域制御の設定条件

シェーパモード	ユーザ種別	帯域制御パラメータの設定条件
RGQ	ユーザ, デフォルトユーザ	<ul style="list-style-type: none"> 最大帯域 ポート帯域 最低帯域 最大帯域 該当ポートの全ユーザ、デフォルトユーザの最低帯域の合計 ポート帯域
LLRLQ オプション付き RGQ	LLRLQ1, LLRLQ2	LLRLQ1, LLRLQ2 の最大帯域と全ユーザ、デフォルトユーザの最低帯域の合計 ポート帯域
	ユーザ, デフォルトユーザ	<ul style="list-style-type: none"> 最大帯域 ポート帯域 最低帯域 最大帯域 LLRLQ1, LLRLQ2 の最大帯域と全ユーザ、デフォルトユーザの最低帯域の合計 ポート帯域
WGQ	ユーザ, デフォルトユーザ	なし
LLRLQ オプション付き WGQ	LLRLQ1, LLRLQ2	LLRLQ1, LLRLQ2 の最大帯域の合計 ポート帯域
	ユーザ, デフォルトユーザ	なし
LLPQ (LLPQ1, LLPQ2, LLPQ4)	ユーザ, デフォルトユーザ	<ul style="list-style-type: none"> 最大帯域 ポート帯域 最低帯域 最大帯域 LLPQ 帯域 最大帯域 該当ポートの全ユーザ、デフォルトユーザの最低帯域の合計 ポート帯域
LLRLQ オプション付き LLPQ (LLPQ1, LLPQ2, LLPQ4)	LLRLQ1, LLRLQ2	LLRLQ1, LLRLQ2 の最大帯域と全ユーザ、デフォルトユーザの最低帯域の合計 ポート帯域

シェーパモード	ユーザ種別	帯域制御パラメータの設定条件
	ユーザ, デフォルトユーザ	<ul style="list-style-type: none"> 最大帯域 ポート帯域 最低帯域 最大帯域 LLPQ 帯域 最大帯域 LLRLQ1, LLRLQ2 の最大帯域と全ユーザ, デフォルトユーザの最低帯域の合計 ポート帯域

表 6-17 ユーザ帯域制御値の仕様

帯域制御パラメータ	帯域制御値
最大帯域	64kbit/s ~ 1000Mbit/s
最低帯域	64kbit/s ~ 1000Mbit/s
LLPQ 帯域	64kbit/s ~ 1000Mbit/s
重み	1 ~ 50

注 WGQ のユーザに指定する場合, 1 ~ 10 になります。

各ユーザは, ポートごとにユニークなユーザ ID を持っています。このユーザ ID と出力優先度によって, サービス (フロー) に適したユーザ帯域制御とスケジューリングを行っているユーザのユーザキューが特定できます。ユーザ ID は, NIF 種別, シェーパモード, およびキュー数によって使用できる値が異なります。NIF ごとに指定できるユーザ ID の範囲を次の表に示します。

表 6-18 NK1GS-8M でシェーパモードごとに指定できるユーザ ID の範囲

シェーパモード	キュー数	ユーザ ID の指定範囲
RGQ, WGQ	8	1 ~ 511
	4	1 ~ 1023
LLPQ1, LLPQ2	8	1 ~ 255
	4	1 ~ 511
LLPQ4	8	1 ~ 255

注

ユーザ ID 0 はデフォルトユーザが使用します。LLRLQ オプション使用時はユーザ ID 1 は LLRLQ1, ユーザ ID 2 は LLRLQ2 が使用するため, 指定できません。

表 6-19 NH1GS-6M でシェーパモードごとに指定できるユーザ ID の範囲

シェーパモード	キュー数	ユーザ ID の指定範囲
RGQ	8	1 ~ 255
	4	1 ~ 511

注

ユーザ ID 0 はデフォルトユーザが使用します。

ユーザ帯域制御の対象となるフレームの範囲は, フレーム間ギャップから FCS までです。ユーザ帯域制御の対象範囲を次の図に示します。

また、ポート帯域制御の対象となるフレームの範囲は、ユーザ帯域制御と同じです。

6.4.4 シェーパ自動設定機能

本機能は、シェーパモードとユーザ数の設定だけで階層化シェーパを簡単に使用する機能です。シェーパ自動設定機能のモードパラメータごとの設定内容を次の表に示します。

表 6-22 シェーパ自動設定機能のモードパラメータごとの設定内容

シェーパ自動設定機能のモードパラメータ		rgq	wgq	llpq
シェーパモード		RGQ	WGQ	LLPQ1
キュー数		8	8	8
最大ユーザ数 ^{1 2}		512 ³	512	256
ポート	帯域制御値	1Gbit/s	1Gbit/s	1Gbit/s
	QoS ごとのバッファ値	デフォルト値 ⁴	デフォルト値 ⁴	デフォルト値 ⁴
ユーザ	最大帯域	最低帯域 × 10 ⁵	-	最低帯域 × 10 ⁵
	最低帯域 ⁶	1Gbit/s ÷ ユーザ数	-	1Gbit/s ÷ ユーザ数
	LLPQ 帯域制御値	-	-	最低帯域 ÷ 2
	重み	1	1	1
	スケジューリング	PQ	PQ	4PQ+4WFQ (10:20:30:40)
	キュー長	デフォルト値 ⁴	デフォルト値 ⁴	デフォルト値 ⁴
	廃棄モード	tail-drop2	tail-drop2	tail-drop2

(凡例) - : 設定なし

注 1

ユーザ数は、コンフィグレーションコマンドで指定します。デフォルトユーザ (ユーザ ID 0) から指定ユーザ数 - 1 番のユーザ ID のユーザまでを割り当てられます。最小ユーザ数は 1 です。

注 2

VLAN ユーザマッピングと併用する場合は、次の条件を満たすように設定してください。
装置で設定している VLAN インタフェースの最大 VLAN ID < シェーパ自動設定機能の最大ユーザ数

注 3

NH1GS-6M の場合、指定できるシェーパモードは RGQ だけで、256 ユーザまでとなります。

注 4

デフォルト値については「6.7.2 バッファ管理」を参照してください。

注 5

ポート帯域制御の最大帯域を超える場合は、ポート帯域制御の最大帯域と同じ値になります。

注 6

WGQ モード以外では、ユーザに均等に帯域を割り当てます。Kbit/s 未满是切り捨てになります。

6.4.5 デフォルトユーザ優先度書き換え

階層化シェーパ機能付き NIF から送信するパケット内のユーザ優先度を 0 に書き換える機能です。本機能を使用しない場合は、ユーザ優先度を 0 に書き換えられません。

なお、マーカー機能でのユーザ優先度書き換えと併用した場合は、本機能が優先されます。

また、VLAN ユーザマッピングと併用した場合、VLAN ユーザマッピングによって対応するキューにキューイングされたあと、ユーザ優先度を 0 に書き換えます。

6.4.6 階層化シェーパ使用時の注意事項

(1) LLPQ による帯域制御

LLPQ 帯域に最低帯域より大きな帯域を設定した場合の注意事項を次に示します。

- 最低帯域を超える入力帯域が低遅延キューにある環境では、ユーザに割り当てる帯域の合計がポート帯域を超えることがあります。この場合、一部のユーザの最低帯域が保証されません。
- 回線帯域以上の負荷が掛かっている環境では、各ユーザの LLPQ 帯域制御の出力帯域は、LLPQ 帯域制御値の比率よりも差が小さくなり、フレーム長が長いトラフィックを送信しているユーザが大きくなります。

6.5 階層化シェーパのコンフィグレーション

6.5.1 シェーパモードの設定

[設定のポイント]

NIF にシェーパモードを設定します。

[コマンドによる設定]

1. `(config)# shaper nif 1`
NIF 1 に対してシェーパ NIF 情報を設定し、シェーパ NIF モードに移行します。
2. `(config-sh-nif)# mode rgq`
NIF 1 のシェーパモードを RGQ に設定します。

6.5.2 ユーザ帯域制御およびスケジューリングの設定

[設定のポイント]

ユーザ帯域制御、スケジューリングなどを設定したシェーパユーザリストを作成し、ポート 1/1 に対して設定します。

[コマンドによる設定]

1. `(config)# shaper user-list rgquser1 peak-rate 10M min-rate 5M weight 1 pq`
ユーザリスト名称 (rgquser1) のシェーパユーザリストを作成します。最大帯域 10Mbit/s、最低帯域 5Mbit/s、重み 1、スケジューリング (PQ) を設定します。
2. `(config)# shaper user-list rgquser2 peak-rate 5M min-rate 3M weight 1 pq`
ユーザリスト名称 (rgquser2) のシェーパユーザリストを作成します。最大帯域 5Mbit/s、最低帯域 3Mbit/s、重み 1、スケジューリング (PQ) を設定します。
3. `(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。
4. `(config-if)# shaper user 1-10 list rgquser1`
ユーザ ID 1 ~ 10 にユーザリスト名称 (rgquser1) を指定し、ユーザ ID 1 ~ 10 を有効にします。
5. `(config-if)# shaper default-user list rgquser2`
デフォルトユーザにユーザリスト名称 (rgquser2) を指定し、デフォルトユーザを有効にします。

6.5.3 ポート帯域制御の設定

該当するポートの出力帯域を、実回線の帯域より低くする場合に設定します。

[設定のポイント]

該当するポート (100Mbit/s) に対し、ポート帯域制御による帯域の設定 (80Mbit/s) を行います。

[コマンドによる設定]

1. `(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。
2. `(config-if)# speed 100`
`(config-if)# duplex full`
該当するポートの回線速度を 100Mbit/s に設定します。
3. `(config-if)# shaper port rate-limit 80M`
ポート帯域を 80Mbit/s に設定します。

6.5.4 シェーパ自動設定機能の設定

シェーパ機能をサポートしているすべての NIF に対して簡単に階層化シェーパを設定します。

[設定のポイント]

装置全体に対して、使用するシェーパモードと一回線当たりのユーザ数 (500) を設定します。通常の階層シェーパの設定とは併用できません。

[コマンドによる設定]

1. `(config)# shaper auto-configuration rgq number-of-user 500`
シェーパ自動設定機能のシェーパモードを RGQ, ユーザ数を 500 に設定します。

6.6 階層化シェーパのオペレーション

show system コマンドでユーザ数を，show shaper コマンドでイーサネットインタフェースに設定した階層化シェーパの内容を確認します。

6.6.1 ユーザ数の確認

装置当たりで使用しているユーザ数の確認方法を次の図に示します。

図 6-17 装置当たりの使用済みユーザ数の確認

```
> show system
Date 2008/06/24 18:36:57 UTC
System: AX6708S, OS-SE Ver. 10.7.A
      :
      :
Flow Database Management
  fldm : default standard
    Filter resources      Used/Max:   1856/   4000
      MAC :      239  IPv4 :   1046  IPv6 :    571
    QoS resources        Used/Max:   1206/   4000
      MAC :      18  IPv4 :    814  IPv6 :    374
  upc-storm-control mode : upc-in-and-storm-control
    UPC resources        Used/Max:    145/    744
      MAC :     100  IPv4 :     30  IPv6 :     15
Hierarchical shaper Database Management                ... 1
  User: 1024/32768
>
```

1. Hierarchical shaper Database Management の User パラメータの内容が，すべての NIF に設定している LLRLQ1，LLRLQ2，ユーザ，およびデフォルトユーザの合計になっていることを確認します。

6.6.2 階層化シェーパの確認

階層化シェーパの確認方法を次の図に示します。

図 6-18 スケジューリングの確認

```

> show shaper
Date 2008/06/24 12:00:00 UTC
NIF 1/Port 1, Shaper_mode:RGO ... 1
Predicted_tail_drop:disable, Vlan_user_map:disable ... 2
Port_Rate_limit=80Mbit/s ... 3

User:default-user, rqgdefuser ... 4
Schedule_mode=PO
Peak_rate=10Mbit/s, Min_rate=5Mbit/s, Weight=1
Queue      send_pkt      discard_pkt  Queue_length
1           6533          3451        10/ 120/ 120
2           2564          1581        5/ 120/ 120
3          2256877          235         4/ 100/ 100
4          4698951           0          4/ 90/ 100
5          15875213           0          3/ 70/ 80
6          25987192           0          1/ 65/ 80
7          28753135           0          1/ 45/ 50
8          38419319           0          1/ 43/ 50
total      116008881          5267         -

User:ID=1, rqguser1 ... 5
Schedule_mode=PO
Peak_rate=5Mbit/s, Min_rate=3Mbit/s, Weight=1
Queue      send_pkt      discard_pkt  Queue_length
1           6324          3781        12/ 120/ 120
2           2873          1761         4/ 120/ 120
3          2200134           331         3/ 100/ 100
4          4781911           0          1/ 89/ 100
5          14890111           0          1/ 65/ 80
6          23091811           0          1/ 63/ 80
7          27576011           0          1/ 41/ 50
8          37910013           0          1/ 35/ 50
total      110459188          5873         -

:
:
:

Discard packets(User not configured):      2585910248
>

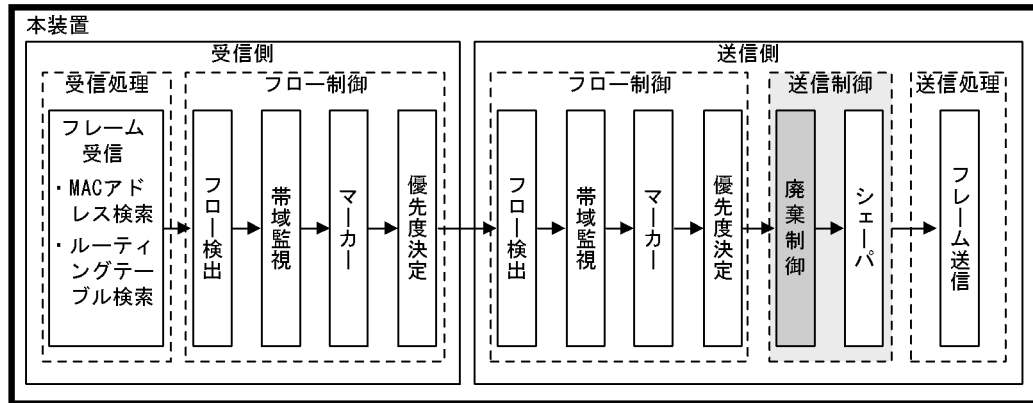
```

1. Shaper mode のパラメータが該当 NIF に指定したシェーパーモードになっていることを確認します。
2. Predicted tail drop のパラメータで早期検出テールドロップ機能が設定されているかどうかを確認します。
3. Port Rate_limit のパラメータが該当ポートに指定したポート帯域制御値になっていることを確認します。
4. User のパラメータに default-user が設定されていて、デフォルトユーザに指定したユーザリストの内容が User:default-user 配下の項目に反映されていることを確認します。
5. User のパラメータに ID:1 が設定されていて、ユーザ ID1 に指定したユーザリスト名称と該当ユーザリストの内容が User:ID=1 配下の項目に反映されていることを確認します。

6.7 廃棄制御解説

この節で説明する廃棄制御の位置づけを次の図に示します。

図 6-19 廃棄制御の位置づけ



(凡例) : この節で説明するブロック

6.7.1 廃棄制御

廃棄制御は、キューイングする各キューに対して廃棄されやすさの度合いを示すキューイング優先度と、キューにフレームが滞留している量に応じて、該当フレームをキューイングするか廃棄するかを制御する機能です。

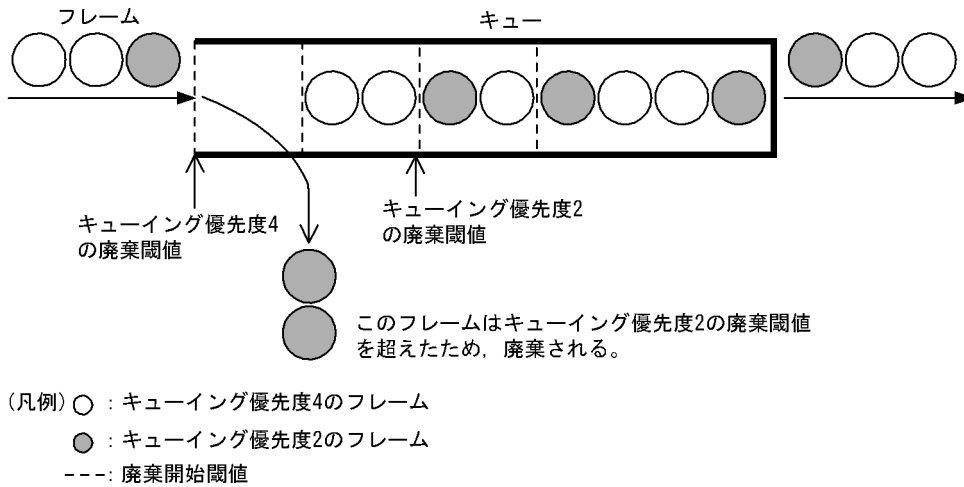
キューにフレームが滞留している場合、キューイング優先度を変えることによって、さらに木目細かいQoSを実現できます。

本装置は、テールドロップ方式で廃棄制御を行います。

(1) テールドロップ

キュー長が廃棄閾値を超えると、フレームを廃棄する機能です。廃棄閾値は、キューイング優先度ごとに異なり、キューイング優先度値が高いほどフレームが廃棄されにくくなります。テールドロップの概念を次の図に示します。キューイング優先度2の廃棄閾値を超えると、キューイング優先度2のフレームをすべて廃棄します。

図 6-20 テールドロップの概念



テールドロップ機能でのキューイング優先度ごとの廃棄閾値を次の表に示します。廃棄閾値は、レガシーシェーパ機能をサポートしている NIF と階層化シェーパ機能をサポートしている NIF で異なります。NIF 種別との対応については、「6.10 NIF 種別と送信制御機能との対応」を参照してください。廃棄閾値は、キュー長に対するキューのたまり具合を百分率で表します。

レガシーシェーパ機能サポート NIF の場合

表 6-23 レガシーシェーパ NIF の廃棄閾値

キュー種別	キューイング優先度に対する廃棄閾値 [%]			
	1	2	3	4
ディストリビューション送信キュー	40	60	85	100
ポート送信キュー				

注 表中のヘッダ部の数字 1 ~ 4 は、キューイング優先度を示します。

階層化シェーパ機能サポート NIF の場合

表 6-24 階層化シェーパ NIF の廃棄閾値

キュー種別	キューイング優先度に対する廃棄閾値 [%]			
	1	2	3	4
ディストリビューション送信キュー	40	60	85	100
ポート送信キュー				
ユーザキュー	25 / 50 / 75			100

注 表中のヘッダ部の数字 1 ~ 4 は、キューイング優先度を示します。

注 次に示す廃棄モードをどれか一つ選択します。

廃棄モード	キューイング優先度 [%]	
	1 ~ 2	3 ~ 4
tail-drop1	25	100

廃棄モード	キューイング優先度 [%]	
	1 ~ 2	3 ~ 4
tail-drop2	50	100
tail-drop3	75	100

キューイング優先度は送信時の廃棄クラスによってキューイング優先度のマッピングが異なります。本装置では NIF 種別に応じて廃棄クラス 2 および廃棄クラス 4 の 2 種類があります。キューイング優先度および廃棄クラスのマッピングについては、「5.10 優先度決定の解説」を参照してください。NIF 種別に応じた廃棄クラスについては、「6.10 NIF 種別と送信制御機能との対応」を参照してください。

6.7.2 バッファ管理

階層化シェーパでは、ポート単位およびユーザ単位でバッファを変更できます。バッファを大きくした場合、パケットが廃棄されにくくなります。ただし、パケットの遅延やほかのキューのトラフィックにも影響します。キューイングするパケットの特性やサービスに応じて変更してください。

階層化シェーパ機能をサポートしている NIF ごとのバッファ容量のデフォルト値を次に示します。

(1) AX6700S, AX6600S の場合

表 6-25 8 キュー制御時のデフォルト値

キュー番号	NK1GS-8M	
	ポート単位	ユーザキュー単位
QoS1	2000	120
QoS2	2000	120
QoS3	1500	100
QoS4	1500	100
QoS5	1500	80
QoS6	1500	80
QoS7	1000	50
QoS8	1000	50

表 6-26 4 キュー制御時のデフォルト値

キュー番号	NK1GS-8M	
	ポート単位	ユーザキュー単位
QoS1	4000	120
QoS2	3000	100
QoS3	3000	80
QoS4	2000	50

表 6-27 バッファ容量

NIF 種別	バッファ容量
NK1GS-8M	96000

(2) AX6300S の場合

表 6-28 8 キュー制御時のデフォルト値

キュー番号	NH1GS-6M	
	ポート単位	ユーザキュー単位
QoS1	1250	120
QoS2	1250	120
QoS3	1000	100
QoS4	1000	100
QoS5	1000	80
QoS6	1000	80
QoS7	750	50
QoS8	750	50

表 6-29 4 キュー制御時のデフォルト値

キュー番号	NH1GS-6M	
	ポート単位	ユーザキュー単位
QoS1	2500	120
QoS2	2000	100
QoS3	2000	80
QoS4	1500	50

表 6-30 バッファ容量

NIF 種別	バッファ容量
NH1GS-6M	48000

6.7.3 早期検出テールドロップ

本機能は、特定のユーザによるバッファの占有を防ぐ機能です。

ユーザは、該当ポートに割り当てたバッファをキュー番号ごとに共有しています。そのため、特定のユーザのユーザキューにフレームが溜まり過ぎると、ほかのユーザの同じキュー番号を持つユーザキューにフレームをキューイングできなくなります。本機能は、ポートに割り当てた各キューのバッファの 7/8 までフレームが溜まった場合に、該当ポートの全ユーザに対して、溜まったキュー番号と同じユーザキューのキュー長を半分にします。

6.7.4 廃棄制御使用時の注意事項

(1) ポートのバッファ枯渇によるフレーム廃棄について

ユーザは、該当ポートに割り当てたバッファをキュー番号ごとに共有しています。そのため、1 ポート内の多数のユーザに対してフレームのキューイングが同時に発生した場合、共有しているポートのバッファが枯渇することがあります。この場合、バッファを割り当てられないユーザが発生します。該当ユーザに対してはフレームがキューイングできないため、そのユーザの帯域の状態に関係なくフレームの廃棄が発生します。

ユーザとポートのバッファ状態は、`show shaper` コマンドで確認してください。

このような状況になるおそれのある環境では、より多くのユーザにバッファが割り当てられるように、ユーザごとのバッファ容量を少なくするか、ポートのバッファ容量を多くしてください。

6.8 廃棄制御のコンフィグレーション

6.8.1 キューイング優先度の設定

特定のフローに対してキューイング優先度を設定します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出を行い、キューイング優先度を設定します。

[コマンドによる設定]

1. (config)# ip qos-flow-list QOS-LIST2
IPv4 QoS フローリスト (QOS-LIST2) を作成します。本リストを作成することによって、IPv4 QoS フローリストモードに移行します。
2. (config-ip-qos)# qos ip any host 192.168.100.10 action priority-class 8
discard-class 1
192.168.100.10 の IP アドレスを宛先とし、出力優先度 = 8、キューイング優先度 = 1 の QoS フローリストを設定します。
3. (config-ip-qos)# exit
IPv4 QoS フローリスト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。
4. (config)# interface vlan 10
VLAN10 のインタフェースモードに移行します。
5. (config-if)# ip qos-flow-group QOS-LIST2 in layer2-forwarding
受信側にレイヤ 2 中継する QoS フローリスト (QOS-LIST2) を有効にします。

6.8.2 階層化シェーパのバッファ管理とテールドロップの設定

[設定のポイント]

階層化シェーパを設定しているポートのバッファと、該当ポートに反映するユーザのキュー長と廃棄制御モードを設定します。

[コマンドによる設定]

1. (config)# shaper user-list rgquser1 peak-rate 10M min-rate 5M pq queue-length 130 110 100 90 90 80 60 40 discard tail-drop1 tail-drop1 tail-drop2 tail-drop2 tail-drop2 tail-drop2 tail-drop3 tail-drop3
ユーザリスト名称 (rgquser1) のシェーパユーザリストを作成します。最大帯域 10Mbit/s、最低帯域 5Mbit/s、スケジューリング (PQ)、キュー 1 から順に 130、110、100、90、90、80、60、40 のキュー長を、tail-drop1、tail-drop1、tail-drop2、tail-drop2、tail-drop2、tail-drop2、tail-drop3、tail-drop3 の廃棄モードを設定します。
2. (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。

3. `(config-if)# shaper port buffer 2100 1900 1700 1500 1500 1300 1100 900`
ポート 1/1 のキュー 1 から順に 2100 , 1900 , 1700 , 1500 , 1500 , 1300 , 1100 , 900 のバッファを設定します。
4. `(config-if)# shaper user 1-10 list rgquser1`
ユーザ ID 1 ~ 10 にユーザリスト名称 (rgquser1) を指定し , ユーザ ID 1 ~ 10 を有効にします。

6.9 廃棄制御のオペレーション

回線にトラフィック (Queue8 の Qlen が 255 程度の滞留が発生するトラフィック) を注入している状態で、show qos queueing interface コマンドによってキューイングされているキュー番号、キューイング優先度、および廃棄パケット数を確認します。対象のイーサネットインタフェースは、ポート 1/11、出力優先度=8、キューイング優先度=1 です。

6.9.1 キューイング優先度の確認

キューイング優先度の確認方法を次の図に示します。

図 6-21 キューイング優先度の確認

```
> show qos queueing interface 1/11 outbound
Date 2007/11/01 12:00:00 UTC
NIF1/Port11 (outbound)
Max_Queue=8, Rate=100Mbit/s, Schedule_mode=pq
Queue1: Qlen=0, Peak_Qlen=0, Limit_Qlen=255, Drop_mode=tail_drop
      send_pkt      discard_pkt      send_byte
total              0              0              0
      :
      :
Queue8: Qlen=191, Peak_Qlen=191, Limit_Qlen=255, Drop_mode=tail_drop
      send_pkt      discard_pkt      send_byte
total              6533             8245             533.0k
>
```

- Queue8 の Qlen の値がカウントされていることを確認します。
- Qlen の値が Limit_Qlen の値の 75% であり、discard1 の discard_pkt のカウンタがインクリメントされていることを確認します。

なお、この表示例は、NIF 種別の NK1G-24S または NH1G-24S の例です。

6.9.2 階層化シェーパのバッファ管理とテールドロップの確認

階層化シェーパのバッファ管理とテールドロップの確認方法を次の図に示します。

図 6-22 階層化シェーパのバッファ管理とテールドロップの確認

```

> show shaper all
Date 2008/06/24 12:00:00 UTC
NIF 1/Port 1, Shaper_mode:RGQ
Predicted_tail_drop:disable, Vlan_user_map:disable
Port Rate_limit=1Gbit/s
Buffer
  QoS1= 194/ 1812/ 2100 QoS2= 82/ 1784/ 1900
  QoS3= 74/ 1582/ 1700 QoS4= 71/ 1422/ 1500
  QoS5= 68/ 1398/ 1500 QoS6= 61/ 1284/ 1300
  QoS7= 51/ 1231/ 1100 QoS8= 41/ 1098/ 900
      :
      :
      :
User:ID=1, USER-A
Schedule_mode=PQ
Peak_rate=500Mbit/s, Min_rate=250Mbit/s, Weight=10
Queue      send_pkt      discard_pkt      Queue_length
1           6324           3781           12/ 120/ 130
2           2873           1761           4/ 120/ 120
3          2200134           331           3/ 100/ 110
4          4781911              0           1/ 89/ 90
5          14890111              0           1/ 65/ 90
6          23091811              0           1/ 63/ 80
7          27576011              0           1/ 41/ 60
8          37910013              0           1/ 35/ 40
total      110459188           5873           -
Queue      send_byte      discard_byte      discard_mode
1           9.2M           5.5M           tail-drop1
2           4.2M           2.5M           tail-drop1
3           3.1G           348.4k         tail-drop2
4           6.8G              0           tail-drop2
5          21.1G              0           tail-drop2
6          32.6G              0           tail-drop2
7          40.0G              0           tail-drop3
8          53.6G              0           tail-drop3
total      156.2G           8.5M           -
      :
      :
      :
Discard packets(User not configured):          2585910248
>

```

Buffer の QoS1 ~ QoS8 に表示されている三つの値のうち、いちばん右側の値がポートに指定したバッファ値になっていることを確認します。

該当する User の各 Queue 番号の Queue_length に表示されている三つの値のうち、いちばん右側の値が指定したキュー長になっていることを確認します。

該当する User の各 Queue 番号の discard_mode に表示されている廃棄モードが指定した廃棄モードになっていることを確認します。

6.10 NIF 種別と送信制御機能との対応

6.10.1 レガシーシェーパ機能サポート NIF

(1) AX6700S , AX6600S の場合

NIF 種別と送信制御機能との対応を次の表に示します。

表 6-31 NIF 種別と送信制御機能との対応 (1/3)

NIF 種別	ポート送信キュー				
	スケジューリング				
	PQ	RR	4PQ+4WFQ	2PQ+4WFQ+2BEQ	4WFQ+4BEQ
NK1G-24T					
NK1G-24S					
NK10G-4RX					
NK10G-8RX					

(凡例) : サポート

表 6-32 NIF 種別と送信制御機能との対応 (2/3)

NIF 種別	ポート送信キュー			
	キュー数指定	ポート帯域制御	廃棄制御	
			テールドロップ	廃棄クラス数
NK1G-24T				4
NK1G-24S				4
NK10G-4RX				4
NK10G-8RX				4

(凡例) : サポート

表 6-33 NIF 種別と送信制御機能との対応 (3/3)

NIF 種別	ディストリビューション送信キュー		
	スケジューリング	廃棄制御	
		PQ	テールドロップ
NK1G-24T			4
NK1G-24S			4
NK10G-4RX			4
NK10G-8RX			4

(凡例) : サポート

(2) AX6300S の場合

NIF 種別と送信制御機能との対応を次の表に示します。

表 6-34 NIF 種別と送信制御機能との対応 (1/3)

NIF 種別	ポート送信キュー				
	スケジューリング ¹				
	PQ	RR	4PQ+4WFQ	2PQ+4WFQ+2BEQ	4WFQ+4BEQ
NH1G-16S ²	-	-	-	-	-
NH1G-24T					
NH1G-24S					
NH1G-48T ²	-	-	-	-	-
NH10G-1RX		-	-	-	-
NH10G-4RX					
NH10G-8RX					

(凡例) : サポート - : 未サポート

注 1 未サポートのスケジューリングを指定した場合、ログメッセージを表示し PQ で動作します。

注 2 送信制御機能をサポートしていません。

表 6-35 NIF 種別と送信制御機能との対応 (2/3)

NIF 種別	ポート送信キュー			
	キュー数指定 ¹	ポート帯域制御 ²	廃棄制御	
			テールドロップ	廃棄クラス数
NH1G-16S ³	-	-	-	-
NH1G-24T				4
NH1G-24S				4
NH1G-48T ³	-	-	-	-
NH10G-1RX	-	-		4
NH10G-4RX				4
NH10G-8RX				4

(凡例) : サポート - : 未サポート

注 1 未サポートの NIF にキュー数指定をした場合、ログメッセージを表示しキュー数は 8 で動作します。

注 2 次のどれかの条件に該当する場合、ログメッセージを表示しポート帯域制御は動作しません。

- 未サポートの NIF にポート帯域制御を指定した場合
- ポート帯域制御の設定帯域が回線速度を超えた場合
- 回線状態が半二重モードの場合

注 3 送信制御機能をサポートしていません。

6. 送信制御

表 6-36 NIF 種別と送信制御機能との対応 (3/3)

NIF 種別	ディストリビューション送信キュー		
	スケジューリング	廃棄制御	
	PQ	テールドロップ	廃棄クラス数
NH1G-16S	-	-	-
NH1G-24T			4
NH1G-24S			4
NH1G-48T	-	-	-
NH10G-1RX	-	-	-
NH10G-4RX			4
NH10G-8RX			4

(凡例) : サポート - : 未サポート

注 送信制御機能をサポートしていません。

6.10.2 階層化シェーパ機能サポート NIF

(1) AX6700S, AX6600S の場合

NIF 種別と送信制御機能との対応を次の表に示します。

表 6-37 NIF 種別と送信制御機能との対応 (1/6)

NIF 種別	ポート送信キュー				
	スケジューリング	キュー数 指定	ポート 帯域制御	廃棄制御	
	PQ			テール ドロップ	廃棄 クラス数
NK1GS-8M			-		4

(凡例) : サポート - : 未サポート

注 ユーザキューのポート帯域制御でサポート

表 6-38 NIF 種別と送信制御機能との対応 (2/6)

NIF 種別	ディストリビューション送信キュー		
	スケジューリング	廃棄制御	
	PQ	テールドロップ	廃棄クラス数
NK1GS-8M			4

(凡例) : サポート

表 6-39 NIF 種別と送信制御機能との対応 (3/6)

NIF 種別	ユーザキュー					
	シェーパモード					
	RGQ	WGQ	LLPQ1	LLPQ2	LLPQ4	LLRLQ
NK1GS-8M						

(凡例) : サポート

表 6-40 NIF 種別と送信制御機能との対応 (4/6)

NIF 種別	ユーザキュー						
	スケジューリング						
	PQ	VLLQ+3 WFQ	4WFQ	PQ+VLLQ+ 2WFQ	2PQ+VLLQ+4WF Q+BEQ	2PQ+4WFQ+2 BEQ	4PQ+4W FQ
NK1GS-8M							

(凡例) : サポート

表 6-41 NIF 種別と送信制御機能との対応 (5/6)

NIF 種別	ユーザキュー		
	ユーザ帯域制御	WGQ 帯域制御	ポート帯域制御
NK1GS-8M			

(凡例) : サポート

表 6-42 NIF 種別と送信制御機能との対応 (6/6)

NIF 種別	ユーザキュー				
	廃棄制御			デフォルト	バッファ
	テール ドロップ	早期検出テール ドロップ	廃棄 クラス数	ユーザ優先度 書き換え	管理
NK1GS-8M			2		

(凡例) : サポート

(2) AX6300S の場合

NIF 種別と送信制御機能との対応を次の表に示します。

表 6-43 NIF 種別と送信制御機能との対応 (1/6)

NIF 種別	ポート送信キュー				
	スケジューリング	キュー数	ポート	廃棄制御	
	PQ	指定	帯域制御	テール ドロップ	廃棄 クラス数
NH1GS-6M			-		4

6. 送信制御

(凡例) : サポート - : 未サポート
 注 ユーザキューのポート帯域制御でサポート

表 6-44 NIF 種別と送信制御機能との対応 (2/6)

NIF 種別	ディストリビューション送信キュー		
	スケジューリング		廃棄制御
	PQ	テールドロップ	廃棄クラス数
NH1GS-6M	-	-	-

(凡例) - : 未サポート

表 6-45 NIF 種別と送信制御機能との対応 (3/6)

NIF 種別	ユーザキュー					
	シェーバモード					
	RGQ	WGQ	LLPQ1	LLPQ2	LLPQ4	LLRLQ
NH1GS-6M		-	-	-	-	-

(凡例) : サポート - : 未サポート

表 6-46 NIF 種別と送信制御機能との対応 (4/6)

NIF 種別	ユーザキュー						
	スケジューリング						
	PQ	VLLQ+3 WFQ	4WFQ	PQ+VLLQ+ 2WFQ	2PQ+VLLQ+4WF Q+BEQ	2PQ+4WFQ+2 BEQ	4PQ+4W FQ
NH1GS-6M							

(凡例) : サポート

表 6-47 NIF 種別と送信制御機能との対応 (5/6)

NIF 種別	ユーザキュー		
	ユーザ帯域制御	WGQ 帯域制御	ポート帯域制御
NH1GS-6M		-	

(凡例) : サポート - : 未サポート

表 6-48 NIF 種別と送信制御機能との対応 (6/6)

NIF 種別	ユーザキュー				
	廃棄制御			デフォルト ユーザ優先度 書き換え	バッファ 管理
	テール ドロップ	早期検出テール ドロップ	廃棄 クラス数		
NH1GS-6M			2		

(凡例) : サポート

6.10.3 送信制御をサポートしていないNIF

次に示す NIF は送信制御をサポートしていません。

- NH1G-16S
- NH1G-48T

7

レイヤ2認証

この章では、本装置のレイヤ2認証機能の概要について説明します。

7.1 概要

7.2 レイヤ2認証と他機能との共存について

7.3 レイヤ2認証共通の機能

7.4 レイヤ2認証使用時の注意事項

7.5 レイヤ2認証共通コンフィグレーション

7.1 概要

7.1.1 レイヤ 2 認証種別

本装置には、次に示すレイヤ 2 レベルの認証機能があります。

- IEEE802.1X
IEEE802.1X に準拠したユーザ認証をする機能です。IEEE802.1X 認証に必要な EAPOL パケットを送信する端末を認証します。
- Web 認証
Web 認証は、汎用 Web ブラウザを利用してユーザ認証をする機能です。汎用 Web ブラウザを使用できる端末で認証操作をします。
- MAC 認証
MAC 認証は、プリンタなど、ユーザによる認証操作ができない端末を認証する機能です。
- 認証 VLAN 【OP-VAA】
認証 VLAN は、専用の認証サーバと連携してユーザ認証をする機能です。

レイヤ 2 認証には、認証動作による認証モードがあります。認証モードごとの機能概要を次の表に示します。

また、これらの機能は、組み合わせて利用できる機能と利用できない機能があります。機能の組み合わせについては「7.2 レイヤ 2 認証と他機能との共存について」を参照してください。

表 7-1 レイヤ 2 認証でサポートする機能

レイヤ 2 認証	認証モード	概要
IEEE802.1X	ポート単位認証	物理ポートまたはチャンネルグループに対して認証を制御します。一つの物理ポートまたは一つのチャンネルグループが一つの認証単位となります。また、ポート単位認証には次に示す三つの認証サブモードがあり、それぞれ認証動作が異なります。 1. シングルモード 一つの認証単位に一つの端末だけ認証して接続します。最初に認証した端末以外の端末から認証要求があると、そのポートの認証状態は未認証状態に戻ります。 2. マルチモード 一つの認証単位に複数端末の接続を許容します。最初に認証した端末以外の端末は認証しません。 3. 端末認証モード 一つの認証単位に複数端末の接続を許容し、端末ごとに認証を行います。
	VLAN 単位認証（静的）	VLAN に対して認証を制御します。複数の端末が接続できます。端末ごとに認証を行い、認証に成功すると VLAN 内で通信できます。
	VLAN 単位認証（動的）	MAC VLAN に所属する端末に対して認証を制御します。複数の端末が接続できます。認証に成功すると MAC VLAN で切り替えた VLAN で通信できます。
Web 認証	固定 VLAN モード	ユーザ認証成功後は、VLAN 内へ通信できます。
	ダイナミック VLAN モード	ユーザ認証成功後は、MAC VLAN で切り替えた VLAN 内へ通信できます。MAC VLAN が設定された物理ポートに認証を設定します。
	レガシーモード	ユーザ認証成功後は、MAC VLAN で切り替えた VLAN 内へ通信できます。MAC VLAN の VLAN に認証を設定します。
MAC 認証	固定 VLAN モード	認証成功後は、VLAN 内へ通信できます。

レイヤ2認証	認証モード	概要
	ダイナミック VLAN モード	認証成功後は、MAC VLAN で切り替えた VLAN 内へ通信できません。
認証 VLAN	-	認証 VLAN 専用サーバで認証を行い、認証結果によって本装置の MAC VLAN で VLAN を切り替えます。切り替え後の VLAN 内へ通信できます。

(凡例) - : 該当しない

7.1.2 認証方式

レイヤ2認証には装置内蔵の認証データで認証するローカル認証方式と、RADIUS サーバで認証する RADIUS 認証方式があります。認証 VLAN を除くレイヤ2認証に対応する認証方式を次の表に示します。

表 7-2 レイヤ2認証の認証方式

レイヤ2認証	認証モード	ローカル認証方式	RADIUS 認証方式
IEEE802.1X	ポート単位認証	×	
	VLAN 単位認証 (静的)	×	
	VLAN 単位認証 (動的)	×	
Web 認証	固定 VLAN モード		
	ダイナミック VLAN モード		
	レガシーモード		
MAC 認証	固定 VLAN モード		
	ダイナミック VLAN モード		

(凡例) : 対応する × : 対応しない

7.2 レイヤ2 認証と他機能との共存について

レイヤ2 認証と他機能との共存について説明します。

7.2.1 レイヤ2 認証と他機能との共存

レイヤ2 認証と他機能との共存仕様を次の表に示します。

表 7-3 他機能との共存仕様

レイヤ2 認証機能	機能名		共存仕様
IEEE802.1X	MAC アドレス学習停止		VLAN およびその VLAN を設定したポートで同時に使用できません。
	MAC アドレス学習数制限		VLAN およびポートで同時に使用できません。
	VLAN	ポート VLAN	ポート単位認証および VLAN 単位認証（静的）で使用できます。
		プロトコル VLAN	装置で同時に使用できません。
		MAC VLAN	VLAN 単位認証（動的）で使用できます。
	デフォルト VLAN		ポート単位認証および VLAN 単位認証（静的）で使用できます。 VLAN 単位認証（動的）では認証前 VLAN に使用できません。
	VLAN 拡張機能	VLAN トンネリング	装置で同時に使用できません。
		EAPOL フォワーディング	装置で同時に使用できません。
	スパンニングツリー		スパンニングツリーを設定したポートには、ポート単位認証または VLAN 単位認証（静的）を設定しないでください。
	Ring Protocol		Ring Protocol を設定したリングポートには、ポート単位認証または VLAN 単位認証（静的）を設定しないでください。
	認証 VLAN		装置で同時に使用できません。
	GSRP		装置で同時に使用できません。
	VRRP		VRRP を設定した VLAN およびその VLAN を設定したポート以外で認証ができます。次の場合は IEEE802.1X の認証ができません。 <ul style="list-style-type: none"> VLAN 単位認証（静的）の場合、VRRP が動作する VLAN VLAN 単位認証（動的）の場合、VRRP が動作する VLAN で認証デフォルト VLAN、MAC VLAN を使用した認証 ポート単位認証の場合、VRRP が動作する VLAN を設定したポート
OADP, CDP		透過できません。	
VRF		装置で同時に使用できません。	
Web 認証	リンクアグリゲーション		固定 VLAN モードおよびダイナミック VLAN モードの認証ポートとして、チャンネルグループのポートは使用できません。

レイヤ2 認証機能	機能名		共存仕様
	MAC アドレス学習停止		VLAN およびその VLAN を設定したポートで同時に使用できません。
	MAC アドレス学習数制限		VLAN およびポートで同時に使用できません。
	VLAN	ポート VLAN	固定 VLAN モードで使用できます。
		プロトコル VLAN	装置で同時に使用できません。
		MAC VLAN	ダイナミック VLAN モードおよびレガシーモードで使用できます。
	デフォルト VLAN		固定 VLAN モードで使用できます。 ダイナミック VLAN モードおよびレガシーモードでは認証前 VLAN に使用できます。
	VLAN 拡張機能	VLAN トンネリング	装置で同時に使用できません。
		EAPOL フォワーディング	ダイナミック VLAN モードで URL リダイレクトを設定した場合は、装置で同時に使用できません。
	スパニングツリー		スパニングツリーを設定したポートには、固定 VLAN モードまたはダイナミック VLAN モードを設定しないでください。
	Ring Protocol		Ring Protocol を設定したリングポートには、固定 VLAN モードまたはダイナミック VLAN モードを設定しないでください。
	認証 VLAN		装置で同時に使用できません。
	DHCP snooping		レガシーモードで指定された VLAN ID が設定されたポートでは使用できません。
	VRRP		VRRP を設定した VLAN およびその VLAN を設定したポート以外で認証ができます。次に示す設定はしないでください。 <ul style="list-style-type: none"> 固定 VLAN モードの場合、VRRP が動作する VLAN を設定したポート ダイナミック VLAN モードの場合、VRRP が動作する VLAN で認証前 VLAN、認証後 VLAN を使用した認証
	VRF		装置で同時に使用できません。
MAC 認証	リンクアグリゲーション		固定 VLAN モードおよびダイナミック VLAN モードの認証ポートとして、チャンネルグループのポートは使用できません。
	MAC アドレス学習停止		VLAN およびその VLAN を設定したポートで同時に使用できません。
	MAC アドレス学習数制限		VLAN およびポートで同時に使用できません。
	VLAN	ポート VLAN	固定 VLAN モードで使用できます。
		プロトコル VLAN	装置で同時に使用できません。
		MAC VLAN	ダイナミック VLAN モードで使用できます。
	デフォルト VLAN		固定 VLAN モードで使用できます。 ダイナミック VLAN モードでは認証前 VLAN に使用できます。
VLAN 拡張機能	VLAN トンネリング	装置で同時に使用できません。	

7. レイヤ2 認証

レイヤ2 認証機能	機能名		共存仕様
		EAPOL フォワーディング	共存できます。
	スパンニングツリー		スパンニングツリーを設定したポートには、MAC 認証を設定しないでください。
	Ring Protocol		Ring Protocol を設定したリングポートには、MAC 認証を設定しないでください。
	認証 VLAN		装置で同時に使用できません。
	VRRP		VRRP を設定した VLAN およびその VLAN を設定したポート以外で認証ができます。VRRP が動作する VLAN を設定したポートを認証ポートに設定しないでください。
	VRF		装置で同時に使用できません。
認証 VLAN	VLAN	ポート VLAN	認証 VLAN の認証端末は接続できません。
		プロトコル VLAN	装置で同時に使用できません。
		MAC VLAN	認証 VLAN の認証端末を接続します。
	デフォルト VLAN		認証前 VLAN に使用できます。
	VLAN 拡張機能	VLAN トネリング	装置で同時に使用できません。
		EAPOL フォワーディング	装置で同時に使用できません。
	IEEE802.1X Web 認証 MAC 認証		装置で同時に使用できません。
	VRF		装置で同時に使用できません。

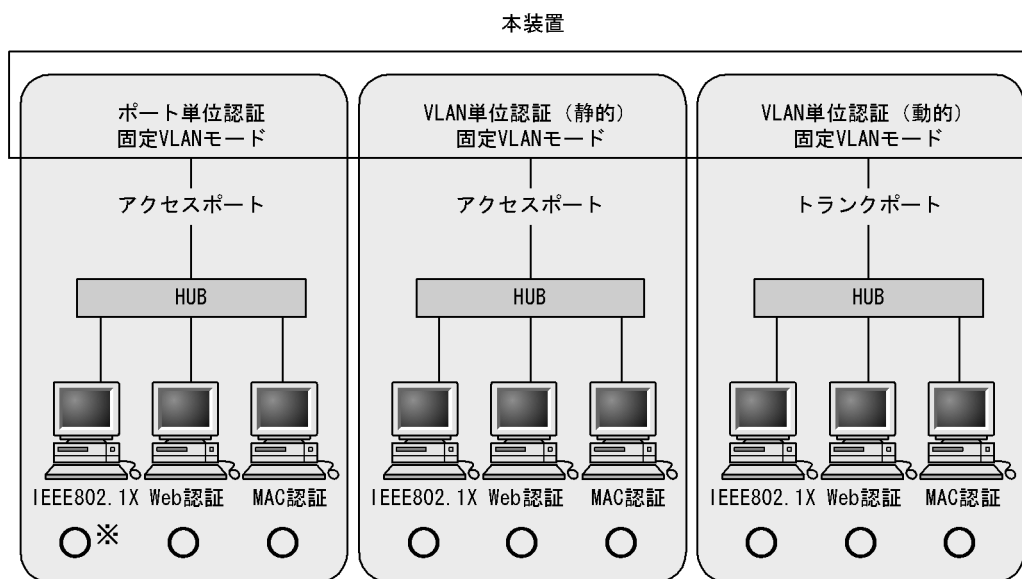
7.2.2 同一ポート内での共存

同一ポートに各レイヤ2 認証の対象ポートとして設定された場合、どの認証モードの組み合わせであれば動作するかを次に示します。

- 固定 VLAN モードの共存
- ダイナミック VLAN モードの共存
- レガシーモードの共存

(1) 同一ポートの固定 VLAN モードの共存

図 7-1 同一ポートの固定 VLAN モードの共存



(凡例) ○ : 動作できる

注※ Web認証およびMAC認証を設定したポートにIEEE802.1Xポート単位認証を設定した場合は、端末認証モードを設定してください。
シングルモードおよびマルチモードを設定しないでください。

[設定しないコンフィギュレーションコマンド]
dot1x force-authorized-port
dot1x port-control force-authorized
dot1x port-control force-unauthorized
dot1x multiple-hosts

表 7-4 同一ポートの固定 VLAN モードの共存

ポートの種類	IEEE802.1X		Web 認証 (固定 VLAN モード)	MAC 認証
	ポート単位認証	VLAN 単位認証 (静的)		
アクセスポート		-		
チャンネルグループの ポート (アクセス ポート)	-	x	-	-
トランクポート	-			
チャンネルグループの ポート (トランク ポート)	-		-	-
上記以外	-	-	-	-

(凡例)

: 動作できる

x : コンフィギュレーションで設定できるが動作できない

7. レイヤ2 認証

- : コンフィグレーションで設定できない

注

Web 認証および MAC 認証を設定したポートに IEEE802.1X のポート単位認証を設定した場合は、端末認証モードを設定してください。シングルモードおよびマルチモードを設定しないでください。

[設定しないコンフィグレーションコマンド]

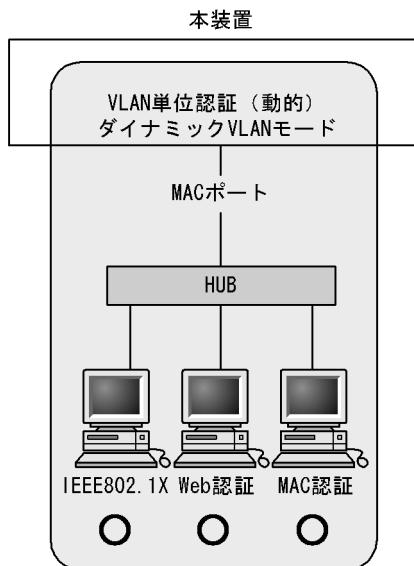
```
dot1x force-authorized-port
dot1x port-control force-authorized
dot1x port-control force-unauthorized
dot1x multiple-hosts
```

[表の見方の一例]

接続先がアクセスポートの場合、IEEE802.1X のポート単位認証、Web 認証（固定 VLAN モード）、MAC 認証の三つの認証モードを同一ポートで利用できます。または、IEEE802.1X の VLAN 単位認証（静的）、Web 認証（固定 VLAN モード）、MAC 認証の三つの認証モードを同一ポートで利用できます。

(2) 同一ポートのダイナミック VLAN モードの共存

図 7-2 同一ポートのダイナミック VLAN モードの共存



(凡例) ○ : 動作できる

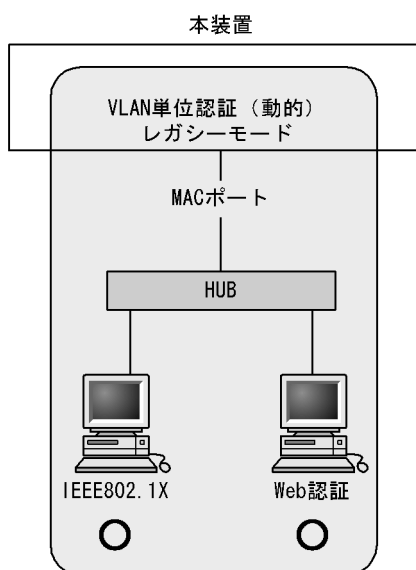
表 7-5 同一ポートのダイナミック VLAN モードの共存

ポートの種類	IEEE802.1X VLAN 単位認証 (動的)	Web 認証 (ダイナミック VLAN モード)	MAC 認証 (ダイナミック VLAN モード)
MAC ポート			
上記以外	×	×	×

(凡例) ○ : 動作できる × : 動作できない

(3) 同一ポートのレガシーモードの共存

図 7-3 同一ポートのレガシーモードの共存



(凡例) ○ : 動作できる

表 7-6 同一ポートのレガシーモードの共存

ポートの種類	IEEE802.1X VLAN 単位認証（動的）	Web 認証 （レガシーモード）
MAC ポート		
上記以外	×	×

(凡例) ○ : 動作できる × : 動作できない

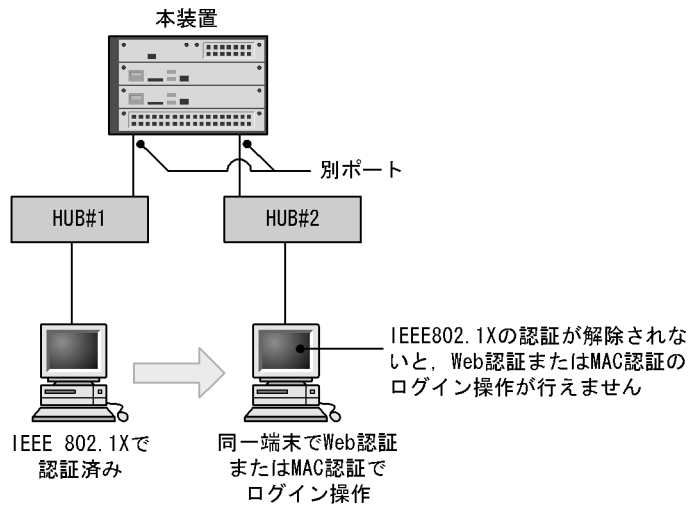
7.2.3 レイヤ2 認証共存時の認証優先

(1) IEEE802.1X と Web 認証または MAC 認証との共存時の認証優先

同一端末（同一 MAC アドレスを持つ端末）で、Web 認証または MAC 認証による成功後に、IEEE802.1X のポート単位認証または VLAN 単位認証（静的）による認証に成功した場合、IEEE802.1X の認証結果が優先され、Web 認証または MAC 認証の認証状態は解除されます（Web 認証では、この場合ログアウト画面は表示されません）。

また、次に示す図のように別々のポートに接続された HUB（図では HUB#1）を介して接続されている端末が、すでに IEEE802.1X（ポート単位認証（端末認証モード）または VLAN 単位認証（静的））で認証されている状態で、別の HUB（図では HUB#2）に接続を変更した場合、いったん IEEE802.1X の認証が解除されないと Web 認証（固定 VLAN モード）または MAC 認証（固定 VLAN モード）のログイン操作を行うことはできません。IEEE802.1X の運用コマンド `clear dot1x auth-state` で認証を解除してください。

図 7-4 IEEE802.1X で認証されている端末のポート移動後の Web 認証または MAC 認証使用



また、同一端末で、Web 認証（ダイナミック VLAN モードまたはレガシーモード）または MAC 認証（ダイナミック VLAN モード）による認証成功後、IEEE802.1X の VLAN 単位認証（動的）による認証に成功した場合、IEEE802.1X の認証結果が優先されて IEEE802.1X で設定された VLAN に切り替わり、Web 認証の認証状態は解除されます（この場合、ログアウト画面は表示されません）。

（2）Web 認証と MAC 認証との共存時の認証優先

同一端末（同一 MAC アドレスを持つ端末）で、MAC 認証が先に認証成功した場合、Web 認証は認証エラーとなります。また、Web 認証が先に認証成功した場合は、Web 認証の認証状態はそのままとなります（MAC 認証の認証はエラーとなります）。

7.3 レイヤ2認証共通の機能

レイヤ2認証共通の機能とその機能を設定するに当たり前提となる項目について説明します。

- 設定時の認証単位
- 認証前端末の通信許可
- 認証済み端末のポート間移動

7.3.1 設定時の認証単位

レイヤ2認証では、認証の設定を物理ポート単位またはVLAN単位に行います。どちらの単位で設定するかは、レイヤ2認証機能および認証モードによって異なります。

認証単位ごとのレイヤ2認証機能と認証モードを次の表に示します。

表 7-7 認証単位ごとのレイヤ2認証機能と認証モード

認証単位	レイヤ2認証機能と認証モード
物理ポート	<ul style="list-style-type: none"> • IEEE802.1X (ポート単位認証) • Web 認証 (固定 VLAN モード) • Web 認証 (ダイナミック VLAN モード) • MAC 認証 (固定 VLAN モード) • MAC 認証 (ダイナミック VLAN モード)
VLAN	<ul style="list-style-type: none"> • IEEE802.1X (VLAN 単位認証 (静的)) • IEEE802.1X (VLAN 単位認証 (動的)) • Web 認証 (レガシーモード) • 認証 VLAN

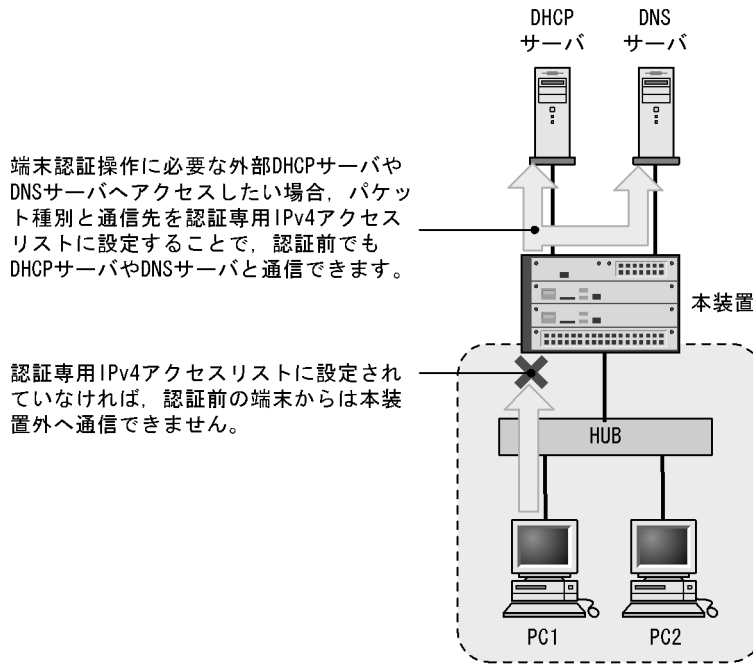
7.3.2 認証前端末の通信許可

(1) 認証専用 IPv4 アクセスリスト

認証前状態の端末に対して、DHCP サーバから IP アドレスの配布や DNS サーバによる名前解決ができるようにするには、認証前状態の端末が DHCP サーバや DNS サーバと通信できる必要があります。なお、Web 認証を設定している場合、DHCP パケットは通信できます。

認証前状態の端末が本装置外の装置 (DHCP サーバや DNS サーバ) と通信できるようにするには、認証専用の IPv4 アクセスリスト (以降、認証専用 IPv4 アクセスリストと呼びます) を設定します。

図 7-5 認証専用 IPv4 アクセスリスト設定後の通信



通常のアクセスリストで設定されたフィルタ条件は、認証専用 IPv4 アクセスリストで設定されたフィルタ条件よりも優先されます。

認証前の端末に外部 DHCP サーバから IP アドレスを配布する場合、認証専用 IPv4 アクセスリストのフィルタ条件に、対象となる DHCP サーバ向けの bootps パケットを通信させる設定が必要になります。この場合は、次に示すようにフィルタ条件を必ず設定してください。

[必要なフィルタ条件設定例]

DHCP サーバの IP アドレスが 10.10.10.254 の場合

```
permit udp any host 10.10.10.254 eq bootps
permit udp any host 255.255.255.255 eq bootps
```

なお、認証前の端末に本装置内蔵の DHCP サーバから IP アドレスを配布する場合、認証専用 IPv4 アクセスリストのフィルタ条件に bootps パケットの設定をすると、装置内蔵の DHCP サーバが使用できません。

[認証専用 IPv4 アクセスリスト設定時の注意]

コンフィグレーションコマンド authentication ip access-group を設定する場合、次の点に注意してください。

- 指定できる認証専用 IPv4 アクセスリストは 1 個だけです。
- 認証専用 IPv4 アクセスリストで設定できるフィルタ条件が収容条件を超えている場合、収容条件内のものだけ設定されます。
- 認証専用 IPv4 アクセスリストで適用できるアクションは permit だけで、次のフィルタ条件に限定されます。
 - プロトコル名称が tcp または udp
 - 宛先 IP アドレス
 - 宛先 L4 ポート
- 認証専用 IPv4 アクセスリストのフィルタ条件に、宛先 IP アドレスとして Web 認証専用 IP アドレスが

含まれるアドレスを設定した場合は、Web 認証によるログイン操作ができません。

(2) 動作可能なレイヤ2認証

認証専用 IPv4 アクセスリストが動作するレイヤ2認証を次の表に示します。

表 7-8 認証専用 IPv4 アクセスリストが動作するレイヤ2認証

機能	IEEE802.1X			Web 認証			MAC 認証	
	ポート単 位認証	VLAN 単 位認証 (静的)	VLAN 単 位認証 (動的)	固定 VLAN モード	ダイナ ミック VLAN モード	レガ シー モード	固定 VLAN モード	ダイナ ミック VLAN モード
認証専用 IPv4 アクセスリス ト						×		

(凡例) : 動作できる × : 動作できない

(3) DHCP snooping 設定時の注意

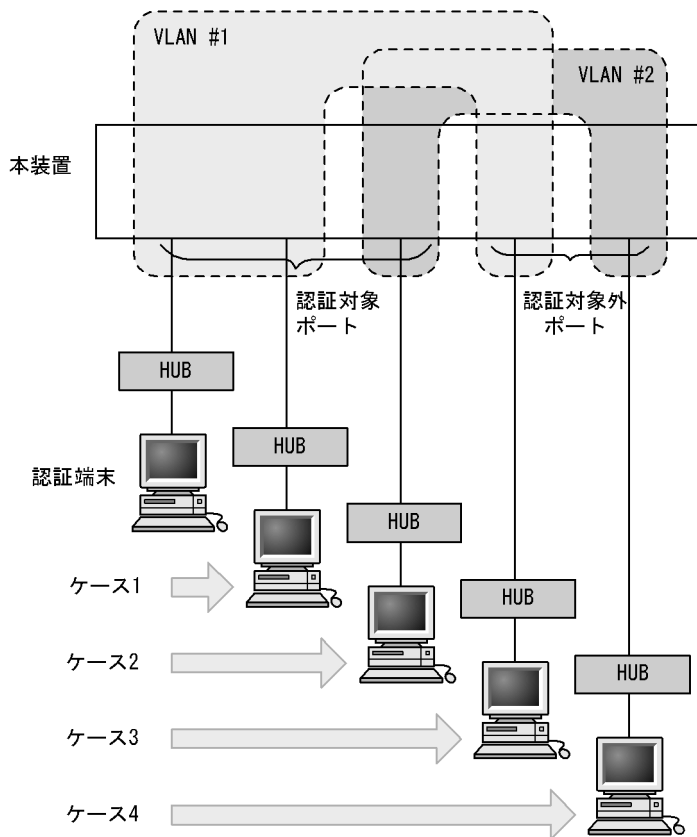
DHCP snooping で untrust ポートに設定されたポートでは、認証専用 IPv4 アクセスリストのフィルタ条件にプロトコル名称 bootps または bootpc を設定しても、端末から送信される DHCP パケットは DHCP snooping の対象となるため、DHCP snooping で許可された DHCP パケットだけが装置外へ送信されます。

7.3.3 認証済み端末のポート間移動

レイヤ2認証で認証された端末をほかのポートに移動した場合、ポートの状態や認証状態がどのように変わるか説明します。

認証済み端末のポート間移動には次の図に示す四つのケースがあります。

図 7-6 認証済み端末のポート間移動例



これら四つのケースについて、レイヤ2 認証ごとに説明します。

(1) IEEE802.1X でのポート間移動時の動作

IEEE802.1X で認証された端末がポートを移動した場合のポートや認証の状態について、認証モードごとに次の表に示します。

表 7-9 IEEE802.1X でのポート間移動時の動作 (ポート単位認証)

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートのMACアドレステーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	移動後、再認証操作	ポート情報が更新	移動前の認証解除	移動後に認証されるまで通信不可
2	認証対象ポート	別 VLAN	移動後、再認証操作	未更新	認証状態が残る	移動後に認証されるまで通信不可
3	認証対象外ポート	同一 VLAN	移動前の認証解除	削除	移動前の認証解除	通信可
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

表 7-10 IEEE802.1X でのポート間移動時の動作 (VLAN 単位認証 (静的))

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレス テーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	認証が継続する	ポート情報が更新	継続	通信可
2	認証対象ポート	別 VLAN	移動後, 再認証操作	未更新	認証状態が残る	移動後に認証されるまで通信不可
3	認証対象外ポート	同一 VLAN	-	-	-	-
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

(凡例)

- : VLAN 単位認証 (静的) は VLAN 単位での設定のため, 同一 VLAN に認証対象外ポートはありません

表 7-11 IEEE802.1X でのポート間移動時の動作 (VLAN 単位認証 (動的))

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレス テーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	認証が継続する	ポート情報が更新	継続	通信可
2	認証対象ポート	別 VLAN	移動後, 再認証操作	未更新	移動前の認証解除	移動後に認証されるまで通信不可
3	認証対象外ポート	同一 VLAN	-	-	-	-
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信不可

(凡例)

- : VLAN 単位認証 (動的) は VLAN 単位での設定のため, 同一 VLAN に認証対象外ポートはありません

(2) Web 認証でのポート間移動時の動作

Web 認証で認証された端末がポートを移動した場合のポートや認証の状態について, 認証モードごとに次の表に示します。

表 7-12 Web 認証でのポート間移動時の動作 (固定 VLAN モード)

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレス テーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	認証が継続される	ポート情報が更新	継続	通信可
2	認証対象ポート	別 VLAN	移動後, 認証操作が必要	削除	移動前の認証解除	移動後に認証されるまで通信不可
3	認証対象外ポート	同一 VLAN	認証解除	削除	移動前の認証解除	通信可
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

表 7-13 Web 認証でのポート間移動時の動作 (ダイナミック VLAN モード)

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレス テーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	認証が継続される	ポート情報が更新	継続	通信可
2	認証対象ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信不可
3	認証対象外ポート	同一 VLAN	認証解除	削除	移動前の認証解除	通信可
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

表 7-14 Web 認証でのポート間移動時の動作 (レガシーモード)

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレス テーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	認証が継続される	ポート情報が更新	継続	通信可
2	認証対象ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信不可
3	認証対象外ポート	同一 VLAN	-	-	-	-
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

(凡例)

- : Web 認証 (レガシーモード) は VLAN 単位での設定のため、同一 VLAN に認証対象外ポートはありません

(3) MAC 認証でのポート間移動時の動作

MAC 認証で認証された端末がポートを移動した場合のポートや認証の状態について、認証モードごとに次の表に示します。

表 7-15 MAC 認証でのポート間移動時の動作 (固定 VLAN モード)

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレス テーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	認証が継続される	ポート情報が更新	継続	通信可
2	認証対象ポート	別 VLAN	移動後、再認証	削除	移動前の認証解除	移動後に認証されるまで通信不可
3	認証対象外ポート	同一 VLAN	認証解除	削除	移動前の認証解除	通信可
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

表 7-16 MAC 認証でのポート間移動時の動作 (ダイナミック VLAN モード)

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレス テーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	認証が継続される	ポート情報が更新	継続	通信可
2	認証対象ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信不可
3	認証対象外ポート	同一 VLAN	認証解除	削除	移動前の認証解除	通信可
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

7.4 レイヤ 2 認証使用時の注意事項

7.4.1 本装置の設定および状態変更時の注意

(1) set clock コマンドを使用する際の注意

認証接続時間を装置の時刻を用いて管理しているため、運用コマンド set clock で日時を変更した場合、認証接続時間に影響が出ます。

例えば、3 時間後の時刻に値を変更した場合、認証接続時間が 3 時間経過した状態となります。また、逆に 3 時間前の時刻に値を変更した場合は、認証接続時間が 3 時間延長されます。

(2) 認証モードを変更する場合の注意

Web 認証が有効な状態で認証モードを変更する、または MAC 認証が有効な状態で認証モードを変更する場合は、すべての認証対象ポートに対してコンフィグレーションコマンド shutdown を実行して認証端末が接続されていない状態にしたあと、約 60 秒の間隔をおいてから認証モードを変更してください。認証モードを変更したあと、すべての認証対象ポートに対してコンフィグレーションコマンド no shutdown を実行してください。

認証端末が接続されている状態で認証モードを変更した場合は、運用コマンド restart web-authentication または restart mac-authentication を実行して、Web 認証プログラムまたは MAC 認証プログラムを再起動してください。

7.4.2 RADIUS サーバ使用時の注意

(1) RADIUS サーバの設定でホスト名を指定した場合の注意事項

RADIUS サーバをホスト名で指定した場合、DNS サーバへ接続できないなどの理由によって名前解決ができない環境では、次に示す現象が発生することがあります。

運用コマンドを実行した場合

- 実行結果の表示が遅くなります。
- 表示が途中で止まり、しばらくして継続表示されます。
- IEEE802.1X では、「Connection failed to 802.1X program.」が表示されます。
- Web 認証および MAC 認証では、「Can't execute.」が表示されます。

コンフィグレーションコマンドを実行した場合

- コンフィグレーションの保存またはコンフィグレーションの反映に時間が掛かる場合があります。

SNMP マネージャによる IEEE802.1X MIB 情報を取得する場合

- 応答が遅くなる、または SNMP 受信タイムアウトになります。

上記の現象を避けるため、RADIUS サーバの設定に IPv4 アドレスまたは IPv6 アドレスで指定することを推奨します。ホスト名での指定が必要な場合は、必ず DNS サーバからの応答があることを確認してください。

(2) IEEE802.1X で RADIUS サーバとの通信が切れた場合の注意事項

IEEE802.1X では、RADIUS サーバとの通信が切れた場合、またはコンフィグレーションコマンド radius-server host で設定された RADIUS サーバが存在しない場合、ログイン要求 1 件ずつに対して、コ

ンフィグレーションコマンド `radius-server timeout` で指定されたタイムアウト時間およびコンフィグレーションコマンド `radius-server retransmit` で設定された再送回数分だけの時間が掛かるため、1 ログイン要求当たりの認証処理に時間が掛かります。

また、複数の RADIUS サーバが設定された場合でも、コンフィグレーションコマンド `radius-server host` の順にログインごとに毎回アクセスするため、先に設定された RADIUS サーバで障害などによって通信ができなくなると、認証処理に時間が掛かります。

このようなときは、ログイン操作をいったん止め、コンフィグレーションコマンド `radius-server host` で正常な RADIUS サーバを設定し直したあとに、ログイン操作を行ってください。

7.5 レイヤ2 認証共通コンフィグレーション

7.5.1 コンフィグレーションコマンド一覧

レイヤ2 認証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 7-17 コンフィグレーションコマンド一覧

コマンド名	説明	適用するレイヤ2 認証		
		IEEE802.1X	Web 認証	MAC 認証
authentication ip access-group	認証前状態の端末からのパケットを本装置の外部に転送したい場合、転送したいパケット種別を IPv4 アクセスリストで指定します。			

(凡例) : 設定可

注 Web 認証は固定 VLAN モードおよびダイナミック VLAN モードで適用します。

7.5.2 レイヤ2 認証共通コンフィグレーションコマンドのパラメータ設定

(1) 認証専用 IPv4 アクセスリストの設定

[設定のポイント]

認証前状態の端末から本装置の外部への通信を許可する認証専用 IPv4 アクセスリストを設定します。

[コマンドによる設定]

```
1. (config)# ip access-list extended 100
   (config-ext-nacl)# permit udp any any eq bootps
   (config-ext-nacl)# exit
   (config)# authentication ip access-group 100
```

認証前の端末から DHCP パケットを許可する認証専用 IPv4 アクセスリストを設定します。

8

IEEE802.1X の解説

IEEE802.1X は OSI 階層モデルの第 2 レイヤで認証を行う機能です。この章では IEEE802.1X の概要について説明します。

8.1 IEEE802.1X の概要

8.2 拡張機能の概要

8.3 IEEE802.1X 使用時の注意事項

8.1 IEEE802.1X の概要

IEEE802.1X は、不正な LAN 接続を規制する機能です。バックエンドに認証サーバ（一般的には RADIUS サーバ）を設置し、認証サーバによる端末の認証が通過した上で、本装置の提供するサービスを利用できるようにします。

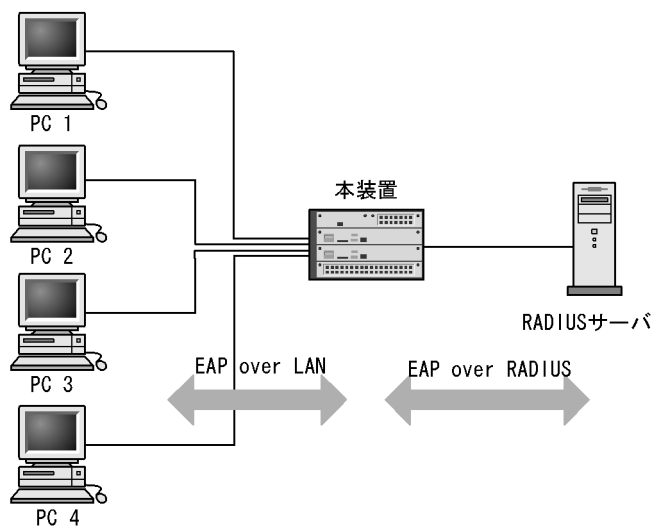
IEEE802.1X の構成要素と動作概略を次の表に示します。

表 8-1 構成要素と動作概略

構成要素	動作概略
本装置 (Authenticator)	端末の LAN へのアクセスを制御します。また、端末と認証サーバ間で認証情報のリレーを行います。端末と本装置間の認証処理にかかわる通信は EAP Over LAN(EAPOL) で行います。本装置と認証サーバ間は EAP Over RADIUS を使って認証情報を交換します。なお、本章では、「本装置」または「Authenticator」と表記されている場合、本装置自身と本装置に搭載されている Authenticator ソフトウェアの両方を意味します。
端末 (Supplicant)	EAPOL を使用して端末の認証情報を本装置とやりとりします。なお、本章では、「端末」または「Supplicant」と表記されている場合、端末自身と端末に搭載されている Supplicant ソフトウェアの両方を意味します。「Supplicant ソフトウェア」と表記されている場合、Supplicant 機能を持つソフトウェアだけを意味します。
認証サーバ (Authentication Server)	端末の認証を行います。認証サーバは端末の認証情報を確認し、本装置の提供するサービスへのアクセスを要求元の端末に許可すべきかどうかを本装置に通知します。

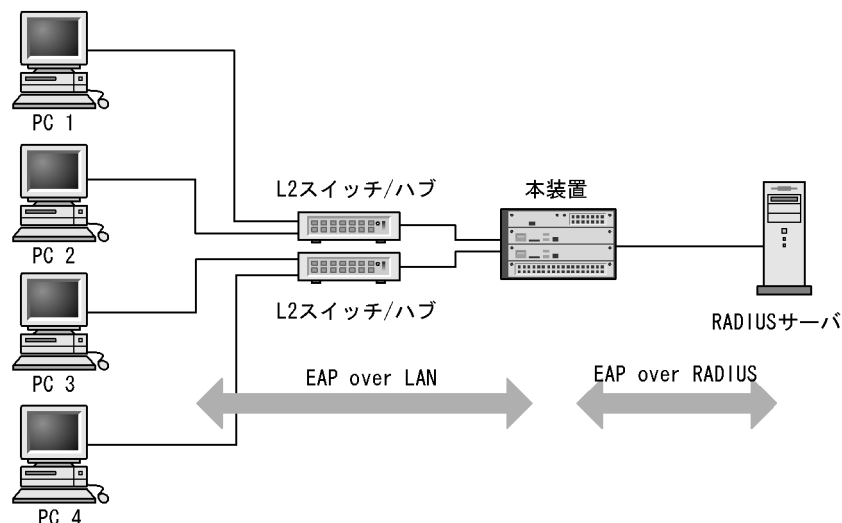
標準的な IEEE802.1X の構成では、本装置のポートに直接端末を接続して運用します。本装置を使った IEEE802.1X 基本構成を次の図に示します。

図 8-1 IEEE802.1X 基本構成



また、本装置では一つのポートで複数の端末の認証を行う拡張機能をサポートしています（マルチモードおよび端末認証モード）。本拡張機能を使用した場合、端末と本装置間に L2 スイッチやハブを配置することで、ポート数によって端末数が制限を受けない構成にできます。本構成を行う場合、端末と本装置間に配置する L2 スイッチは EAPOL を透過する必要があります。その場合の構成を次の図に示します。

図 8-2 端末との間に L2 スイッチを配置した IEEE802.1X 構成



8.1.1 サポート機能

本装置でサポートする機能を以下に示します。

(1) 認証動作モード

本装置でサポートする認証動作モード (PAE モード) は Authenticator です。本装置が Supplicant として動作することはありません。

(2) 認証方式

本装置でサポートする認証方式は RADIUS サーバ認証です。端末から受信した EAPOL パケットを EAPoverRADIUS に変換し、認証処理は RADIUS サーバで行います。RADIUS サーバは EAP 対応されている必要があります。

本装置が使用する RADIUS の属性名を「表 8-2 認証で使用する属性名 (その 1 Access-Request)」から「表 8-5 認証で使用する属性名 (その 4 Access-Reject)」に示します。

表 8-2 認証で使用する属性名 (その 1 Access-Request)

属性名	Type 値	説明
User-Name	1	認証されるユーザ名。
NAS-IP-Address	4	認証を要求している, Authenticator(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。
NAS-Port	5	Supplicant を認証している認証単位の IfIndex。
Service-Type	6	提供するサービスタイプ。 Framed(2) 固定。
Framed-MTU	12	Supplicant ~ Authenticator 間の最大フレームサイズ。 (1466) 固定。
State	24	Authenticator と RADIUS サーバ間の State 情報の保持を可能にする。
Called-Station-Id	30	ブリッジやアクセスポイントの MAC アドレス。本装置の MAC アドレス (ASCII, "-" 区切り)。

属性名	Type 値	説明
Calling-Station-Id	31	Supplicant の MAC アドレス (ASCII, "-" 区切り)。
NAS-Identifier	32	Authenticator を識別する文字列 (ホスト名の文字列)。
NAS-Port-Type	61	Authenticator がユーザ認証に使用している, 物理ポートのタイプ。Ethernet(15) 固定。
Connect-Info	77	Supplicant のコネクションの特徴を示す文字列。 ポート単位認証: 物理ポート ("CONNECT Ethernet") CH ポート ("CONNECT Port-Channel") VLAN 単位認証 (静的): ("CONNECT VLAN") VLAN 単位認証 (動的): ("CONNECT DVLAN")
EAP-Message	79	EAP パケットをカプセル化する。
Message-Authenticator	80	RADIUS/EAP パケットを保護するために使用する。
NAS-Port-Id	87	Supplicant を認証する Authenticator のポートを識別するための文字列。 ポート単位認証: "Port x/y", "ChGr x" VLAN 単位認証 (静的): "VLAN x" VLAN 単位認証 (動的): "DVLAN x" (x, y には数字が入る)
NAS-IPv6-Address	95	認証を要求している, Authenticator (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。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。

表 8-3 認証で使用する属性名 (その 2 Access-Challenge)

属性名	Type 値	説明
Reply-Message	18	ユーザに表示されるメッセージ。
State	24	Authenticator と RADIUS サーバ間の State 情報の保持を可能にする。
Session-Timeout	27	Supplicant へ送信した EAP-Request に対する応答待ちタイムアウト値。
EAP-Message	79	EAP パケットをカプセル化する。
Message-Authenticator	80	RADIUS/EAP パケットを保護するために使用する。

表 8-4 認証で使用する属性名 (その 3 Access-Accept)

属性名	Type 値	説明
Service-Type	6	提供するサービスタイプ。Framed(2) 固定。
Reply-Message	18	ユーザに表示されるメッセージ。
Session-Timeout	27	Supplicant の再認証タイム値。
Termination-Action	29	Radius サーバからの再認証タイム満了時のアクション指示。
Tunnel-Type	64	トンネル・タイプ。VLAN 単位認証 (動的) でだけ意味を持つ。VLAN(13) 固定。
Tunnel-Medium-Type	65	トンネルを作成する際のプロトコル。VLAN 単位認証 (動的) でだけ意味を持つ。IEEE802(6) 固定。
EAP-Message	79	EAP パケットをカプセル化する。

属性名	Type 値	説明
Message-Authenticator	80	RADIUS/EAP パケットを保護するために使用する。
Tunnel-Private-Group-ID	81	VLAN を識別する文字列。Accept 時は、認証済みの Supplicant に割り当てる VLAN を意味する。 VLAN 単位認証（動的）でだけ意味を持つ。 次に示す文字列が対応する。 (1)VLAN ID を示す文字列 (2)"VLAN"+VLAN ID を示す文字列 文字列にスペースを含んではいけない（含めた場合 VLAN 割り当ては失敗する）。 （設定例） VLAN10 の場合 (1) の場合 "10" (2) の場合 "VLAN10"
Acct-Interim-Interval	85	Interim パケット送信間隔（秒）。 60 以上を設定すると Interim パケットが送信される（60 未満では送信しない）。 この値を設定する場合、600 以上にすることを推奨する。600 未満にした場合ネットワークのトラフィックが増大するため注意が必要である。

注

RADIUS から返送される Access-Accept で Termination-Action が Radius-Request(1) の場合、同時に設定された Session-Timeout の値が、再認証するまでの時間（単位：秒）となります。なお、Session-Timeout の値によって次に示す動作となります。

0 : 再認証は無効となります。

1 ~ 60 : 再認証タイマ値を 60 秒として動作します。

61 ~ 65535 : 設定された値で動作します。

表 8-5 認証で使用する属性名（その 4 Access-Reject）

属性名	Type 値	説明
Reply-Message	18	ユーザに表示されるメッセージ。
EAP-Message	79	EAP パケットをカプセル化する。
Message-Authenticator	80	RADIUS/EAP パケットを保護するために使用する。

(3) 認証アルゴリズム

本装置でサポートする認証アルゴリズムを次の表に示します。

表 8-6 サポートする認証アルゴリズム

認証アルゴリズム	概要
EAP-MD5-Challenge	UserPassword とチャレンジ値の比較を行う。
EAP-TLS	証明書発行機構を使用した認証方式。
EAP-PEAP	EAP-TLS トンネル上で、ほかの EAP 認証アルゴリズムを用いて認証する。
EAP-TTLS	EAP-TLS トンネル上で、他方式 (EAP, PAP, CHAP など) の認証アルゴリズムを用いて認証する。

(4) RADIUS Accounting 機能

本装置は RADIUS Accounting 機能をサポートします。この機能は IEEE802.1X 認証で認証許可となった端末へのサービス開始やサービス停止のタイミングでユーザアカウント情報を送信し、利用状況追

跡を行えるようにするための機能です。RADIUS Authentication サーバと RADIUS Accounting サーバを別のサーバに設定することによって、認証処理とアカウント処理の負荷を分散させることができます。

RADIUS Accounting 機能を使用する際に、RADIUS サーバに送信される情報を次の表に示します。

表 8-7 RADIUS Accounting がサポートする属性

属性名	Type 値	解説	アカウント処理要求種別による送信の有無		
			start	stop	Interim-Update
User-Name	1	認証されるユーザ名。			
NAS-IP-Address	4	認証を要求している、Authenticator(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。			
NAS-Port	5	Supplicant を認証している認証単位の IfIndex。			
Service-Type	6	提供するサービスタイプ。 Framed(2) 固定。			
Calling-Station-Id	31	Supplicant の MAC アドレス (ASCII, "-" 区切り)			
NAS-Identifier	32	Authenticator を識別する文字列。(ホスト名の文字列)			
Acct-Status-Type	40	Accounting 要求種別 Start(1), Stop(2), Interim-Update(3)			
Acct-Delay-Time	41	Accounting 情報送信遅延時間(秒)			
Acct-Input-Octets	42	Accounting 情報(受信オクテット数)。 (0) 固定。	-		
Acct-Output-Octets	43	Accounting 情報(送信オクテット数)。 (0) 固定。	-		
Acct-Session-Id	44	Accounting 情報を識別する ID。			
Acct-Authentic	45	認証方式 (RADIUS(1), Local(2), Remote(3))			
Acct-Session-Time	46	Accounting 情報(セッション持続時間)	-		
Acct-Input-Packets	47	Accounting 情報(受信パケット数)。 (0) 固定。	-		
Acct-Output-Packets	48	Accounting 情報(送信パケット数)。 (0) 固定。	-		
Acct-Terminate-Cause	49	Accounting 情報(セッション終了要因) 詳細は、「表 8-8 Acct-Terminate-Cause での切断要因」を参照。 User Request (1), Lost Carrier (2), Admin Reset (6), Reauthentication Failure (20), Port Reinitialized (21)	-		-
NAS-Port-Type	61	Authenticator がユーザ認証に使用している、物理ポートのタイプ。 Ethernet(15) 固定。			

属性名	Type 値	解説	アカウントング要求種別による送信の有無		
			start	stop	Interim-Update
NAS-Port-Id	87	Supplicant を認証する Authenticator のポートを識別するために使用する。 NAS-Port-Id は、可変長のストリングであり、NAS-Port が長さ 4 オクテットの整数値である点で NAS-Port と異なる。 ポート単位認証：“Port x/y”，“ChGr x” VLAN 単位認証（静的）：“VLAN x” VLAN 単位認証（動的）：“DVLAN x” (x, y には数字が入る)			
NAS-IPv6-Address	95	認証を要求している、Authenticator(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。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。			

(凡例) : 送信する - : 送信しない

表 8-8 Acct-Terminate-Cause での切断要因

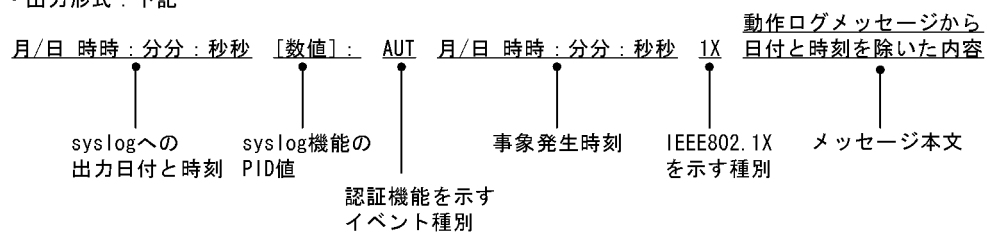
切断要因	値	解説
User Request	1	Supplicant からの要求で切断した。 • 認証端末から logoff を受信した場合
Lost Carrier	2	モデムのキャリア信号がなくなった。 • 内部エラー
Admin Reset	6	管理者の意思で切断した。 • 認証単位でコンフィグレーションを削除した場合 • force-authorized を設定した場合 • force-unauthorized を設定した場合 • force-authorized-port を設定した場合
Reauthentication Failure	20	再認証に失敗した。
Port Reinitialized	21	ポートの MAC が再初期化された。 • リンクダウンした場合 • clear dot1x auth-state を実行した場合

(5) syslog サーバへの動作ログ記録

IEEE802.1X の内部動作ログを syslog サーバに出力できます。なお、内部動作ログと同じ項目が出力されます。syslog サーバへの出力形式を次の図に示します。

図 8-3 syslog サーバへの出力形式

- ・ イベント種別 : AUT
- ・ 出力形式 : 下記



また、コンフィグレーションコマンド dot1x logging enable および logging event-kind によって、出力を開始および停止できます。

8.2 拡張機能の概要

本装置では、標準的な IEEE802.1X に対して機能拡張を行っています。拡張機能の概要を以下に示します。

8.2.1 認証モード

本装置の IEEE802.1X では、三つの基本認証モードとその下に三種類の認証サブモードを設けています。基本認証モードは、認証制御を行う単位を示し、認証サブモードは認証のさせ方を指定します。また、基本認証モードと認証サブモードに対して設定可能なオプションを設けています。各認証モードの関係を次の表に示します。

表 8-9 認証モードとオプションの関係

基本認証モード	認証サブモード	認証オプション
ポート単位認証	シングルモード	-
	マルチモード	-
	端末認証モード	認証除外端末オプション 認証端末数制限オプション
VLAN 単位認証（静的）	端末認証モード	認証除外端末オプション
		認証除外ポートオプション
		認証端末数制限オプション
VLAN 単位認証（動的）	端末認証モード	認証除外端末オプション
		認証端末数制限オプション
		認証デフォルト VLAN

（凡例） - : 該当なし

本装置の IEEE802.1X では、チャンネルグループについても一つの束ねられたポートとして扱います。この機能での「ポート」の表現には通常のポートとチャンネルグループを含むものとします。

（1）基本認証モード

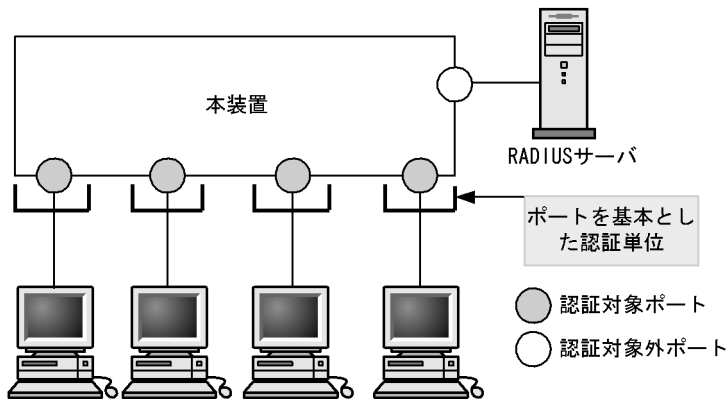
本装置でサポートする基本認証モードを以下に示します。

（a）ポート単位認証

認証の制御を物理ポートまたはチャンネルグループに対して行います。IEEE802.1X の標準的な認証単位です。この認証モードでは IEEE 802.1Q VLAN Tag の付与された EAPOL フレームを扱うことはできません。IEEE 802.1Q VLAN Tag の付与された EAPOL フレームを受信すると廃棄します。

ポート単位認証の構成例を次の図に示します。

図 8-4 ポート単位認証の構成例

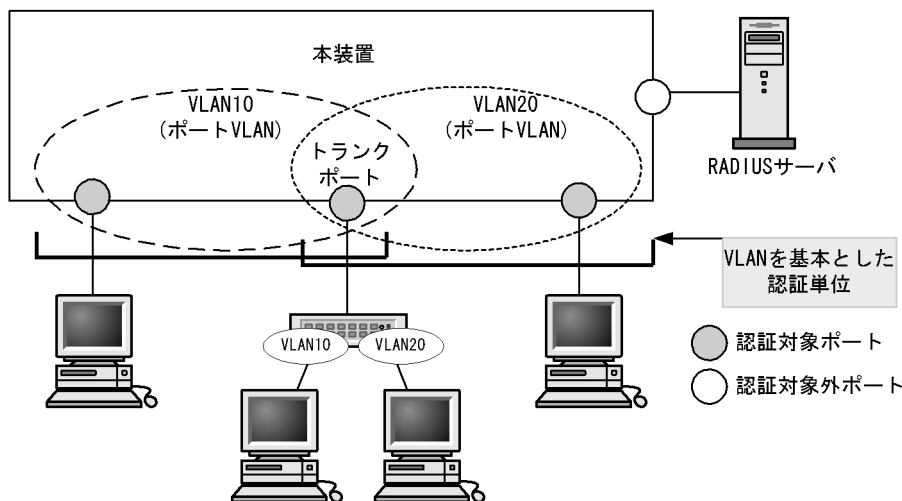


(b) VLAN 単位認証 (静的)

認証の制御を VLAN に対して行います。IEEE 802.1Q VLAN Tag の付与された EAPOL フレームを扱うことができます。端末と本装置の間に L2 スイッチを配置し、L2 スイッチを用いて IEEE 802.1Q VLAN Tag の付与を行う場合に使用します。Tag の付与されていない EAPOL フレームについては、ポートに設定されているネイティブ VLAN で受信したと認識します。

VLAN 単位認証 (静的) の構成例を次の図に示します。

図 8-5 VLAN 単位認証 (静的) の構成例



(c) VLAN 単位認証 (動的)

認証の制御を MAC VLAN に所属する端末に対して行います。IEEE 802.1Q VLAN Tag の付与された EAPOL フレームを扱うことができません。このフレームを受信した場合には破棄します。

指定された MAC VLAN のトランクポートおよびアクセスポートは認証除外ポートとして扱われます。

認証に成功した端末は、認証サーバである RADIUS サーバからの VLAN 情報 (MAC VLAN の VLAN ID) に従い、動的に VLAN の切り替えを行います。

VLAN 単位認証 (動的) の構成例と動作イメージを次の図に示します。

図 8-6 VLAN 単位認証 (動的) の構成例

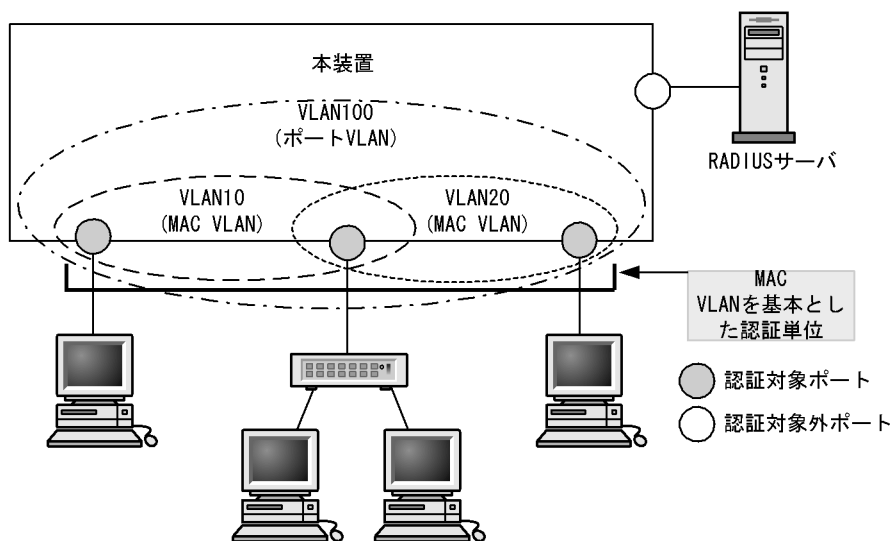
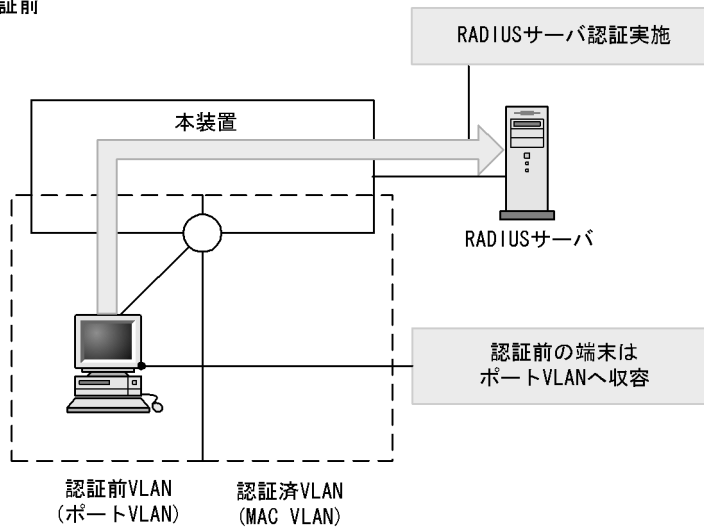
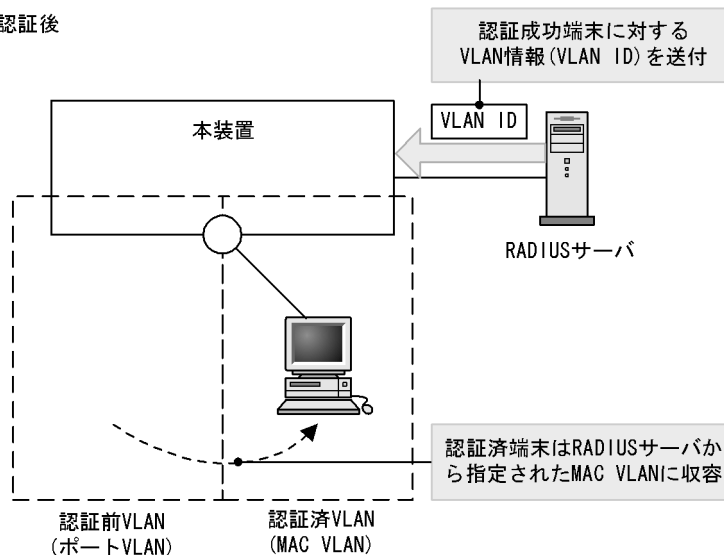


図 8-7 VLAN 単位認証（動的）の動作イメージ

● 認証前



● 認証後



(2) 認証サブモード

基本認証モードに対して設定する認証サブモードを以下に示します。

(a) シングルモード

一つの認証単位内に一つの端末だけ認証して接続するモードです。IEEE802.1X の標準的な認証モードです。最初の端末が認証している状態でほかの端末からの EAP を受信すると、そのポートの認証状態は未認証状態に戻り、コンフィグレーションコマンドで指定された時間が経過したあとに認証シーケンスを再開します。

(b) マルチモード

一つの認証単位内に複数端末の接続を許容しますが、認証対象の端末はあくまで最初に EAP を受信した 1 端末だけのモードです。最初に認証を受けた端末の認証状態に応じて、そのほかの端末の packets を通信するかどうかが決まります。最初の端末が認証されている状態でほかの端末の EAP を受信すると無視し

ます。

(c) 端末認証モード

一つの認証単位内に複数端末の接続を許容し、端末ごと（送信元 MAC アドレスで識別）に認証を行うモードです。端末が認証されている状態でほかの端末の EAP を受信すると、EAP を送信した端末との間で個別の認証シーケンスが開始されます。

(3) 認証モードオプション

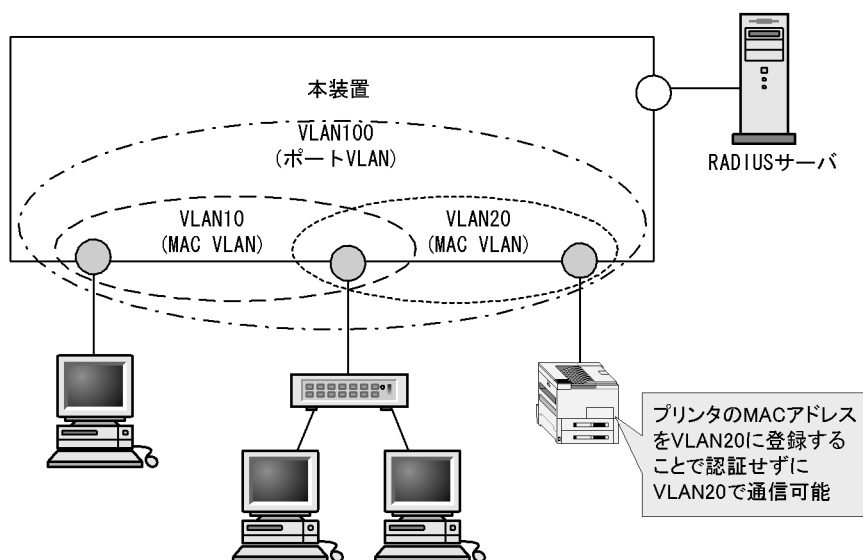
認証モード / 認証サブモードに対するオプション設定を以下に示します。

(a) 認証除外端末オプション

スタティック MAC アドレス学習機能および MAC VLAN 機能によって MAC アドレスが設定された端末については認証を不要とし、通信を許可するオプション設定です。Supplicant 機能を持たないプリンタなどの装置やサーバなど認証が不要な端末を、端末単位で認証対象から除外したいときに使用します。端末認証モードの場合だけ使用可能なオプションです。

VLAN 単位認証（動的）での認証除外端末構成例を次の図に示します。

図 8-8 VLAN 単位認証（動的）での認証除外端末構成例



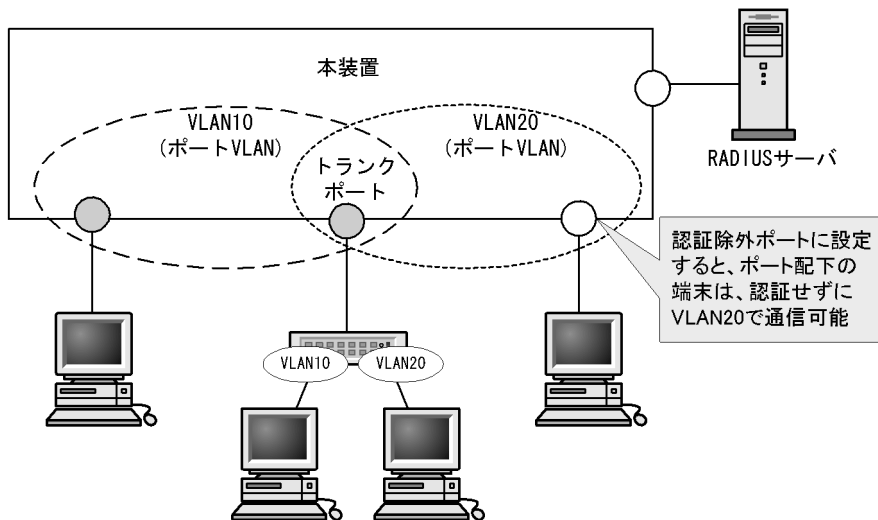
(b) 認証除外ポートオプション

特定の物理ポート番号またはチャンネルグループ番号を指定することで、その物理ポートまたはチャンネルグループ配下の端末については認証を不要とし、通信を許可するオプション設定です。VLAN 単位認証（静的）の場合だけ使用可能であり、認証対象となる VLAN の中に認証対象外としたいポートがある場合に使用します。

同一ポートに複数の VLAN 単位認証（静的）の VLAN を設定している場合、すべての VLAN で認証除外ポートとなります。

VLAN 単位認証（静的）での認証除外ポート構成例を次の図に示します。

図 8-9 VLAN 単位認証（静的）での認証除外ポート構成例



(c) 認証端末数制限オプション

認証単位内に収容する最大認証端末数を制限するオプション設定です。端末認証モードだけで有効です。認証単位ごとの設定値を次の表に示します。

表 8-10 認証端末数制限オプション

認証モード	初期値	最小値	最大値
ポート単位認証	256	1	256
VLAN 単位認証（静的）	256	1	256
VLAN 単位認証（動的）	4096	1	4096

(d) 認証デフォルト VLAN 機能

認証デフォルト VLAN 機能は、IEEE802.1X に未対応などの理由によって MAC VLAN に収容できない端末をポート VLAN に収容する機能です。VLAN 単位認証（動的）に設定したポートに対してポート VLAN またはデフォルト VLAN が設定されている場合、その VLAN は認証デフォルト VLAN として動作します。次に示すような場合、端末は認証デフォルト VLAN に収容します。

- IEEE802.1X 未対応の端末
- 認証前の IEEE802.1X 対応の端末
- 認証または再認証に失敗した端末
- RADIUS サーバから指定された VLAN ID が MAC VLAN でない場合
- RADIUS サーバから指定された VLAN ID がポートに設定されていない場合

8.2.2 端末検出動作切り替えオプション

端末の認証開始を誘発するために、本装置は tx-period コマンドで指定した間隔で EAP-Request/Identity をマルチキャスト送信します。認証サブモードが端末認証モードの場合、認証単位に複数の端末が存在する可能性があるため、本装置ではすべての端末の認証が完了するまで EAP-Request/Identity の送信を継続することをデフォルトの動作としています。このとき、認証単位当たりの端末数が増えると EAP-Request/Identity に応答した端末の認証処理で装置に負荷を掛けるおそれがあるため、認証済み端末からの応答には認証シーケンスを一部省略することで、装置の負荷を低減しています。

ただし、使用する Supplicant ソフトウェアの種類によっては、認証シーケンスの省略によって認証済み端末の通信が途切れる問題が発生することがあります。そのため、認証済み端末に対する動作を切り替えるオプションを用意しています。本オプションは supplicant-detection コマンドで選択を行い、次に示す二種類の動作を指定できます。

(1) shortcut

装置の負荷を低減するため、認証済み端末に対する EAP-Request/Identity 契機の認証シーケンスを一部省略します。一部の Supplicant ソフトウェアを本モードで使用すると、EAP-Request/Identity による認証時に認証済み端末との通信が途切れる場合があります。そのときに、使用する Supplicant ソフトウェアが EAP-Start を自発的に送信できる場合は disable を指定してください。

(2) disable

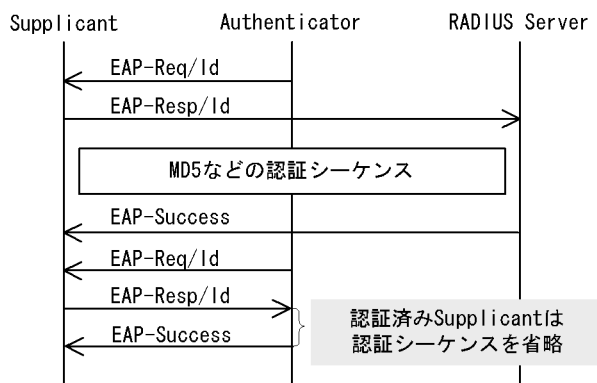
認証済み端末が存在する場合は EAP-Request/Identity の送信を停止します。本モードは未認証の端末からフレームを受信した場合に、その端末に対して本装置から EAP-Request/Identity を送信し、認証の開始を促します。VLAN 単位認証（動的）で使用する場合には、ポートで認証デフォルト VLAN の設定が必要です。

自発的に EAP-Start を送信しない Supplicant ソフトウェアと、認証シーケンスを省略すると問題の発生する Supplicant ソフトウェアとを混在して使用する場合に指定してください。

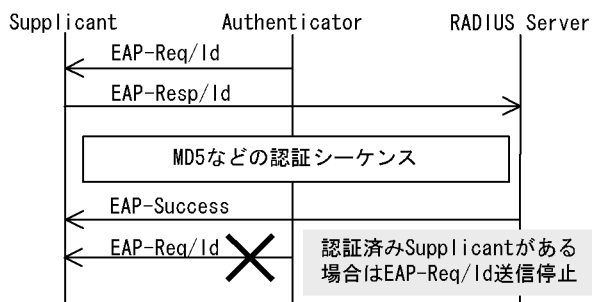
それぞれの動作シーケンスを次の図に示します。

図 8-10 shortcut, disable の EAP-Request/Identity のシーケンス

●shortcut指定時のシーケンス（デフォルト）



●disable指定時のシーケンス



8.2.3 端末要求再認証抑止機能

端末から送信される EAPOL-Start を契機とする再認証処理を抑止する機能です。多数の端末から短い間隔で再認証要求が行われるような場合に、再認証処理のために本装置の負荷が上昇するのを防ぎます。本機能の設定が行われている場合、端末の再認証は本装置がコンフィグレーションで指定した時間間隔で行う定期的な再認証処理で行われます。

8.2.4 RADIUS サーバ接続機能

(1) RADIUS サーバとの接続

RADIUS サーバは最大 4 台まで指定できます。指定時には、サーバの IPv4 アドレス、IPv6 アドレスまたはホスト名を指定できますが、IEEE802.1X では IPv4 アドレスまたは IPv6 アドレスでの指定を推奨します。ホスト名を指定する場合は、「7.4.2 RADIUS サーバ使用時の注意」を参照の上、指定してください。ホスト名を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 IP アドレスを一つ決定し、RADIUS サーバと通信を行います。優先順序の詳細については、マニュアル「コンフィグレーションガイド Vol.1 10.1 解説」を参照してください。また、本装置と RADIUS サーバとの接続は、認証の対象外となっているポートを使用してください。

RADIUS サーバへの接続は、コンフィグレーションの順に行い、接続に失敗したときは次の RADIUS サーバとの接続を試みます。すべての RADIUS サーバとの接続に失敗した場合は、端末に EAP-Failure を送信して認証シーケンスを終了します。

RADIUS サーバとの接続後に認証シーケンスの途中で通信タイムアウトを検出した場合は、端末に EAP-Failure を送信し、認証シーケンスを終了します。

(2) VLAN 単位認証（動的）で VLAN を動的に割り当てるときの設定

本装置でサポートする VLAN 単位認証（動的）で VLAN の動的割り当てを実施する場合、RADIUS サーバへ次に示す属性を設定する必要があります。属性の詳細については、「表 8-4 認証で使用する属性名（その 3 Access-Accept）」を参照してください。

- Tunnel-Type
- Tunnel-Medium-Type
- Tunnel-Private-Group-Id

(3) RADIUS サーバでの本装置の識別の設定

RADIUS プロトコルでは RADIUS クライアント（NAS）を識別するキーとして、要求パケットの送信元 IP アドレスを使用するよう規定されています。本装置では要求パケットの送信元 IP アドレスとして次に示すアドレスを使用します。

- 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送信元 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 アドレスを送信元 IP アドレスとして使用します。

本装置にローカルアドレスが設定されている場合、RADIUS サーバに登録する本装置の IP アドレスとして、ローカルアドレスで指定した IP アドレスを指定してください。RADIUS サーバと通信する送信インタフェースが特定できない場合であっても、ローカルアドレスを設定することによって、RADIUS サーバに設定する本装置の IP アドレスを特定できるようになります。

8.2.5 EAPOL フォワーディング機能

IEEE802.1X を使用しない VLAN で EAPOL フレームを中継する機能です。EAPOL フレームは宛先 MAC アドレスが IEEE 802.1D で予約されているアドレスであるため通常は中継を行いませんが、IEEE802.1X を使用していない場合はこの機能によって中継が可能です。ほかの Authenticator と端末の間の L2 スイッチとして本装置を使用する場合に設定します。

本機能の設定例は、マニュアル「コンフィグレーションガイド Vol.1 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」を参照してください。

8.2.6 VLAN 単位認証（動的）の動作モード

VLAN 単位認証（動的）の対象ポートで次に示す設定がある場合、認証デフォルト VLAN 機能は動作しなくなります。

- Web 認証（ダイナミック VLAN モード）を設定したポート
- MAC 認証（ダイナミック VLAN モード）を設定したポート

8.3 IEEE802.1X 使用時の注意事項

(1) 他機能との共存

IEEE802.1X と他機能との共存仕様については、「7.2 レイヤ 2 認証と他機能との共存について」を参照してください。

(2) MAC VLAN をアクセスポートとして指定した場合の注意事項

- VLAN 単位認証（動的）の MAC VLAN をアクセスポートとして指定した場合、本装置の指定したポートから EAPOL フレームが送信されますが、ユーザ側で EAPOL フレームに対する認証応答を行っても、指定ポートは認証除外ポートとして扱われますので認証成功または失敗に関わらず、指定ポートでの疎通が可能となります。
- MAC VLAN をアクセスポートとして指定したインタフェースにポート単位認証を設定できますが、共存はできませんので使用しないでください。

(3) Interim パケットの送信間隔についての注意事項

RADIUS Accounting の Interim パケットを使用する場合、RADIUS パケットの Acct-Interim-Interval 属性で指定される送信間隔は、600 以上の値を設定することを推奨します。600 より小さい値を設定した場合、全認証済端末数の Interim パケットが送信されるので RADIUS サーバおよびネットワークの負荷が増大するため注意が必要です。

(4) スタティックエントリ登録 MAC と VLAN 単位認証（動的）モードの共存についての注意事項

VLAN 単位認証（動的）を設定している VLAN 内の MAC VLAN モードのインタフェースに対し、`mac-address-table static` コマンドで MAC アドレステーブルにスタティックエントリが登録されていると、該当する端末は正常に認証処理を行うことができません。

(5) VLAN 単位認証（動的）での MAC アドレス学習のエイジング時間設定について

VLAN 単位認証（動的）を使用する場合、指定する MAC VLAN と認証デフォルト VLAN として使用するポート VLAN では、MAC アドレスエントリのエイジング時間に 0（無限）を指定しないでください。0（無限）を指定すると、端末の所属する VLAN が切り替わったときに、切り替わる前の VLAN の MAC アドレスエントリがエイジングで消去されないで残り続けるため、不要な MAC アドレスエントリが蓄積することになります。切り替わる前の VLAN に不要な MAC アドレスエントリが蓄積した場合は、`clear mac-address-table` コマンドで消去してください。

(6) タイマ値の変更について

タイマ値（`tx-period`、`reauth-period`、`supp-timeout`、`quiet-period`、`keep-unauth`）を変更した場合、変更した値が反映されるのは、各認証単位で現在動作中のタイマがタイムアウトして 0 になったときです。すぐに変更を反映させたい場合には、`clear dot1x auth-state` コマンドを使用して認証状態をいったん解除してください。

(7) 端末と本装置の間に L2 スイッチを配置する場合の注意事項

端末からの応答は一般的にマルチキャストとなるため、端末と本装置の間に L2 スイッチを配置する場合、端末からの応答による EAPOL フレームは L2 スイッチの同一 VLAN の全ポートへ転送されます。したがって、L2 スイッチの VLAN を次のように設定すると、同一端末からの EAPOL フレームが本装置の複数のポートへ届き、複数のポートで同一端末に対する認証処理が行われるようになります。そのため、認

証動作が不安定になり、通信が切断されたり、認証ができなくなったりします。

- L2 スwitchの同一 VLAN に設定されているポートを、本装置の認証対象となっている複数のポートに接続した場合
- L2 スwitchの同一 VLAN に設定されているポートを、複数の本装置の認証対象となっているポートに接続した場合

端末と本装置の間に L2 スwitchを配置する場合の禁止構成例と正しい構成例を次の図に示します。

図 8-11 禁止構成例

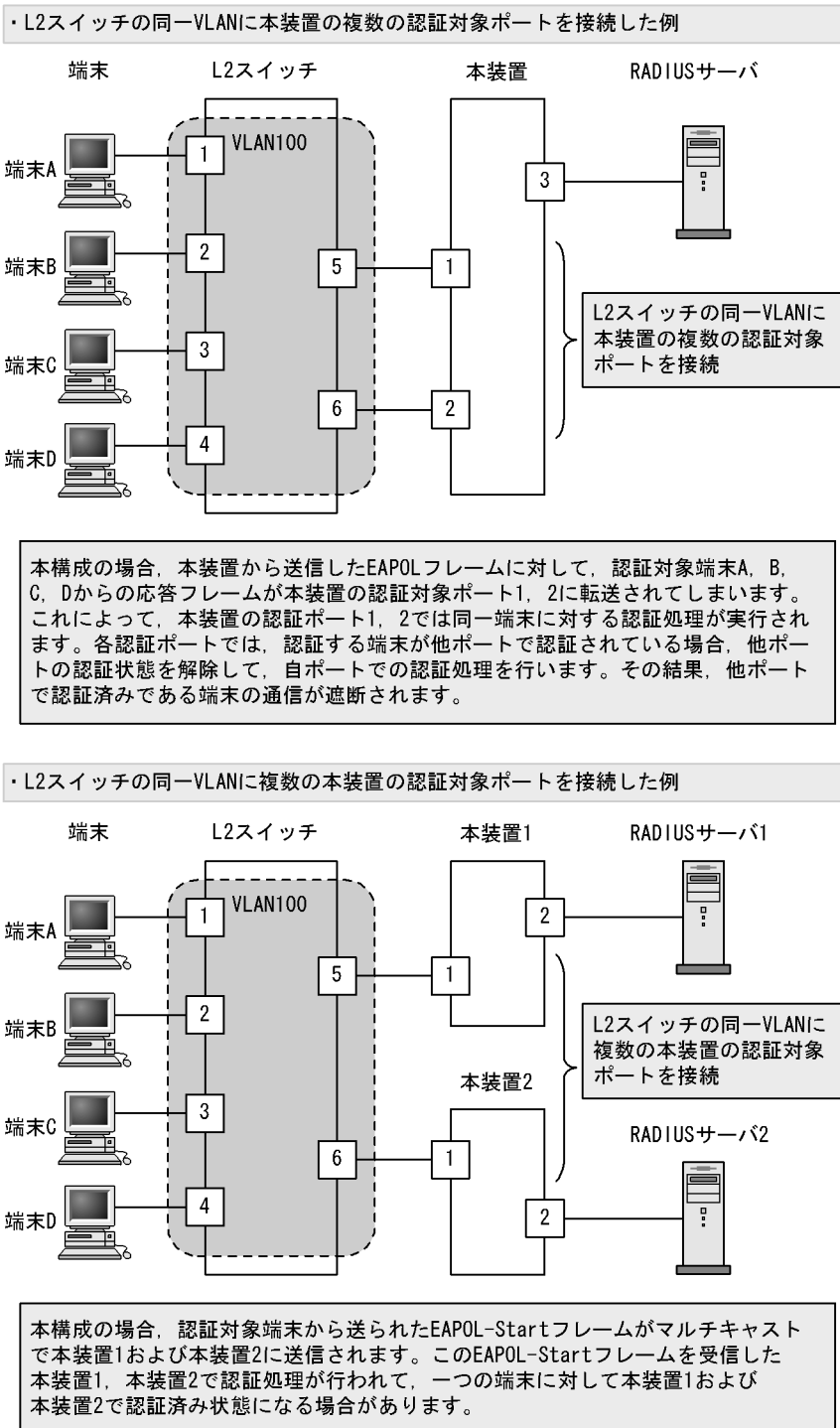
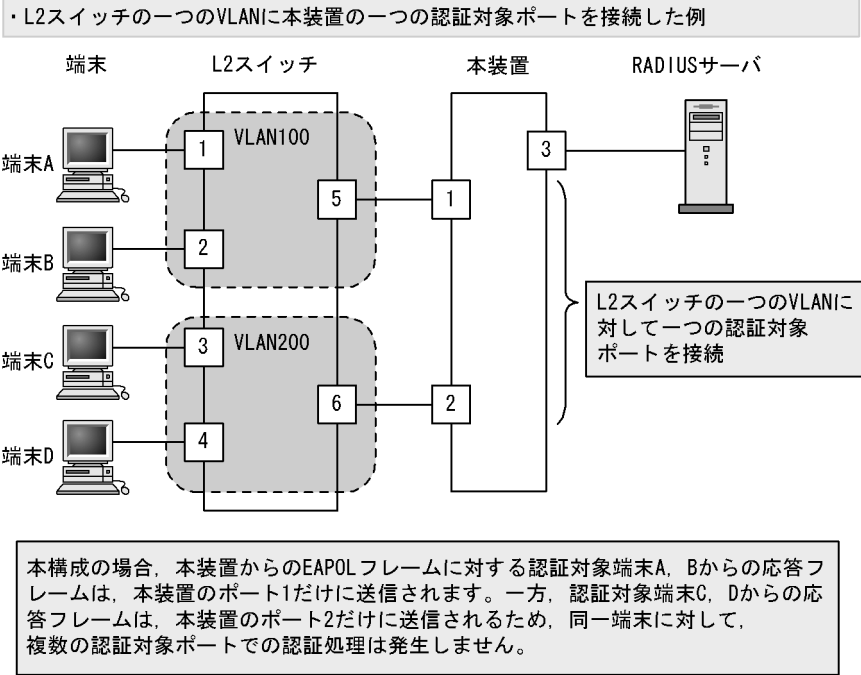


図 8-12 正しい構成例



9

IEEE802.1X の設定と運用

IEEE802.1X は OSI 階層モデルの第 2 レイヤで認証を行う機能です。この章では、IEEE802.1X のオペレーションについて説明します。

9.1 IEEE802.1X のコンフィグレーション

9.2 IEEE802.1X のオペレーション

9.1 IEEE802.1X のコンフィグレーション

9.1.1 コンフィグレーションコマンド一覧

IEEE802.1X 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 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
aaa accounting dot1x default	RADIUS サーバでアカウント集計を行う場合に設定します。
aaa authentication dot1x default	IEEE802.1X のユーザ認証を RADIUS サーバで行うことを設定します。
aaa authorization network default	RADIUS サーバから指定された VLAN 情報に従って、VLAN 単位認証（動的）を行う場合に設定します。
dot1x force-authorized-port	VLAN 単位認証（静的）で、認証不要で通信を許可するポートまたはチャンネルグループを設定します。
dot1x ignore-eapol-start dot1x vlan ignore-eapol-start dot1x vlan dynamic ignore-eapol-start	Supplicant からの EAPOL-Start 受信時に、EAP-Request/Identity を送信しない設定をします。
dot1x logging enable	IEEE802.1X の動作ログに出力する情報を syslog サーバへ出力します。
dot1x loglevel	動作ログメッセージを記録するメッセージレベルを指定します。
dot1x max-req dot1x vlan max-req dot1x vlan dynamic max-req	Supplicant からの応答がない場合に EAP-Request/Identity を再送する最大回数を設定します。
dot1x max-supplicant dot1x vlan max-supplicant dot1x vlan dynamic max-supplicant	認証単位の最大認証端末数を設定します。
dot1x multiple-hosts dot1x multiple-authentication	ポート単位認証の認証サブモードを設定します。
dot1x port-control	ポート単位認証を有効にします。
dot1x reauthentication dot1x vlan reauthentication dot1x vlan dynamic reauthentication	認証済み端末の再認証の有効 / 無効を設定します。
dot1x supplicant-detection dot1x vlan supplicant-detection dot1x vlan dynamic supplicant-detection	認証サブモードに端末認証モードを指定したときの端末検出動作のオプションを設定します。
dot1x system-auth-control	IEEE802.1X を有効にします。
dot1x timeout keep-unauth	ポート単位認証のシングルモードで、複数の端末からの認証要求を検出したときに、そのポートでの通信遮断状態を保持する時間を設定します。
dot1x timeout quiet-period dot1x vlan timeout quiet-period dot1x vlan dynamic timeout quiet-period	認証（再認証を含む）に失敗した Supplicant の認証処理再開を許可するまでの待機時間を設定します。
dot1x timeout reauth-period dot1x vlan timeout reauth-period dot1x vlan dynamic timeout reauth-period	認証済み端末の再認証を行う間隔を設定します。
dot1x timeout server-timeout dot1x vlan timeout server-timeout dot1x vlan dynamic timeout server-timeout	認証サーバからの応答待ち時間を設定します。

コマンド名	説明
dot1x timeout supp-timeout dot1x vlan timeout supp-timeout dot1x vlan dynamic timeout supp-timeout	Supplicant へ送信した EAP-Request/Identity に対して、Supplicant からの応答待ち時間を設定します。
dot1x timeout tx-period dot1x vlan timeout tx-period dot1x vlan dynamic timeout tx-period	定期的な EAP-Request/Identity の送信間隔を設定します。
dot1x vlan enable	VLAN 単位認証（静的）を有効にします。
dot1x vlan dynamic enable	VLAN 単位認証（動的）を有効にします。
dot1x vlan dynamic radius-vlan	VLAN 単位認証（動的）で、RADIUS サーバからの VLAN 情報により動的な VLAN 割り当てを許可する VLAN を設定します。

9.1.2 IEEE802.1X の基本的な設定

IEEE802.1X の基本認証モード設定について説明します。

(1) IEEE802.1X を有効にする設定

[設定のポイント]

グローバルコンフィグレーションモードで IEEE802.1X を有効にします。このコマンドを実行しないと、IEEE802.1X のほかのコマンドが有効になりません。

[コマンドによる設定]

1. (config)# dot1x system-auth-control
IEEE802.1X を有効にします。

(2) ポート単位認証の設定

物理ポートまたはチャンネルグループを認証の対象に設定します。

[設定のポイント]

アクセスポートを設定し、そのポートでポート単位認証を有効にします。認証サブモードを設定します。認証サブモードの設定を省略するとシングルモードになります。

[コマンドによる設定]

1. (config)# interface gigabitethernet 1/1
(config-if)# switchport mode access
ポート 1/1 に access モードを設定します。
2. (config-if)# dot1x multiple-authentication
認証サブモードを端末認証モードに指定します。
3. (config-if)# dot1x port-control auto
ポート単位認証を有効にします。

(3) VLAN 単位認証（静的）の設定

ポート VLAN を認証の対象に設定します。

[設定のポイント]

ポート VLAN を設定し、その VLAN で VLAN 単位認証（静的）を有効にします。

[コマンドによる設定]

1. `(config)# vlan 10`
`(config-vlan)# state active`
`(config-vlan)# exit`
VLAN ID 10 にポート VLAN を設定します。
2. `(config)# dot1x vlan 10 enable`
VLAN ID 10 で VLAN 単位認証（静的）を有効にします。

(4) VLAN 単位認証（動的）の設定

MAC VLAN を認証の対象に設定します。

[設定のポイント]

MAC VLAN を設定し、その VLAN で VLAN 単位認証（動的）を有効にします。

また、VLAN 単位認証（動的）認証に成功した端末を RADIUS サーバから指定された VLAN 情報に従い登録するためには、コンフィギュレーションコマンド `aaa authorization network default` の設定も必要となります。

[コマンドによる設定]

1. `(config)# vlan 100 mac-based`
`(config-vlan)# state active`
`(config-vlan)# exit`
VLAN ID 100 に MAC VLAN を設定します。
2. `(config)# dot1x vlan dynamic radius-vlan 100`
VLAN ID 100 を VLAN 単位認証（動的）の対象に設定します。
3. `(config)# dot1x vlan dynamic enable`
VLAN 単位認証（動的）を有効にします。

9.1.3 認証モードオプションの設定

認証モードオプションやパラメータの設定について説明します。

(1) 認証除外端末オプションの設定

IEEE802.1X を持たない端末など、認証を行わないで通信を許可する端末の MAC アドレスを設定します。

[設定のポイント]

ポート単位認証、VLAN 単位認証（静的）では、MAC アドレステーブルにスタティックなエントリを登録します。VLAN 単位認証（動的）では、MAC VLAN に MAC アドレスを登録します。

[コマンドによる設定](ポート単位認証)

1. `(config)# interface gigabitethernet 1/1`

```
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# dot1x multiple-authentication
(config-if)# dot1x port-control auto
(config-if)# exit
```

ポート 1/1 に VLAN ID 10 を設定し、認証サブモードが端末認証モードのポート単位認証を設定します。

```
2. (config)# mac-address-table static 0012.e200.0001 vlan 10 interface
gigabitethernet 1/1
```

ポート 1/1 の VLAN ID 10 に認証しないで通信させたい MAC アドレス (0012.e200.0001) をスタティックに設定します。

[コマンドによる設定] (VLAN 単位認証 (動的))

```
1. (config)# vlan 100 mac-based
(config-vlan)# mac-address 0012.e200.0001
(config-vlan)# exit
```

VLAN ID 100 の MAC VLAN で通信可能とする端末の MAC アドレスを設定します。端末は、IEEE802.1X の認証を行わないで VLAN ID 100 で通信できます。

```
2. (config)# dot1x vlan dynamic radius-vlan 100
(config)# dot1x vlan dynamic enable
```

VLAN ID 100 を VLAN 単位認証 (動的) の対象に設定して有効にします。

(2) 認証除外ポートオプションの設定

[設定のポイント]

VLAN 単位認証 (静的) を設定した VLAN に所属するポートで、認証を行わずに通信を許可するポートを設定します。ポートに複数の VLAN を設定している場合は、すべての VLAN について認証を行わずに通信が可能になります。

[コマンドによる設定]

```
1. (config)# interface gigabitethernet 1/1
(config-if)# dot1x force-authorized-port
```

VLAN 単位認証 (静的) を指定した VLAN に属しているポート 1/1 では認証を行わず、通信できるように設定します。

[注意事項]

認証除外ポートに VLAN 単位認証 (静的) を設定した VLAN を追加した場合、そのポートの通信が一度途絶えることがあります。

(3) 認証端末数制限の設定

[設定のポイント]

認証単位ごとに、認証を許可する最大端末数を設定します。ポート単位認証では、認証サブモードに端末認証モードを設定している場合に有効となります。

[コマンドによる設定](ポート単位認証)

1. (config)# interface gigabitethernet 1/1
 (config-if)# dot1x multiple-authentication
 (config-if)# dot1x port-control auto
 (config-if)# dot1x max-supPLICANT 50
 ポート 1/1 で認証を許可する最大端末数を 50 に設定します。

[コマンドによる設定](VLAN 単位認証 (静的))

1. (config)# dot1x vlan 10 max-supPLICANT 50
 VLAN 単位認証 (静的) に設定した VLAN ID 10 で認証を許可する最大端末数を 50 に設定します。

[コマンドによる設定](VLAN 単位認証 (動的))

1. (config)# dot1x vlan dynamic max-supPLICANT 50
 VLAN 単位認証 (動的) で認証を許可する最大端末数を 50 に設定します。

(4) 端末検出動作の切替設定

端末の認証開始を誘発するために、本装置は tx-period コマンドで指定した間隔で EAP-Request/Identity をマルチキャスト送信します。このとき、EAP-Request/Identity に応答した認証済み端末に対する認証シーケンス動作を設定します。デフォルトは、認証処理を省略します。

[設定のポイント]

shortcut は、認証処理を省略して本装置の負荷を軽減します。disable は、認証済みの端末が存在する場合には、定期的な EAP-Request/Identity の送信を行いません。

[コマンドによる設定](ポート単位認証)

1. (config)# interface gigabitethernet 1/1
 (config-if)# dot1x multiple-authentication
 (config-if)# dot1x port-control auto
 (config-if)# dot1x supPLICANT-detection disable
 ポート 1/1 に認証済み端末が存在する場合には EAP-Request/Identity を送信しないように設定します。

[コマンドによる設定](VLAN 単位認証 (静的))

1. (config)# dot1x vlan 10 supPLICANT-detection shortcut
 VLAN 単位認証 (静的) に設定した VLAN ID 10 で、認証済み端末からの EAP-Response/Identity 受信では、再認証処理を省略して認証成功とするように設定します。

[コマンドによる設定](VLAN 単位認証 (動的))

1. (config)# dot1x vlan dynamic supPLICANT-detection shortcut
 VLAN 単位認証 (動的) で認証済み端末からの EAP-Response/Identity 受信では、再認証処理を省略して認証成功とするように設定します。

9.1.4 認証処理に関する設定

(1) 端末へ再認証を要求する機能の設定

ログオフを送信しないでネットワークから外れた端末は本装置から認証を解除できないため、認証済みの端末に対して再認証を促すことで応答のない端末の認証を解除します。

[設定のポイント]

認証済みの端末ごとに、reauth-period タイマに設定している時間間隔で EAP-Request/Identity を送信します。reauth-period タイマの設定値は、tx-period タイマ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](ポート単位認証)

1. (config)# interface gigabitethernet 1/1
(config-if)# dot1x reauthentication
(config-if)# dot1x timeout reauth-period 360

ポート 1/1 での再認証要求機能を有効に設定し、再認証の時間間隔を 360 秒に設定します。

[コマンドによる設定](VLAN 単位認証 (静的))

1. (config)# dot1x vlan 10 reauthentication
(config)# dot1x vlan 10 timeout reauth-period 360

VLAN 単位認証 (静的) に設定した VLAN ID 10 での再認証機能を有効に設定し、再認証の時間間隔を 360 秒に設定します。

[コマンドによる設定](VLAN 単位認証 (動的))

1. (config)# dot1x vlan dynamic reauthentication
(config)# dot1x vlan dynamic timeout reauth-period 360

VLAN 単位認証 (動的) での再認証機能を有効に設定し、再認証の時間間隔を 360 秒に設定します。

(2) 端末への EAP-Request フレーム再送の設定

端末の認証中に、本装置から送信する EAP-Request (認証サーバからの要求メッセージ) に対して、端末から応答がない場合の再送時間と再送回数を設定します。

[設定のポイント]

再送時間間隔と再送回数の総時間が、reauth-period タイマに設定している時間より短い時間になるように設定してください。

[コマンドによる設定](ポート単位認証)

1. (config)# interface gigabitethernet 1/1
(config-if)# dot1x timeout supp-timeout 60
ポート 1/1 での EAP-Request フレームの再送時間を 60 秒に設定します。
2. (config-if)# dot1x max-req 3
ポート 1/1 での EAP-Request フレームの再送回数を 3 回に設定します。

[コマンドによる設定](VLAN 単位認証 (静的))

1. (config)# dot1x vlan 10 timeout supp-timeout 60
VLAN 単位認証 (静的) に設定した VLAN ID 10 での EAP-Request フレームの再送時間を 60 秒に設定します。
2. (config)# dot1x vlan 10 max-req 3
VLAN 単位認証 (静的) に設定した VLAN ID 10 での EAP-Request フレームの再送回数を 3 回に設定します。

[コマンドによる設定](VLAN 単位認証 (動的))

1. (config)# dot1x vlan dynamic timeout supp-timeout 60
VLAN 単位認証 (動的) での EAP-Request フレームの再送時間を 60 秒に設定します。
2. (config)# dot1x vlan dynamic max-req 3
VLAN 単位認証 (動的) での EAP-Request フレームの再送回数を 3 回に設定します。

(3) 端末からの認証要求を抑止する機能の設定

端末からの EAP-Start フレーム受信による認証処理を抑止します。本機能を設定した場合、新規認証および再認証は、それぞれ tx-period タイマ、reauth-period タイマの時間間隔で行われます。

[設定のポイント]

多数の端末から短い時間間隔で再認証要求が行われ、装置の負荷が高い場合に設定を行い、負荷を低減します。本コマンドの設定前に dot1x reauthentication コマンドの設定が必要です。

[コマンドによる設定](ポート単位認証)

1. (config)# interface gigabitethernet 1/1
(config-if)# dot1x reauthentication
(config-if)# dot1x ignore-eapol-start
ポート 1/1 で EAP-Start フレーム受信による認証処理を抑止します。

[コマンドによる設定](VLAN 単位認証 (静的))

1. (config)# dot1x vlan 10 reauthentication
(config)# dot1x vlan 10 ignore-eapol-start
VLAN 単位認証 (静的) に設定した VLAN ID 10 で EAP-Start フレームによる認証処理を抑止します。

[コマンドによる設定](VLAN 単位認証 (動的))

1. (config)# dot1x vlan dynamic reauthentication
(config)# dot1x vlan dynamic ignore-eapol-start
VLAN 単位認証 (動的) で EAP-Start フレーム受信による認証処理を抑止します。

(4) 認証失敗時の認証処理再開までの待機時間設定

認証に失敗した端末に対する認証再開までの待機時間を設定します。

[設定のポイント]

認証に失敗した端末から、短い時間に認証の要求が行われることで装置の負荷が高くなることを抑止します。

ユーザが ID やパスワードの入力誤りによって認証が失敗した場合でも、設定した時間を経過しないと認証処理を再開しないので、設定時には注意してください。

[コマンドによる設定](ポート単位認証)

1. (config)# interface gigabitethernet 1/1
(config-if)# dot1x timeout quiet-period 300

ポート単位認証を設定しているポート 1/1 に認証処理再開までの待機時間を 300 秒に設定します。

[コマンドによる設定](VLAN 単位認証 (静的))

1. (config)# dot1x vlan 10 timeout quiet-period 300

VLAN 単位認証 (静的) を設定している VLAN ID 10 に認証処理再開までの待機時間を 300 秒に設定します。

[コマンドによる設定](VLAN 単位認証 (動的))

1. (config)# dot1x vlan dynamic timeout quiet-period 300

VLAN 単位認証 (動的) に認証処理再開までの待機時間を 300 秒に設定します。

(5) EAP-Request/Identity フレーム送信の時間間隔設定

自発的に認証を開始しない端末に対して、認証開始を誘発するために本装置から定期的に EAP-Request/Identity を送信する時間間隔を設定します。

[設定のポイント]

本機能は、tx-period タイマに設定してある時間間隔で EAP-Request/Identity をマルチキャスト送信します。認証済みの端末からも EAP-Response/Identity の応答を受信し、装置の負荷を高くする可能性がありますので、以下の計算式で決定される値を設定してください。

$$\text{reauth-period} > \text{tx-period} \quad (\text{装置で認証を行う総端末数} \div 20) \times 2$$

tx-period のデフォルト値が 30 秒であるため、300 台以上の端末で認証を行う場合は、tx-period タイマ値を変更してください。

[コマンドによる設定](ポート単位認証)

1. (config)# interface gigabitethernet 1/1
(config-if)# dot1x timeout tx-period 300

ポート単位認証を設定しているポート 1/1 に EAP-Request/Identity フレーム送信の時間間隔を 300 秒に設定します。

[コマンドによる設定](VLAN 単位認証 (静的))

1. (config)# dot1x vlan 10 timeout tx-period 300

VLAN 単位認証 (静的) を設定している VLAN ID 10 に EAP-Request/Identity フレーム送信の時間間隔を 300 秒に設定します。

[コマンドによる設定](VLAN 単位認証 (動的))

1. (config)# dot1x vlan dynamic timeout tx-period 300

VLAN 単位認証 (動的) に EAP-Request/Identity フレーム送信の時間間隔を 300 秒に設定します。

(6) 認証サーバ応答待ち時間のタイマ設定

認証サーバへの要求に対する応答がない場合の待ち時間を設定します。設定した時間が経過すると、Supplicant へ認証失敗を通知します。radius-server コマンドで設定している再送を含めた総時間と比較して短い方の時間で Supplicant へ認証失敗を通知します。

[設定のポイント]

radius-server コマンドで複数のサーバを設定している場合、各サーバの再送回数を含めた総応答待ち時間よりも短い時間を設定すると、認証サーバへ要求している途中で Supplicant へ認証失敗を通知します。設定したすべての認証サーバから応答がないときに認証失敗を通知したい場合は、本コマンドの設定時間の方を長く設定してください。

[コマンドによる設定](ポート単位認証)

1. (config)# interface gigabitethernet 1/1
(config-if)# dot1x timeout server-timeout 300

ポート単位認証を設定しているポート 1/1 に認証サーバからの応答待ち時間を 300 秒に設定します。

[コマンドによる設定](VLAN 単位認証 (静的))

1. (config)# dot1x vlan 10 timeout server-timeout 300

VLAN 単位認証 (静的) を設定している VLAN ID 10 に認証サーバからの応答待ち時間を 300 秒に設定します。

[コマンドによる設定](VLAN 単位認証 (動的))

1. (config)# dot1x vlan dynamic timeout server-timeout 300

VLAN 単位認証 (動的) に認証サーバからの応答待ち時間を 300 秒に設定します。

(7) 複数端末からの認証要求時の通信遮断時間の設定

ポート単位認証 (シングルモード) が動作しているポートで、複数の端末からの認証要求を検出した場合に、そのポートでの通信を遮断する時間を設定します。

[設定のポイント]

ポートに接続されてはいけない端末を排除するのに必要な時間を設定してください。

[コマンドによる設定]

1. (config)# interface gigabitethernet 1/1
(config-if)# dot1x timeout keep-unauth 1800

ポート単位認証を設定しているポート 1/1 に通信遮断状態の時間を 1800 秒に設定します。

(8) syslog サーバへの出力設定

動作ログの syslog サーバへの出力を設定します。

[設定のポイント]

IEEE802.1X の認証情報および動作情報を記録した動作ログを, syslog サーバへ出力する設定をします。

[コマンドによる設定]

1. (config)# dot1x logging enable
(config)# logging event-kind aut
動作ログを syslog サーバに出力する設定をします。

9.1.5 RADIUS サーバ関連の設定

(1) アカウンティングの設定

[設定のポイント]

RADIUS サーバを指定し, アカウンティング集計を行うことを設定します。

[コマンドによる設定]

1. (config)# aaa accounting dot1x default start-stop group radius
RADIUS サーバにアカウンティング集計を行うことを設定します。

(2) RADIUS サーバで認証を行うための設定

[設定のポイント]

ユーザ認証を RADIUS サーバで行うことを設定します。

[コマンドによる設定]

1. (config)# aaa authentication dot1x default group radius
RADIUS サーバでユーザ認証を行うように設定します。

(3) VLAN 単位認証 (動的) 使用時の設定

[設定のポイント]

VLAN 単位認証 (動的) で, 認証した端末を RADIUS サーバから指定された VLAN に従って登録することを設定します。

[コマンドによる設定]

1. (config)# aaa authorization network default group radius
RADIUS サーバから指定された VLAN に登録することを設定します。

9.2 IEEE802.1X のオペレーション

9.2.1 運用コマンド一覧

IEEE802.1X の状態を確認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
show dot1x	認証単位ごとの状態や認証済みの Supplicant 情報を表示します。
show dot1x logging	IEEE802.1X プログラムの動作ログメッセージを表示します。
show dot1x statistics	IEEE802.1X 認証にかかわる統計情報を表示します。
clear dot1x auth-state	認証済みの端末情報をクリアします。
clear dot1x logging	IEEE802.1X プログラムの動作ログメッセージをクリアします。
clear dot1x statistics	IEEE802.1X 認証にかかわる統計情報を 0 にクリアします。
reauthenticate dot1x	IEEE802.1X 認証状態を再認証します。
restart dot1x	IEEE802.1X プログラムを再起動します。
dump protocols dot1x	IEEE802.1X プログラムで採取している制御テーブル情報、統計情報をファイルへ出力します。

9.2.2 IEEE802.1X 状態の表示

(1) 認証状態の表示

IEEE802.1X の状態は show dot1x コマンドで確認してください。

(a) 装置全体の状態表示

IEEE802.1X の設定一覧は、show dot1x コマンドを実行して確認してください。

図 9-1 show dot1x コマンドの実行結果

```
> show dot1x
Date 2006/03/20 10:52:40 UTC
System 802.1X : Enable
```

Port/ChGr/VLAN	AccessControl	PortControl	Status	Supplicants
Port 1/1	---	Auto	Authorized	1
Port 1/2	Multiple-Hosts	Auto	Unauthorized	0
Port 1/3	Multiple-Auth	Auto	---	0
ChGr 32	Multiple-Auth	Auto	---	1
VLAN 10	Multiple-Auth	Auto	---	1
VLAN 11	Multiple-Auth	Auto	---	0
VLAN 12	Multiple-Auth	Auto	---	0
VLAN (Dynamic)	Multiple-Auth	Auto	---	1

(b) ポート単位認証の状態表示

ポート単位認証におけるポートごとの状態情報を show dot1x port コマンドを実行して確認してください。チャンネルグループごとの状態は show dot1x channel-group-number コマンドを実行して確認してください。

ポート番号を指定すると、指定したポートの情報を表示します。

detail パラメータを指定すると、認証している端末の情報を表示します。

図 9-2 show dot1x port コマンド (detail パラメータ指定時) の実行結果

```
> show dot1x port 1/1 detail
Date 2006/03/20 10:52:48 UTC
Port 1/1
AccessControl : ---
Status : Authorized
Supplicants : 1 / 1
TxTimer(s) : 9 / 30
ReAuthSuccess : 0
KeepUnauth(s) : --- / 3600
PortControl : Auto
Last EAPOL : 0012.e200.0021
ReAuthMode : Enable
ReAuthTimer(s) : 3585 / 3600
ReAuthFail : 0

Supplicants MAC      Status      AuthState      BackEndState  ReAuthSuccess
                    SessionTime(s) Date/Time
0012.e200.0021      Authorized  Authenticated  Idle          0
                    15
                    2006/03/20 10:52:32
```

(c) VLAN 単位認証 (静的) の状態表示

VLAN 単位認証 (静的) における VLAN ごとの状態は、show dot1x vlan コマンドを実行して確認してください。VLAN ID を指定すると、指定した VLAN の情報を表示します。detail パラメータを指定すると、認証している端末の情報を表示します。

図 9-3 show dot1x vlan コマンド (detail パラメータ指定時) の実行結果

```
> show dot1x vlan 20 detail
Date 2006/03/20 10:52:48 UTC
VLAN 20
AccessControl : Multiple-Auth
Status : ---
Supplicants : 2 / 2 / 256
TxTimer(s) : 3518 / 3600
ReAuthSuccess : 0
SuppDetection : Shortcut
Port(s) : 1/1-10, ChGr 1-5
Force-Authorized Port(s) : 1/4,8-10, ChGr 1-5
PortControl : Auto
Last EAPOL : 0012.e200.0003
ReAuthMode : Enable
ReAuthTimer(s) : 3548 / 3600
ReAuthFail : 0

Supplicants MAC      Status      AuthState      BackEndState  ReAuthSuccess
                    SessionTime(s) Date/Time
[Port 1/1]
0012.e200.0003      Authorized  Authenticated  Idle          0
                    84
                    2006/03/20 10:51:24
[Port 1/3]
0012.e200.0004      Authorized  Authenticated  Idle          0
                    5
                    2006/03/20 10:51:03
```

(d) VLAN 単位認証 (動的) の状態表示

VLAN 単位認証 (動的) における VLAN ごとの状態は、show dot1x vlan dynamic コマンドを実行して確認してください。VLAN ID を指定すると、指定した VLAN の情報を表示します。detail パラメータを指定すると、認証している端末の情報を表示します。

図 9-4 show dot1x vlan dynamic コマンド (detail パラメータ指定時) の実行結果

```
> show dot1x vlan dynamic detail
Date 2006/03/20 10:52:48 UTC
VLAN (Dynamic)
AccessControl : Multiple-Auth          PortControl : Auto
Status        : ---                    Last EAPOL   : 0012.e200.0005
Supplicants  : 1 / 1 / 256             ReAuthMode  : Disable
TxTimer(s)   : 3556 / 3600            ReAuthTimer(s): 3586 / 3600
ReAuthSuccess : 0                     ReAuthFail  : 0
SuppDetection : Shortcut
VLAN(s) : 20

Supplicants MAC      Status      AuthState      BackEndState  ReAuthSuccess
[VLAN 20]
0012.e200.0005      Authorized  Authenticated  Idle          0
44                  2006/03/20 10:52:03
```

9.2.3 IEEE802.1X 認証状態の変更

(1) 認証状態の初期化

認証状態の初期化を行うには、clear dot1x auth-state コマンドを使用します。ポート番号、VLAN ID、端末の MAC アドレスのどれかを指定できます。何も指定しなかった場合は、すべての認証状態を初期化します。

コマンドを実行した場合、再認証を行うまで通信ができなくなるので注意してください。

図 9-5 装置内すべての IEEE802.1X 認証状態を初期化する実行例

```
> clear dot1x auth-state
Initialize all 802.1X Authentication Information. Are you sure? (y/n) :y
```

(2) 強制的な再認証

強制的に再認証を行うには、reauthenticate dot1x コマンドを使用します。ポート番号、VLAN ID、端末の MAC アドレスのどれかを指定できます。指定がない場合は、すべての認証済み端末に対して再認証を行います。

コマンドを実行しても、再認証に成功した Supplicant の通信に影響はありません。

図 9-6 装置内すべての IEEE802.1X 認証ポート、VLAN で再認証する実行例

```
> reauthenticate dot1x
Reauthenticate all 802.1X ports and vlans. Are you sure? (y/n) :y
```

10 Web 認証の解説

Web 認証は、汎用 Web ブラウザを用いて認証されたユーザ単位に VLAN へのアクセス制御を行う機能です。この章では Web 認証について解説します。

10.1	概要
10.2	システム構成例
10.3	認証機能
10.4	認証手順
10.5	内蔵 Web 認証 DB および RADIUS サーバの準備
10.6	認証エラーメッセージ
10.7	Web 認証画面入れ替え機能
10.8	系切替時の引き継ぎ情報
10.9	Web 認証使用時の注意事項

10.1 概要

Web 認証は、Internet Explorer などの汎用の Web ブラウザ（以降、単に Web ブラウザと表記）を利用してユーザ ID およびパスワードを使った認証によってユーザを認証します。本装置は、認証に成功したユーザが使用する端末の MAC アドレスを使用して認証後のネットワークへのアクセスを可能にします。

この機能によって、端末側に特別なソフトウェアをインストールすることなく、Web ブラウザだけで認証ができます。

(1) 認証モード

本装置は次に示す認証モードをサポートしています。

- 固定 VLAN モード
端末が認証に成功したあと、MAC アドレスを MAC アドレステーブルに登録して、VLAN 内へ通信できるようにします。端末が認証ネットワークへログインする方法として、本装置の Web 認証専用 IP アドレスを使用する方法があります。
- ダイナミック VLAN モード
端末が認証に成功したあと、MAC アドレスを MAC VLAN と MAC アドレステーブルに登録して、認証前のネットワークと認証後のネットワークを分離します。端末が認証ネットワークへログインする方法として、本装置の URL リダイレクト機能を使用する方法と Web 認証専用 IP アドレスを使用する方法があります。
- レガシーモード
端末が認証に成功したあと、MAC アドレスを MAC VLAN に登録して、認証前のネットワークと認証後のネットワークを分離します。端末は、認証前の VLAN インタフェースの IP アドレスで本装置にログインします（このモードは、Ver.11.3 までのダイナミック VLAN モードです）。

ダイナミック VLAN モードおよびレガシーモードの記述で、認証前の端末が所属する VLAN を認証前 VLAN と呼びます。また、認証後の VLAN を認証後 VLAN と呼びます。

(2) 認証方式

本装置は固定 VLAN モード、ダイナミック VLAN モードおよびレガシーモードのどの認証モードでも、次に示すローカル認証方式または RADIUS 認証方式のどちらかの方式を選択できます。

- ローカル認証方式
本装置に内蔵した認証用 DB（内蔵 Web 認証 DB と呼びます）にユーザ情報を登録しておき、PC から入力された情報との一致を確認して認証する方式です。ネットワーク内に RADIUS サーバを置かない小規模ネットワークに適しています。
- RADIUS 認証方式
ネットワーク内に設置した RADIUS サーバを用いて認証する方式です。比較的規模の大きなネットワークに適しています。

(3) 認証ネットワーク

本装置の Web 認証は、IPv4 ネットワークを認証対象とします。したがって、認証の対象となる端末を収容する VLAN インタフェースには、IPv4 アドレスを設定する必要があります。ただし、RADIUS サーバの設定では、IPv4 アドレスまたは IPv6 アドレスのどちらでも指定できます。

10.2 システム構成例

ここでは、固定 VLAN モード、動的 VLAN モードおよびレガシーモードの各認証モードについて、ローカル認証方式および RADIUS 認証方式の場合のシステム構成を示します。

また、認証対象の端末への IP アドレス設定方法の違いによるネットワーク構成例を示します。

10.2.1 固定 VLAN モード

固定 VLAN モードでは、認証対象端末が認証前のときは、MAC アドレステーブルに登録されず、接続された VLAN 内へ通信できない状態です。認証が成功すると、端末の MAC アドレスを MAC アドレステーブルに登録し、VLAN 内へ通信できるようになります。

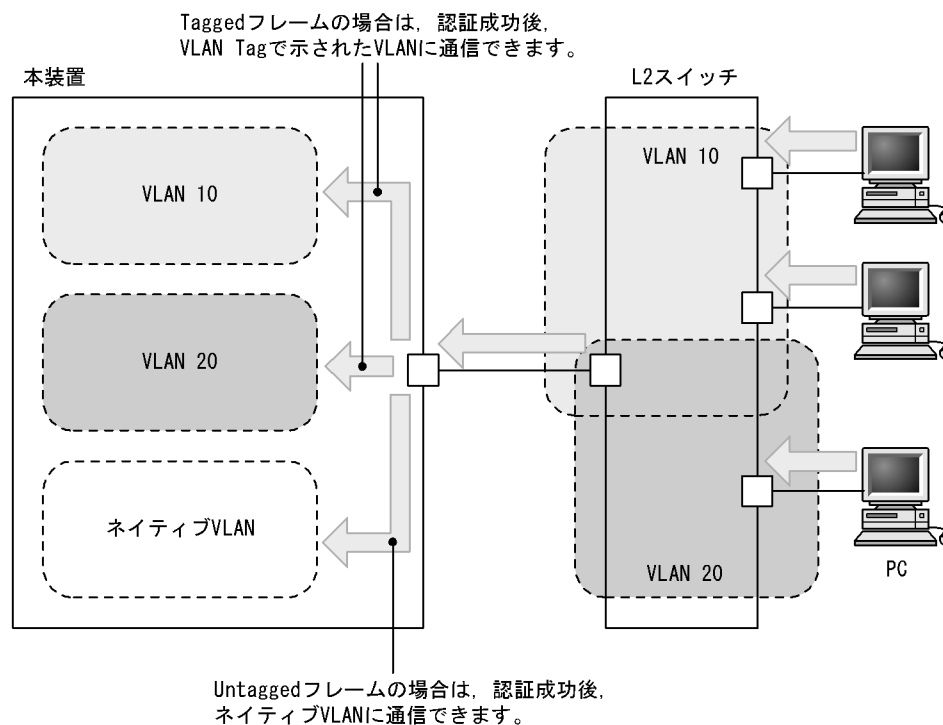
本装置では認証ポートとして次のポートを設定できます。

- アクセスポート
- トランクポート

なお、トランクポートに入ってきた Tagged フレームおよび Untagged フレームの扱いを次に示します。

- 認証時のパケットが Tagged フレームの場合、認証成功後は VLAN Tag で示された VLAN に通信できます。
- 認証時のパケットが Untagged フレームの場合、認証成功後はネイティブ VLAN に通信できます。

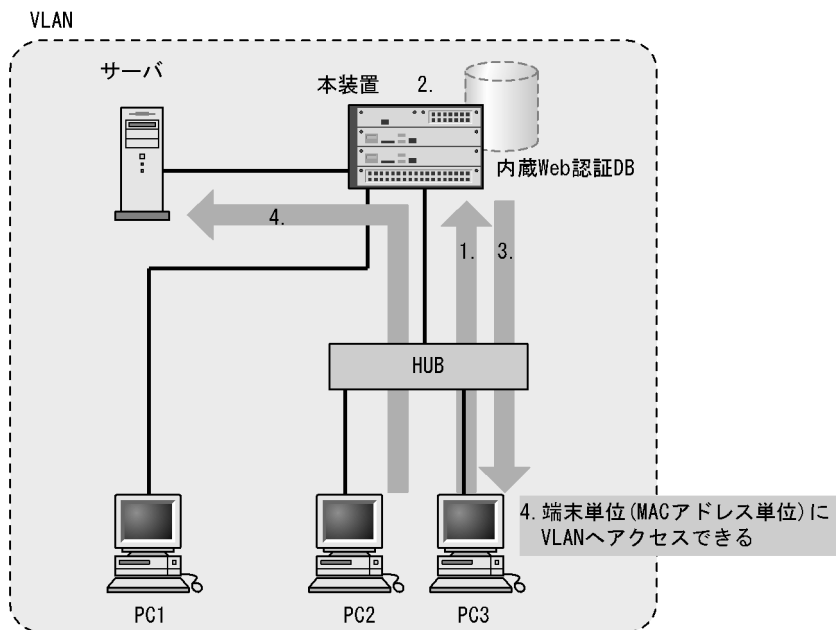
図 10-1 トランクポートの扱い



(1) ローカル認証方式

内蔵 Web 認証 DB を使用したローカル認証方式の構成を次の図に示します。

図 10-2 固定 VLAN モード時のローカル認証方式の構成

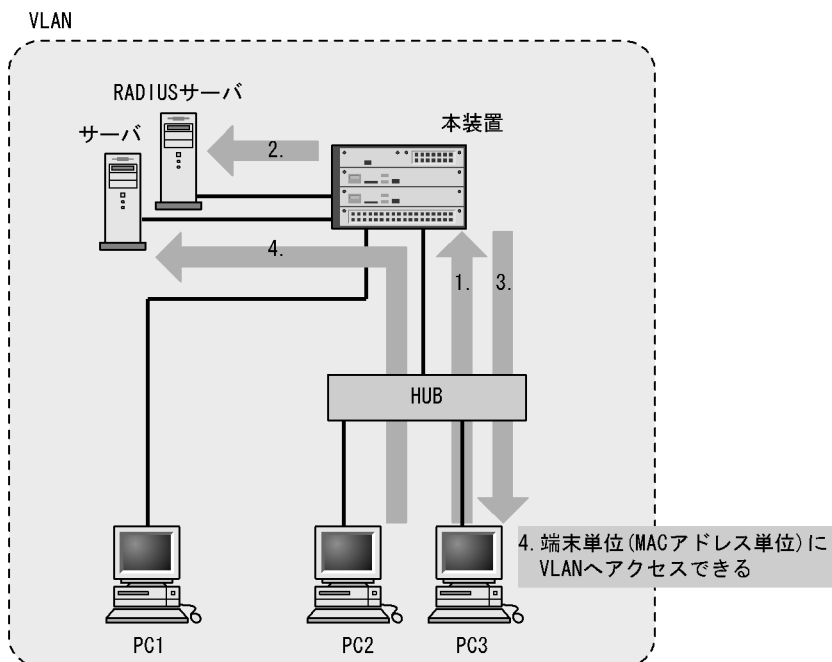


1. HUB 経由で接続された PC から Web ブラウザを起動し、本装置にアクセスします。
2. 本装置の内蔵 Web 認証 DB に登録されたユーザ情報と、PC から入力されたユーザ ID およびパスワードとの一致を確認する認証を行います。
3. 認証が成功であれば、認証成功画面を PC に表示します。
4. 認証済み PC は接続された VLAN のサーバに接続できるようになります。

(2) RADIUS 認証方式

RADIUS サーバを使用した RADIUS 認証方式の構成を次の図に示します。

図 10-3 固定 VLAN モード時の RADIUS 認証方式の構成



1. HUB 経由で接続された PC から Web ブラウザを起動し、本装置にアクセスします。
2. RADIUS サーバに登録されたユーザ情報と、PC から入力されたユーザ ID およびパスワードとの一致を確認する認証を行います。
3. 認証が成功であれば、認証成功画面を PC に表示します。
4. 認証済み PC は接続された VLAN のサーバに接続できるようになります。

10.2.2 ダイナミック VLAN モード

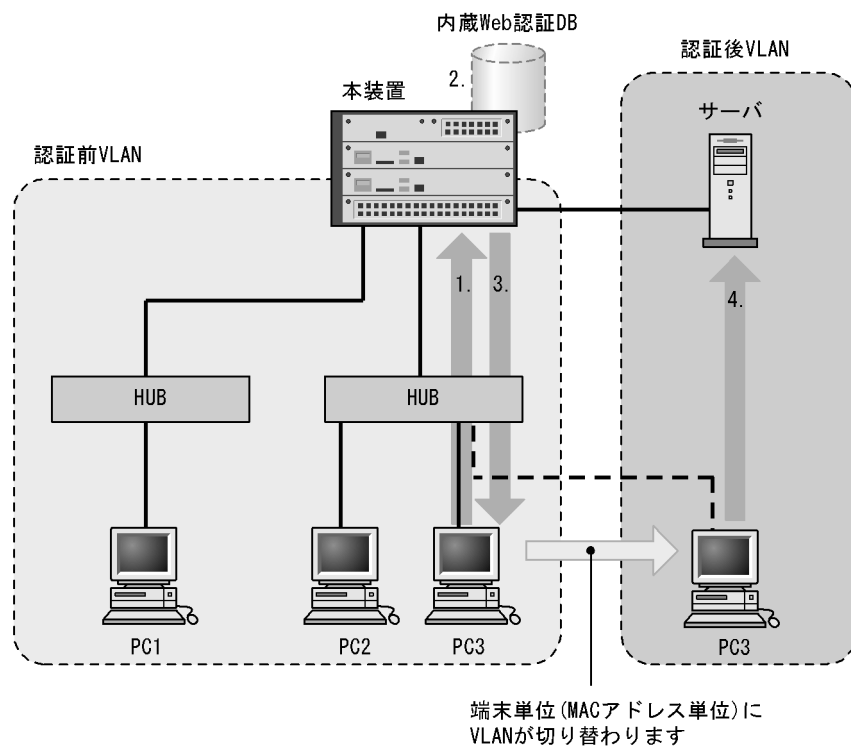
ダイナミック VLAN モードでは、認証前 VLAN に收容されていた端末を、認証成功後、内蔵 Web 認証 DB または RADIUS に登録されている VLAN ID を使用して、MAC VLAN と MAC アドレステーブルに登録して認証後 VLAN への通信を許可します。このため、次に示す設定が必要になります。

- MAC VLAN が設定されているポートを認証ポートとして設定
- 認証前 VLAN と認証後 VLAN 間に不要な通信を禁止するアクセスリストの設定

(1) ローカル認証方式

内蔵 Web 認証 DB を使用したローカル認証方式の構成を次の図に示します。

図 10-4 ダイナミック VLAN モードのローカル認証方式の構成

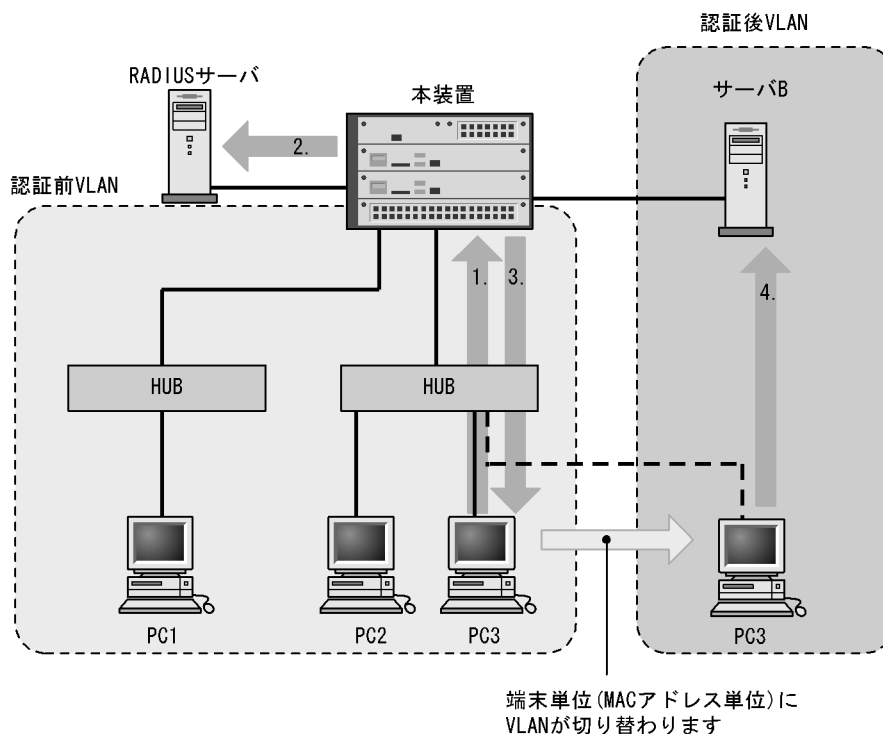


1. HUB 経由で接続された PC から Web ブラウザを起動し、本装置にアクセスします。
2. 本装置の内蔵 Web 認証 DB に登録されたユーザ情報と、PC から入力されたユーザ ID およびパスワードとの一致を確認する認証を行います。
3. 認証が成功であれば、認証成功画面を PC に表示し、認証後 VLAN へ切り替わります。
4. 認証済みの PC は、認証後 VLAN のサーバに接続できるようになります。

(2) RADIUS 認証方式

RADIUS サーバを使用した RADIUS 認証方式の構成を次の図に示します。

図 10-5 ダイナミック VLAN モードの RADIUS 認証方式の構成



1. HUB 経由で接続された PC から Web ブラウザを起動し、本装置にアクセスします。
2. RADIUS サーバに登録されたユーザ情報と、PC から入力されたユーザ ID およびパスワードとの一致を確認する認証を行います。
3. 認証が成功であれば、認証成功画面を PC に表示し、認証後 VLAN へ切り替わります。
4. 認証済みの PC は、認証後 VLAN のサーバに接続できるようになります。

10.2.3 レガシーモード

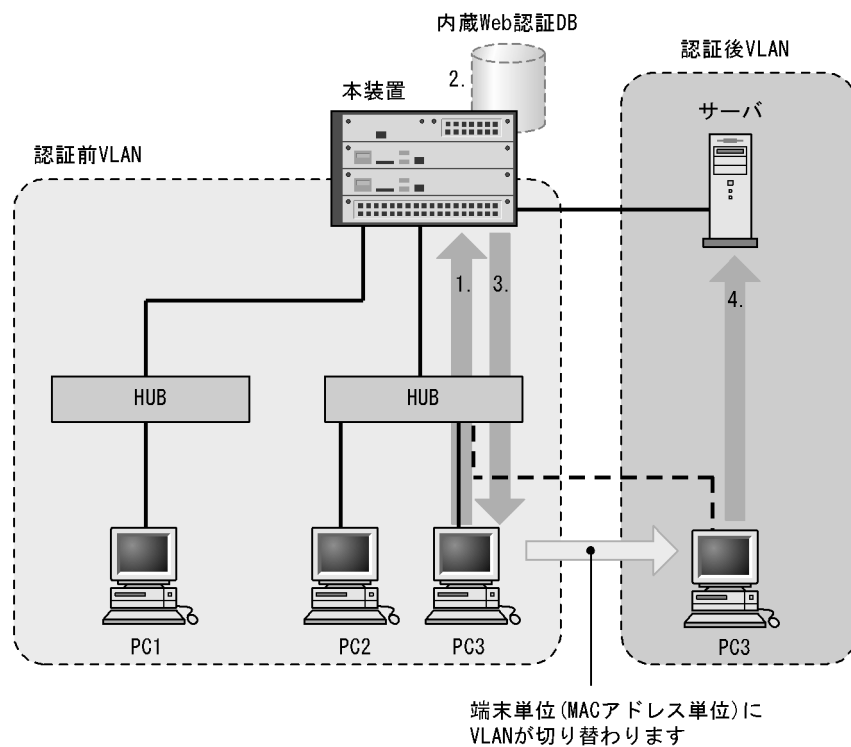
このモードでは、認証前 VLAN をネイティブ VLAN に、認証後 VLAN を MAC VLAN として設定しておきます。認証対象端末が認証前は、端末の MAC アドレスを認証前 VLAN に収容していますが、認証が成功すると、認証後 VLAN に収容します。このため、次に示す設定が必要になります。

- 認証後に切り替わる VLAN の設定
- 認証前 VLAN と認証後 VLAN 間に不要な通信を禁止するアクセスリストの設定

(1) ローカル認証方式

内蔵 Web 認証 DB を使用したローカル認証方式の構成を次の図に示します。

図 10-6 Web 認証システム構成図（ローカル認証方式）

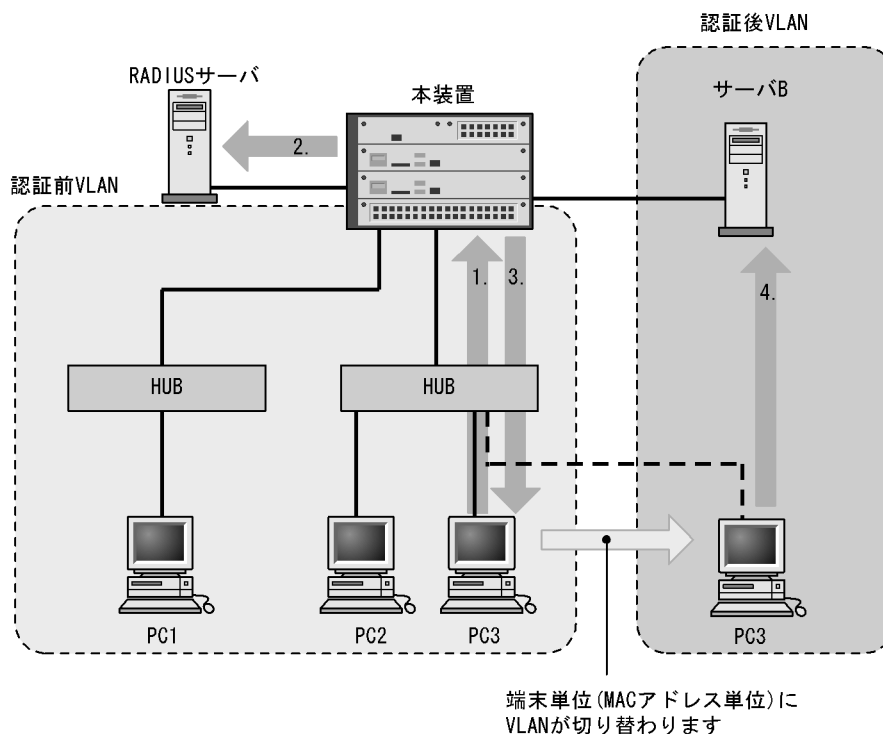


1. HUB 経由で接続された PC から Web ブラウザを起動し、本装置にアクセスします。
2. 本装置の内蔵 Web 認証 DB に登録されたユーザ情報と、PC から入力されたユーザ ID およびパスワードとの一致を確認する認証を行います。
3. 認証が成功であれば、認証成功画面を PC に表示し、認証後 VLAN へ切り替わります。
4. 認証済みの PC は、認証後 VLAN のサーバに接続できるようになります。

(2) RADIUS 認証方式

RADIUS サーバを使用した RADIUS 認証方式の構成を次の図に示します。

図 10-7 Web 認証システム構成図 (RADIUS 認証方式)



1. HUB 経由で接続された PC から Web ブラウザを起動し、本装置にアクセスします。
2. RADIUS サーバに登録されたユーザ情報と、PC から入力されたユーザ ID およびパスワードとの一致を確認する認証を行います。
3. 認証が成功であれば、認証成功画面を PC に表示し、認証後 VLAN へ切り替わります。
4. RADIUS サーバから送られる VLAN ID の情報に従って、認証済みの PC は、認証後 VLAN のサーバに接続できるようになります。

10.2.4 IP アドレス設定方法による構成例

Web 認証の対象となる端末に IP アドレスを設定する方法には次の三つがあります。Web 認証は IPv4 ネットワークを対象とするため、ここで説明する IP アドレスは IPv4 アドレスです。

- 本装置内蔵の DHCP サーバ機能で IP アドレスを配布する
- 外部 DHCP サーバを使用する
- 手動で端末の IP アドレスを設定する

固定 VLAN モードでは、認証の前後で端末の IP アドレスを変更する必要はありません。一方、ダイナミック VLAN モードでは、認証の前後で端末が収容される VLAN の変更に伴い IP サブネットも変更されるため、IP アドレスを変更する必要があります。

次に、ダイナミック VLAN モードでの IP アドレス設定方法ごとのシステム構成例を示します。

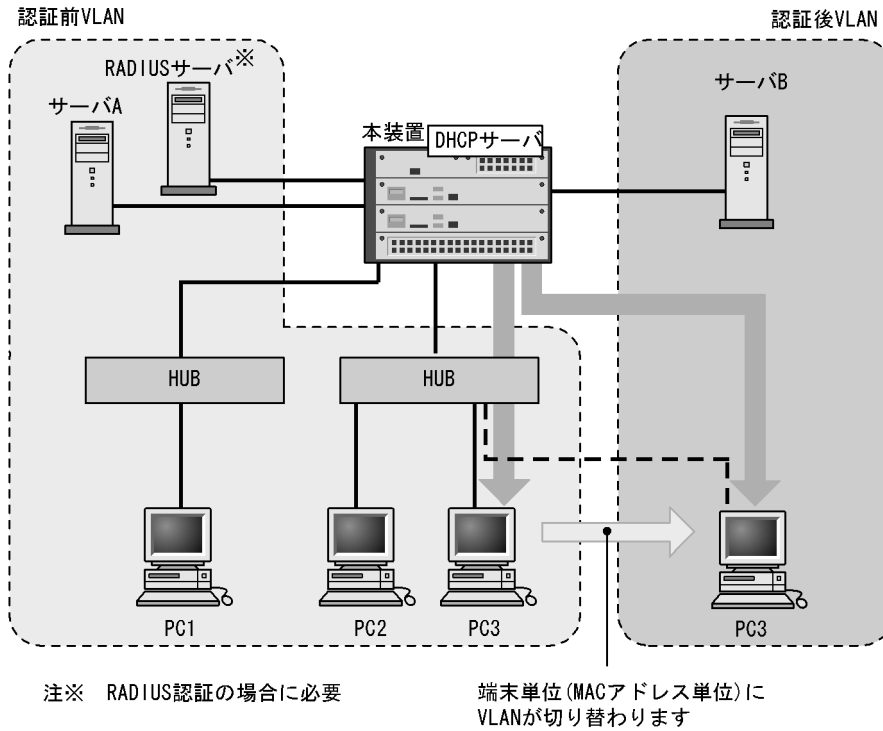
(1) 本装置内蔵の DHCP サーバ機能で IP アドレスを配布する場合

本装置に実装している DHCP サーバを用意する際の構成例を次の図に示します。

認証端末に対して、DHCP サーバ機能から、認証前 VLAN の IP アドレスが配布されたあと、Web ブラウザを用いて認証を行います。

認証が完了すると端末は、認証後 VLAN に切り替わります。VLAN が切り替わり、端末の IP アドレスリースタイムアウト後に、DHCP サーバから認証後 VLAN の IP アドレスが配布され、端末からアクセスできるようになります。

図 10-8 Web 認証システム構成図（内蔵 DHCP サーバ使用）



注意

- DHCP サーバに、認証前 VLAN 用の IP アドレス配布設定と、認証後 VLAN 用の IP アドレス配布設定とを行う必要があります。
- DHCP サーバに、デフォルトゲートウェイアドレスを端末に配布するための設定が必要です。

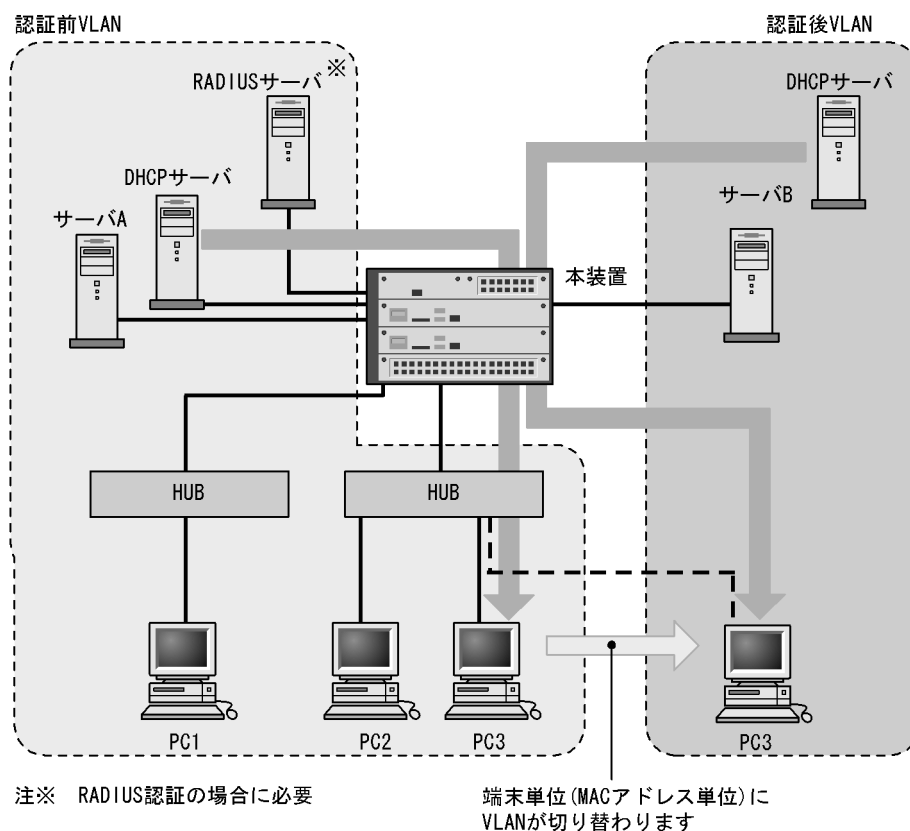
(2) 外部 DHCP サーバを使用する場合

端末認証する際に使用する IP アドレスの配布および認証後の IP アドレス配布を外部 DHCP サーバから行う場合の構成例を次の図に示します。

認証端末には外部 DHCP サーバから、認証前 VLAN の IP アドレスが配布されたあと Web ブラウザによって認証を行います。

認証が完了すると端末は、認証後 VLAN に切り替わります。端末の IP アドレスリースタイムアウト後に、外部 DHCP サーバから認証後 VLAN の IP アドレスが配布されます。

図 10-9 Web 認証システム構成図 (外部 DHCP サーバ)



注意

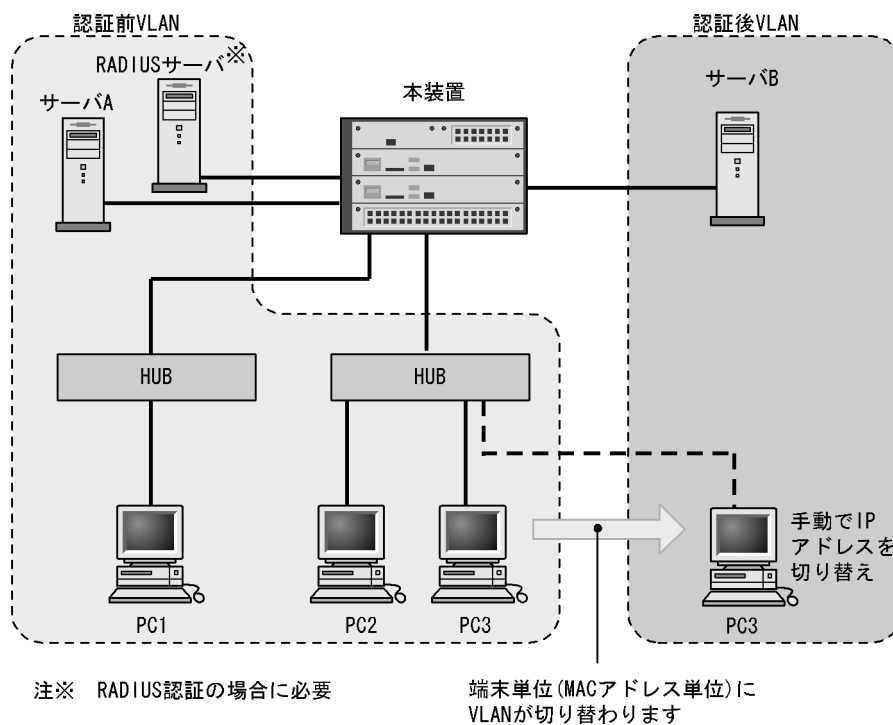
- 外部 DHCP サーバに、デフォルトゲートウェイアドレスを端末に配布するための設定が必要です。

(3) 手で端末の IP アドレスを設定する場合

認証対象端末の IP アドレスを、認証完了後に手で設定変更する場合の構成例を次の図に示します。

認証前 VLAN に接続された端末は、認証後に手で IP アドレスを認証後 VLAN のサブネットの属する IP アドレスに変更することによって認証後 VLAN へのアクセスが可能となります。

図 10-10 Web 認証システム構成図 (手動 IP アドレス切り替え)



注意

- 認証後に誤った IP アドレスを設定した場合、認証が成功であってもネットワークにアクセスできなくなります。

10.3 認証機能

10.3.1 認証前端末の通信許可

認証前端末の通信を許可するには認証専用 IPv4 アクセスリストの設定が必要です。認証専用 IPv4 アクセスリストについては「7.3 レイヤ 2 認証共通の機能」を参照してください。

10.3.2 認証ネットワークへのログイン

固定 VLAN モードでは、認証前の端末が認証ネットワークへログインする方法として、Web 認証専用 IP アドレスを使用する方法があります。そのため、Web 認証専用 IP アドレスの設定が必要です。

ダイナミック VLAN モードでは、認証前の端末が認証ネットワークへログインする方法として、URL リダイレクト機能を使用する方法と Web 認証専用 IP アドレスを使用する方法があります。どちらの方法も、Web 認証専用 IP アドレスの設定が必要です。

Web 認証専用 IP アドレスは、Web 認証で使用する、端末から本装置へのアクセス専用の IPv4 アドレスです。このアドレスは装置のインターフェースに付けられたアドレスとは異なるため、異なる IP サブネットに収容される端末から認証ネットワークへのログイン操作およびログアウト操作を、すべて同じ IP アドレスで実施できます。また、Web 認証専用 IP アドレスは装置外には送出ししないので、ネットワーク内の複数の本装置に同じアドレスを設定できます。したがって、どの端末からも同じ操作で認証ネットワークへのログインおよびログアウトができます。

注意

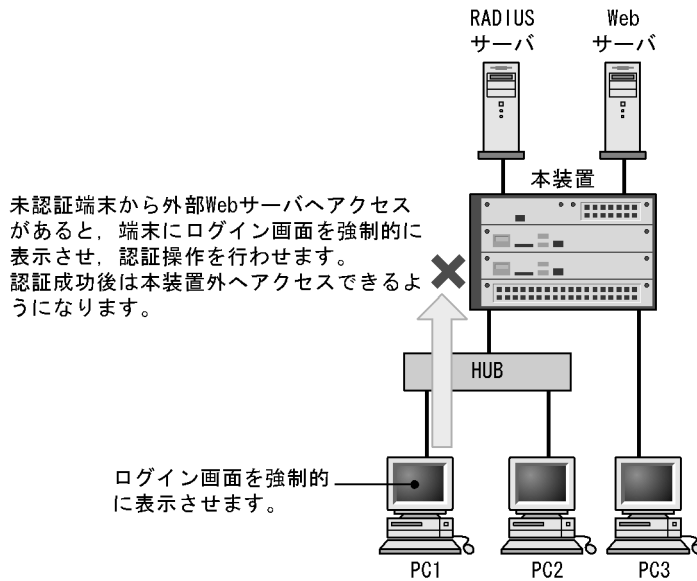
- Web 認証専用 IP アドレスを使用する場合、端末のデフォルトゲートウェイの設定で本装置のインターフェースの IP アドレスを指定してください。

(1) URL リダイレクト機能

認証前の端末が認証ネットワークへログインする場合に、認証前の端末から装置外の Web サーバ宛での http または https アクセスを検出し、端末の画面に強制的にログイン画面を表示してログイン操作をさせることができます。URL リダイレクト機能は、コンフィグレーションコマンド `web-authentication redirect-vlan` を設定すると有効になります。

また、コンフィグレーションコマンド `web-authentication ip address` で FQDN (Fully Qualified Domain Name) を指定すれば、リダイレクト先 URL として使用できます。

図 10-11 URL リダイレクト機能



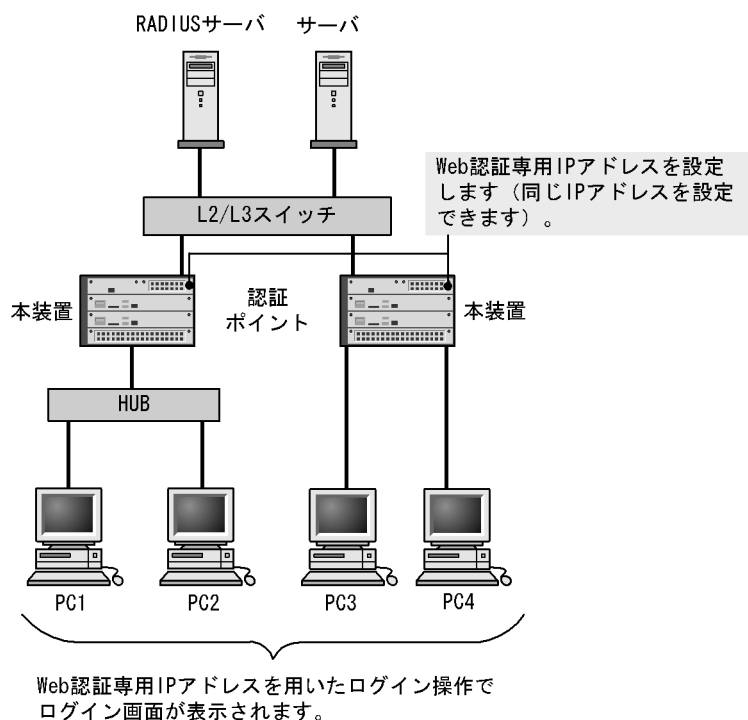
注意

- 端末の Web ブラウザにプロキシサーバを設定した状態で、次のどちらかの方法で URL リダイレクトを使用する場合は、必ず Web 認証専用 IP アドレスがプロキシサーバの適用を受けないように設定してください。
 - コンフィグレーションコマンド `web-authentication redirect-mode` で、`https` パラメータを設定
 - 認証前状態の端末から `https` でアクセス
- 本機能を使用して、認証前の端末から `https` で URL アクセスを行ったとき、装置に登録された証明書のドメイン名と一致していない場合、証明書不一致の警告メッセージが Web ブラウザ上に表示されます。なお、警告メッセージが表示されても、続行する操作を行うと、Web 認証のログイン画面が表示されてログイン操作が行えます。
- 次に示すコンフィグレーションが設定、変更、および削除された場合は、運用コマンド `restart web-authentication web-server` で Web サーバを再起動してください。
 - `web-authentication ip address`
 - `web-authentication port`
 - `web-authentication redirect-vlan`
 - `web-authentication web-port`

(2) Web 認証専用 IP アドレスによるログイン操作

本装置に設定された Web 認証専用の IP アドレスを使用してログイン操作、およびログアウト操作ができます。

図 10-12 Web 認証専用 IP アドレスによるログイン操作



10.3.3 認証ネットワークからのログアウト

認証ネットワークにログインした端末をログアウトする方法を次の表に示します。

表 10-1 認証モードごとのログアウト方法

ログアウト方法	固定 VLAN モード	ダイナミック VLAN モード	レガシーモード
Web 画面によるログアウト			
最大接続時間超過時のログアウト			
認証済み端末の接続監視機能によるログアウト		-	-
認証済み端末の MAC アドレステーブルエージングによるログアウト	-		
運用コマンドによるログアウト			
認証済み端末からの特殊パケット受信によるログアウト		-	-
認証端末接続ポートのリンクダウンによるログアウト		-	-
VLAN 設定変更によるログアウト			
認証方式の切り替えによるログアウト			
認証モードの切り替えによるログアウト			
Web 認証の停止によるログアウト			

(凡例) : サポート - : 該当なし

ダイナミック VLAN モードおよびレガシーモードの場合、上記の方法でログアウトしたあと、端末の IP アドレスを認証前の IP アドレスに変更してください。また、DHCP サーバを使用している場合は、端末から IP アドレスの再配布を指示してください。

- DHCP サーバを使用している場合、端末の IP アドレスをいったん削除してから、DHCP サーバへ IP アドレスの配布を指示してください。（例：Windows の場合、コマンドプロンプトから `ipconfig / release` を実行した後に、`ipconfig /renew` を実行してください。）
- IP アドレスを手動で設定している場合、手動で端末の IP アドレスを認証前の IP アドレスに変更してください。

(1) Web 画面によるログアウト

認証済み端末からログアウト用 URL にアクセスして、端末にログアウト画面を表示させます。画面上のログアウト操作によって Web 認証は認証解除を行います。認証が解除されると、ログアウト完了画面を表示します。

(2) 最大接続時間超過時のログアウト

コンフィグレーションコマンド `web-authentication max-timer` で設定された最大接続時間を超えた場合に、強制的に Web 認証の認証状態を解除して、端末から本装置外への通信を停止します。この際に設定された最大接続時間が経過してから 1 分以内で認証解除が行われます。この場合には、端末にログアウト完了画面を表示しません。

最大接続時間を超えても使用したい場合は、端末から再度、認証ネットワークへのログイン操作を行ってください。ユーザ ID、パスワードおよび MAC アドレスの組み合わせで認証済みであることが確認された場合に限り、接続時間を延長できます（さらに最大接続時間分だけ延長します）。

なお、コンフィグレーションコマンド `web-authentication max-timer` で最大接続時間を短縮したり、延長したりした場合、現在認証中のユーザには適用されず、次回ログイン時から設定が有効となります。

(3) 認証済み端末の接続監視機能によるログアウト

認証済み端末に対し、コンフィグレーションコマンド `web-authentication logout polling interval` で指定された時間間隔で ARP パケットを用い ARP 返答パケットを受信することによって端末の接続監視を行います。コンフィグレーションコマンド `web-authentication logout polling retry-interval` と `web-authentication logout polling count` で設定された時間を超えても ARP 返答パケットが受信できない場合、タイムアウトしていると判断し、強制的に Web 認証の認証状態を解除します。この場合には、端末にログアウト完了画面を表示しません。

なお、この機能はコンフィグレーションコマンド `no web-authentication logout polling enable` で無効にできます。

注意

接続監視機能の設定値としてデフォルトを使用した場合、認証されている数が多いと、接続タイムアウトと判定してから認証が解除されるまで 1 分程度掛かります。

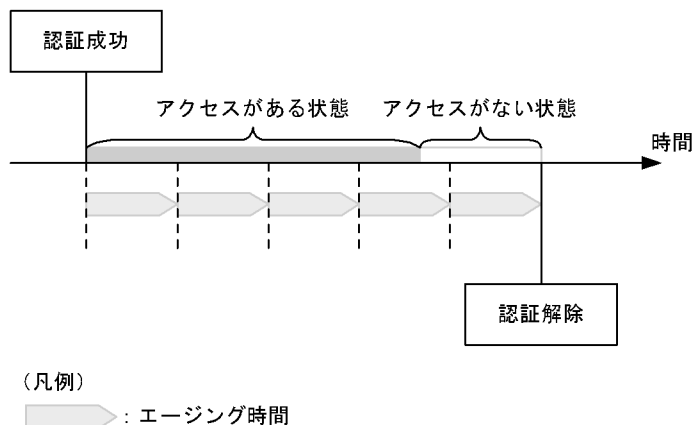
なお、本装置の CPU 負荷が高い場合は、認証解除までさらに時間が掛かることがあります。

(4) 認証済み端末の MAC アドレステーブルエージングによるログアウト

認証済み端末に対し、MAC アドレステーブルを周期的に監視し、端末からのアクセスがあるかをチェックしています。該当する端末からのアクセスがない状態が続いた場合に、強制的に Web 認証の認証状態を解除します。この場合には、端末にログアウト完了画面を表示しません。

MAC アドレステーブルのエージング時間と、MAC アドレステーブルエージングによるログアウトの関係を次の図に示します。

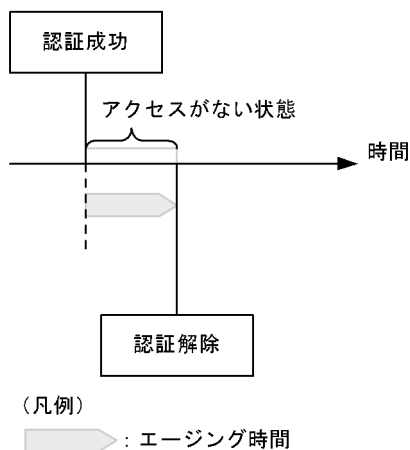
図 10-13 認証済み端末の MAC アドレステーブルエージングによるログアウト



また、認証成功直後に端末からのアクセスがないと、MAC アドレステーブルエージングに合わせて、強制的に認証を解除します。

認証成功直後からアクセスがない場合のログアウトを次の図に示します。

図 10-14 認証成功直後からアクセスがない場合のログアウト



なお、この機能はコンフィグレーションコマンド `no web-authentication auto-logout` で無効にできます (アクセスがない状態が続いた場合でも強制的にログアウトしない設定が可能)。

さらに、レガシーモードでは、認証後に切り替わった VLAN に端末からの通信がまったくないと、MAC アドレス学習が行われません。この場合、認証済みであっても MAC アドレステーブルに MAC アドレスが登録されていないので、強制的にログアウトします。したがって、認証後は必ず通信を行ってください。

(5) 運用コマンドによるログアウト

運用コマンド `clear web-authentication auth-state` でユーザ単位に、強制的にログアウトができます。なお、同一ユーザ ID で複数ログインを行っている場合、同じユーザ ID を持つ認証をすべてログアウトします。この場合には、端末にログアウト完了画面を表示しません。

(6) 認証済み端末からの特殊パケット受信によるログアウト

認証済み端末から送信された特殊パケットを受信した場合、該当する端末の認証を解除します。この場合には、端末にログアウト完了画面を表示しません。特殊パケットの条件を次に示します。

- 認証済み端末から Web 認証専用 IP アドレスで送出された ping パケット
- コンフィグレーションコマンド `web-authentication logout ping tos-windows` で設定された TOS 値を持っているパケット
- コンフィグレーションコマンド `web-authentication logout ping ttl` で設定された TTL 値を持っているパケット

(7) 認証端末接続ポートのリンクダウンによるログアウト

認証済み端末が接続しているポートのリンクダウンを検出した場合、該当するポートに接続された端末の認証を解除します。この場合には、端末にログアウト完了画面を表示しません。

(8) VLAN 設定変更によるログアウト

コンフィグレーションコマンドで認証端末が含まれる VLAN の設定を変更した場合、変更された VLAN に含まれる端末の認証を解除します。この場合には、端末にログアウト完了画面を表示しません。

[コンフィグレーションの変更内容]

- VLAN を削除した場合
- VLAN を停止 (suspend) した場合

(9) 認証方式の切り替えによるログアウト

認証方式が RADIUS 認証方式からローカル認証方式に切り替わった場合、またはローカル認証方式から RADIUS 認証方式に切り替わった場合、すべての端末の認証を解除します。この場合には、端末にログアウト完了画面を表示しません。

(10) 認証モードの切り替えによるログアウト

`copy` コマンドでコンフィグレーションを変更して、認証モードが切り替わる設定をした場合、すべての端末の認証を解除します。この場合には、端末にログアウト完了画面を表示しません。

(11) Web 認証の停止によるログアウト

コンフィグレーションコマンドで Web 認証の定義が削除されて Web 認証が停止した場合、すべての端末の認証を解除します。この場合には、端末にログアウト完了画面を表示しません。

10.3.4 認証済み端末のポート間移動

認証済み端末がポート間移動した場合には、「7.3 レイヤ 2 認証共通の機能」を参照してください。

10.3.5 アカウント機能

認証結果は次のアカウント機能によって記録されます。

(1) Web 認証内蔵のアカウントログ

認証結果は本装置の Web 認証のアカウントログに記録されます。記録されたアカウントログは運用コマンド `show web-authentication logging` で表示できます。出力される認証結果を次の表に示します。

表 10-2 出力される認証結果

事象	時刻	ユーザ ID	IP アドレス	MAC アドレス	VLAN ID	ポート番号	メッセージ
ログイン成功			1		1		認証成功メッセージ
ログアウト				2			認証解除メッセージ
ログイン失敗			2	2	2	2	失敗要因メッセージ
強制ログアウト			2	2	2	2	強制解除メッセージ

(凡例)

：固定 VLAN モード，ダイナミック VLAN モード，およびレガシーモードで出力される

：固定 VLAN モードとダイナミック VLAN モードで出力される

注 1 ダイナミック VLAN モードのログイン成功時に表示される IP アドレスには，認証前の IP アドレスが表示されます。また，VLAN ID には認証後の VLAN ID が表示されます。

注 2 メッセージによっては IP アドレスなどの情報が出力されない場合があります。

本装置の Web 認証のアカウントログは，最大 2100 行まで記録できます。2100 行を超えた場合，古い順に記録が削除され，最新のアカウント情報が追加記録されていきます。

(2) RADIUS サーバのアカウント機能への記録

コンフィグレーションコマンド `aaa accounting web-authentication default start-stop group radius` を設定すると，RADIUS サーバのアカウント機能を使用できます。アカウント機能には次の情報が記録されます。記録される情報を次に示します。

- ログイン情報 : ログイン成功時に次の情報が記録されます。
サーバに記録された時刻，ユーザ ID，MAC アドレス
- ログアウト情報 : ログアウト時に次の情報が記録されます。
サーバに記録された時刻，ユーザ ID，MAC アドレス，ログインからログアウトまでの経過時間
- 強制ログアウト時 : ログアウト時に次の情報が記録されます。
サーバに記録された時刻，ユーザ ID，MAC アドレス，ログインからログアウトまでの経過時間

(3) RADIUS サーバへのログイン情報記録 (RADIUS サーバの機能)

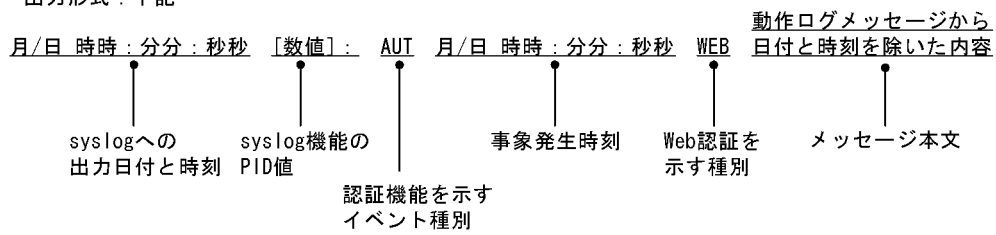
RADIUS 認証方式の場合は，RADIUS サーバが持っている機能によって，ログイン成功 / 失敗が記録されます。ただし，使用する RADIUS サーバによって記録される情報が異なる場合がありますので，詳細は RADIUS サーバの説明書を参照してください。

(4) syslog サーバへの動作ログ記録

Web 認証の動作ログを syslog サーバに出力できます。また，動作ログは Web 認証のアカウントログを含みます。syslog サーバへの出力形式を次の図に示します。

図 10-15 syslog サーバへの出力形式

- ・ イベント種別 : AUT
- ・ 出力形式 : 下記



また、コンフィグレーションコマンド `web-authentication logging enable` および `logging event-kind aut` によって、出力を開始および停止できます。

10.4 認証手順

Web 認証を用いたユーザ認証は次の手順で行います。Web ブラウザ Internet Explorer Version6.0 を用いて説明します。

(1) Web 認証のログイン画面表示

固定 VLAN モードでは、Web 認証専用 IP アドレスの URL にアクセスすると、Web 認証のログイン画面が表示されますので、ログイン画面からユーザ ID とパスワードを入力します。

[固定 VLAN モードのログイン URL 指定]

- Web 認証専用 IP アドレスの URL 指定 : `http://Web 認証専用 IP アドレス /login.html`

ダイナミック VLAN モードで URL リダイレクト機能を使用する場合は、URL リダイレクト機能によって Web 認証のログイン画面が表示されます。また、Web 認証専用 IP アドレスの URL にアクセスしても Web 認証のログイン画面が表示されます。ログイン画面が表示されたら、ユーザ ID とパスワードを入力します。

[ダイナミック VLAN モードのログイン URL 指定]

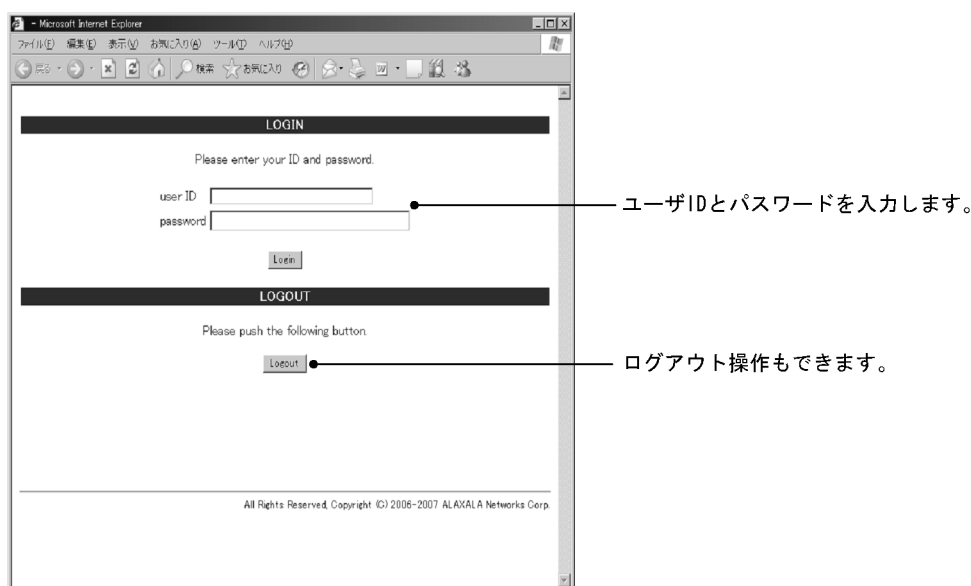
- URL リダイレクト機能無効時の URL 指定 : `http://Web 認証専用 IP アドレス /login.html`
- Web 認証専用 IP アドレスの URL 指定 : `http://Web 認証専用 IP アドレス /login.html`

レガシーモードでは、Web 認証のログイン URL にアクセスすると、Web 認証のログイン画面が表示されますので、ログイン画面からユーザ ID とパスワードを入力します。

[レガシーモードのログイン URL 指定]

- ログイン URL : `http:// 認証前 VLAN のインタフェース IP アドレス /login.html`

図 10-16 ログイン画面



(2) ログイン画面に入力されたユーザ ID、パスワードの認証

入力されたユーザ ID とパスワードを基に、ローカル認証方式の場合は内蔵 Web 認証 DB に登録されてい

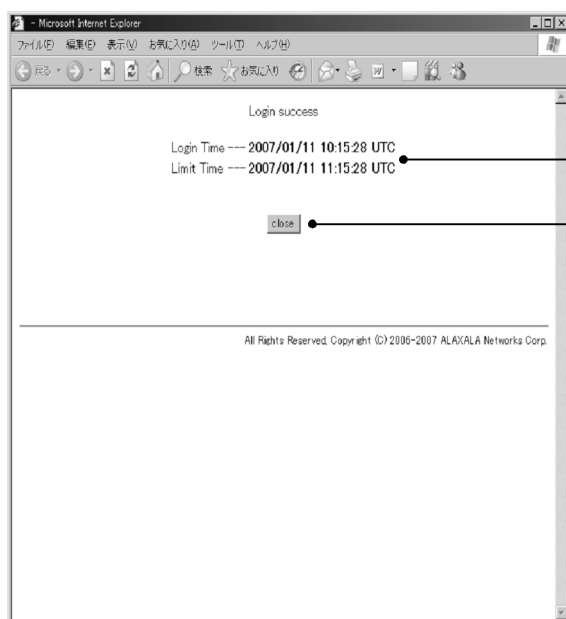
るユーザ情報と一致しているかチェックします。また、RADIUS 認証方式の場合は RADIUS サーバに問い合わせを行い、認証可否のチェックをします。

(3) 認証成功結果を表示

内蔵 Web 認証 DB または RADIUS サーバに登録されているユーザ情報と一致した場合、ログイン成功画面を表示し、認証ネットワークへ通信できます。

また、コンフィグレーションコマンド `web-authentication jump-url` で認証成功後にアクセスする URL が指定されている場合は、端末にログイン成功画面が表示されたあとに指定された URL へのアクセスが行われます。

図 10-17 ログイン成功画面



ログイン時刻とログアウト時刻（自動ログアウトする時刻）を表示します。

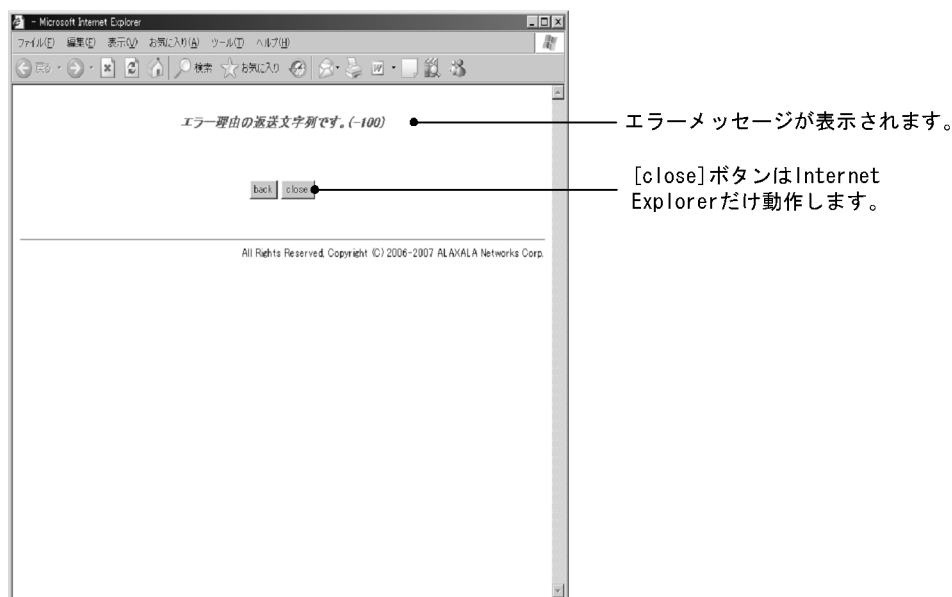
[close] ボタンは Internet Explorer だけ動作します。

(4) 認証失敗時の画面表示

認証が失敗となった場合は、認証エラー画面を表示します。

認証エラー画面に表示されるエラーの発生理由を、「10.6 認証エラーメッセージ」に示します。

図 10-18 ログイン失敗画面



(5) Web 認証からのログアウト画面表示

認証済み端末から Web 認証のログアウト URL にアクセスして、端末にログアウト画面を表示させます。
または、ログイン URL にアクセスして、端末にログイン画面を表示させます。

固定 VLAN モードまたはダイナミック VLAN モードの場合、Web 認証専用 IP アドレスの URL にアクセスします。

[固定 VLAN モードまたはダイナミック VLAN モードのログアウト URL 指定]

- Web 認証専用 IP アドレスのログアウト URL : `http://Web 認証専用 IP アドレス /logout.html`
- Web 認証専用 IP アドレスのログイン URL : `http://Web 認証専用 IP アドレス /login.html`

レガシーモードの場合、Web 認証のログアウト URL にアクセスします。

[レガシーモードのログアウト URL 指定]

- ログアウト URL : `http:// 認証後 VLAN のインタフェース IP アドレス /logout.html`

表示した画面上の [Logout] ボタンを押すと、Web 認証は認証解除を行います。

認証が解除されると、ログアウト完了画面を表示します。

図 10-19 ログアウト画面

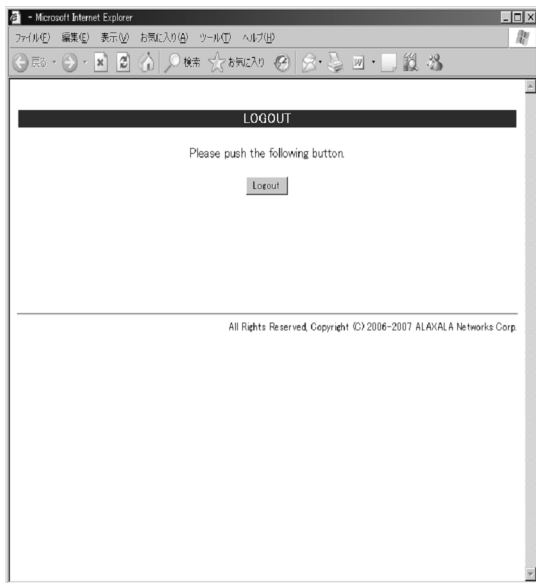
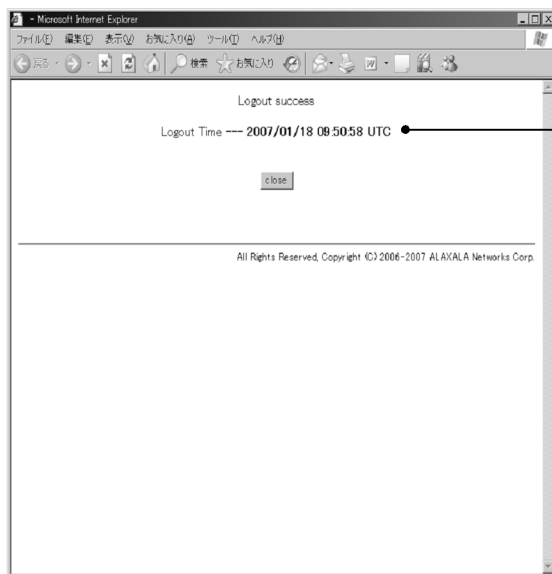


図 10-20 ログアウト完了画面



ログアウト時刻（ログアウト動作が完了した時刻）を表示します。

10.5 内蔵 Web 認証 DB および RADIUS サーバの準備

10.5.1 内蔵 Web 認証 DB の準備

Web 認証のローカル認証方式を使用するに当たっては、事前に内蔵 Web 認証 DB を作成する必要があります。また、本装置の内蔵 Web 認証 DB はバックアップおよび復元できます。

(1) 内蔵 Web 認証 DB の作成

運用コマンド `set web-authentication user` で、ユーザ ID、パスワード、VLAN ID などのユーザ情報を内蔵 Web 認証 DB に登録します。また、登録したユーザ ID ごとのパスワード変更および削除もできます。

登録・変更された内容は、運用コマンド `commit web-authentication` が実行された時点で、内蔵 Web 認証 DB に反映されます。

なお、運用コマンドで内蔵 Web 認証 DB への追加および変更を行った場合、現在認証中のユーザには適用されず、次回ログイン時から有効となります。

(2) 内蔵 Web 認証 DB のバックアップ

運用コマンド `store web-authentication` で、ローカル認証用に作成した内蔵 Web 認証 DB のバックアップを取ることができます。

(3) 内蔵 Web 認証 DB の復元

運用コマンド `load web-authentication` で、ローカル認証用に作成したバックアップファイルから、内蔵 Web 認証 DB の復元ができます。ただし、復元を実行すると、直前に運用コマンド `set web-authentication user` などで登録・更新していた内容は廃棄されて、復元された内容に置き換わりますので、注意が必要です。

10.5.2 RADIUS サーバの準備

Web 認証の RADIUS 認証方式を使用するに当たっては、事前に RADIUS サーバの設定が必要です。

また、本装置の Web 認証機能が使用する RADIUS の属性を示します。

(1) RADIUS サーバの設定

ユーザごとにユーザ ID、パスワード、VLAN ID などのユーザ情報を RADIUS サーバに設定します。なお、RADIUS サーバの詳細な設定方法については、使用する RADIUS サーバの説明書を参照してください。

ユーザごとの VLAN ID は次のように設定します。

1. Tunnel-Type に Virtual LANs (VLAN) を設定 (値 13) します。
2. Tunnel-Medium-Type に 6 を設定します。
3. Tunnel-Private-Group-ID に VLAN ID を次の形式で設定します。

- 数字文字で設定
例：VLAN ID が 2048 の場合、文字列で 2048 を設定
- 文字列 "VLAN" に続いて VLAN ID を数字文字で設定
例：VLAN ID が 2048 の場合、VLAN2048 を設定

ユーザ ID とパスワードには文字数 1 ~ 16 文字で、次の文字が使用できます。

- ユーザ ID : ASCII 文字コードの 0x21 ~ 0x7E
- パスワード : ASCII 文字コードの 0x21 ~ 0x7E

また、認証方式として PAP を設定します。

(2) Web 認証が使用する RADIUS 属性

Web 認証が使用する RADIUS の属性を次の表に示します。

表 10-3 認証で使用する属性名 (その 1 Access-Request)

属性名	Type 値	説明
User-Name	1	ユーザ名を指定します。
User-Password	2	ユーザパスワードを指定します。
NAS-IP-Address	4	ループバックインタフェースの IP アドレス指定時はループバックインタフェースの IP アドレスを格納し、指定されていない場合は RADIUS サーバと通信するインタフェースの IP アドレスを格納します。
Service-Type	6	Framed(2) を設定します。
Calling-Station-Id	31	認証端末の MAC アドレス (小文字 ASCII, "-" 区切り) を指定します。 例: 00-12-e2-12-34-56
NAS-Identifier	32	固定 VLAN モード時に認証端末を収容している VLAN ID を数字文字列で指定します。 例: VLAN ID 100 の場合 100 ダイナミック VLAN モードおよびレガシーモードでは、コンフィグレーションコマンド hostname で指定された装置名を指定します。
NAS-Port-Type	61	Virtual(5) を設定します
NAS-IPv6-Address	95	ループバックインタフェースの IPv6 アドレス指定時はループバックインタフェースの IPv6 アドレスを格納し、指定されていない場合は RADIUS サーバと通信するインタフェースの IPv6 アドレスを格納します。ただし、IPv6 リンクローカルアドレスで通信する場合は、ループバックインタフェースの IPv6 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を格納します。

表 10-4 認証で使用する属性名 (その 2 Access-Accept)

属性名	Type 値	説明
Service-Type	6	Framed(2) が返却される: Web 認証ではチェックしません。
Reply-Message	18	(未使用)
Tunnel-Type	64	ダイナミック VLAN モードおよびレガシーモード時に使用します。VLAN を示す 13 であるかをチェックします。固定 VLAN モード時は使用しません。
Tunnel-Medium-Type	65	ダイナミック VLAN モードおよびレガシーモード時に使用します。IEEE802.1X と同様の値 6 の Tunnel-Medium-Type であるかをチェックします。固定 VLAN モード時は使用しません。

属性名	Type 値	説明
Tunnel-Private-Group-Id	81	ダイナミック VLAN モードおよびレガシーモード時に使用します。 VLAN を表す数字文字列, または “ VLANxx ” xx は VLAN ID を表します。 ただし, 先頭の 1 オクテットの内容が 0x00 ~ 0x1f の場合は, Tag を表している, この場合は 2 オクテット目からの値が VLAN を 表します。また, 先頭の 1 オクテットの内容が 0x20 以上の場合は, 先頭から VLAN を表します。 固定 VLAN モード時は使用しません。

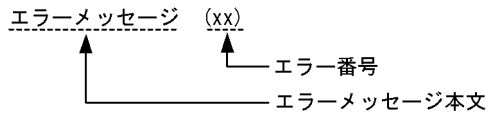
表 10-5 RADIUS Accounting で使用する属性名

属性名	Type 値	説明
User-Name	1	利用者のユーザ名称を格納します。
NAS-IP-Address	4	NAS の IP アドレスを格納します。 ループバックインタフェースの IP アドレス設定時は, ループバック インタフェースの IP アドレスを格納します。なお, 上記以外はサー バと通信するインタフェースの IP アドレスを格納します。
Service-Type	6	Framed(2) を設定します
Calling-Station-Id	31	端末の MAC アドレス (小文字 ASCII, “ - ” 区切り) を設定します。 例: 00-12-e2-12-34-56
NAS-Identifier	32	固定 VLAN モード時に認証端末を収容している VLAN ID を数字文 字列で設定します。 例: VLAN ID 100 の場合 100 ダイナミック VLAN モードおよびレガシーモードでは, コンフィグ レーションコマンド hostname で指定された装置名を指定します。
Acct-Status-Type	40	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	イベント発生時から送信するまでに必要とした時間 (秒) を格納し ます。
Acct-Session-Id	44	プロセス ID を格納します。(ログイン, ログアウトに関しては同じ 値です)
Acct-Authentic	45	ユーザがどのように認証されたかを示す RADIUS, Local のどちら かを格納します。
Acct-Session-Time	46	ログイン後ログアウトするまでの時間 (秒) を格納します。
NAS-Port-Type	61	Virtual(5) を設定します。
NAS-IPv6-Address	95	NAS の IPv6 アドレスを格納します。 ループバックインタフェースの IPv6 アドレス設定時は, ループ バックインタフェースの IPv6 アドレスを格納します。なお, 上記 以外はサーバと通信するインタフェースの IPv6 アドレスを格納し 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, ループバックインタフェースの IPv6 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を格納 します。

10.6 認証エラーメッセージ

認証エラー画面に表示される認証エラーメッセージ表示の形式を次の図に示します。

図 10-21 認証エラーメッセージ形式



認証エラーの発生理由を次の表に示します。

表 10-6 認証エラーメッセージとエラー発生理由対応表

エラーメッセージ内容	エラー番号	エラー発生理由
User ID or password is wrong. Please enter correct user ID and password.	11	ログインユーザ ID が指定されていません
	12	ログインユーザ ID が 16 文字を超えています
	13	パスワードが指定されていない、または指定された文字数が長過ぎます
	14	ログインユーザ ID が内蔵 Web 認証 DB に登録されていません
	15	パスワードが内蔵 Web 認証 DB に登録されていません
	16	GET メソッドの "QUERY_STRING" が 21 文字未満か、または、256 文字を超えています
	17	POST メソッドの "CONTENT_LENGTH" が 21 未満である、または 256 を超えています
	18	ログインユーザ ID に許可されていない文字が指定されています
	20	パスワードに許可されていない文字が指定されています
	22	ローカル認証方式で、認証済みの端末から再ログインを行った際、パスワードが一致していませんでした。
RADIUS: Authentication reject.	31	RADIUS サーバから認証許可以外（アクセス拒否またはアクセスチャレンジ）を受信しました
RADIUS: No authentication response.	32	RADIUS サーバから認証許可を受信できませんでした（受信タイムアウト、または RADIUS サーバの設定がされていない状態です）
You cannot login by this machine.	33	RADIUS に設定されている認証後 VLAN が、Web 認証で定義された VLAN ではありません。 または、VLAN インタフェースに設定されていません
	34	RADIUS 認証方式で、認証済み端末から再ログインを行った際に RADIUS サーバから認証許可以外（アクセス拒否またはアクセスチャレンジ）を受信しました
	35	固定 VLAN モードで、端末が接続されている認証対象ポートがリンクダウンの状態です。 または、ポートが固定 VLAN モードとして設定されていません

エラーメッセージ内容	エラー番号	エラー発生理由
	36	固定 VLAN モードで設定されたポートを収容する VLAN が suspend 状態になっています。 または、VLAN がインタフェースに設定されていません
	41	Web 認証で認証済みの端末から、異なるユーザでのログイン要求がありました。 または、ダイナミック VLAN モードで、異なる VLAN から認証済み端末のログイン要求がありました
	42	内蔵 Web 認証 DB に設定された VLAN ID が、Web 認証で定義された VLAN ではありません。 または、VLAN インタフェースに設定されていません
	44	同一端末で、IEEE802.1X もしくは MAC 認証によって認証済み、またはコンフィグレーションコマンド mac-address で端末の MAC アドレスが MAC VLAN に登録済みのため認証できません
	45	端末が接続されている認証対象ポートがリンクダウンの状態です。 または、ポートが固定 VLAN モードとして設定されていません
	46	認証対象ポートを収容する VLAN が suspend 状態になっています。 または、VLAN がインタフェースに設定されていません
	47	Web 認証のログイン数が最大収容条件を超えたために認証できませんでした
	76	MAC アドレスを MAC アドレステーブルに登録する際、端末が接続されているポートがリンクダウンしています。 または、ポートが固定 VLAN モードとして設定されていません
	77	MAC アドレスを MAC アドレステーブルに登録する際、収容する VLAN が suspend 状態になっています。 または、VLAN がインタフェースに設定されていません
Sorry, you cannot login just now. Please try again after a while.	37	RADIUS 認証途中の認証要求が 256 件を超えています。 再度、ログイン操作を行ってください
	43	Web 認証、MAC 認証、または IEEE802.1X 認証のログイン数が装置最大収容条件を超えたために認証できませんでした
	51	ログイン端末の IP アドレスから MAC アドレスを解決できませんでした
	52	Web サーバが、Web 認証デーモンと接続できませんでした
	53	Web 認証の内部エラー (Web サーバが、Web 認証デーモンにログイン要求を渡せませんでした)
	54	Web 認証の内部エラー (Web サーバが、Web 認証デーモンから応答を受け付けられませんでした)
The system error occurred. Please contact the system administrator.	61	Web 認証の内部エラー (POST メソッドの "CONTENT_LENGTH" が取得できませんでした)
	62	Web 認証の内部エラー (POST/GET で受け取ったパラメータに "&" が 2 個以上含まれていました)

エラーメッセージ内容	エラー番号	エラー発生理由
	63	Web 認証の内部エラー (Web サーバで端末の IP アドレスが取得できませんでした)
	64	RADIUS および Accounting へのアクセスができませんでした(認証失敗となります)
A fatal error occurred. Please inform the system administrator.	65	Web 認証の内部エラー (同時に 256 件を超えた RADIUS への認証要求が起きました)
	72	MAC VLAN に認証した MAC アドレスを登録できませんでした
	73	MAC VLAN から認証解除する MAC アドレスを削除できませんでした
	74	MAC アドレスを MAC アドレステーブルに登録する際にエラーが発生しました
	75	MAC アドレステーブルから MAC アドレスを削除する際にエラーが発生しました
Sorry, you cannot logout just now. Please try again after a while.	81	ログアウト要求された端末の IP アドレスから MAC アドレスを解決できませんでした
The client PC is not authenticated.	82	ログインされていない端末からのログアウト要求です

エラー番号ごとの対処方法

- 1x ~ 2x : 正しいユーザ ID とパスワードで再度ログイン操作を行ってください。
- 3x : RADIUS の設定を見直してください。
- 4x : Web 認証のコンフィグレーション, および内蔵 Web 認証 DB の設定を見直してください。
- 5x : 再度ログイン操作を行ってください。再び本メッセージが表示される場合は, 運用コマンド `restart web-authentication` で Web 認証を再起動してください。
- 6x ~ 7x : 運用コマンド `restart web-authentication` で Web 認証を再起動してください。
- 8x : 再度ログアウト操作を行ってください。

10.7 Web 認証画面入れ替え機能

Web 認証で使用するログイン画面やログアウト画面など、Web ブラウザに表示する画面情報（以降、Web 認証画面と呼びます）は、運用コマンドで入れ替えることができます。その運用コマンドで指定したディレクトリ配下に、次に示す画面のファイルがあった場合、該当する Web 認証画面と置き換えます。また、次に示すファイル以外に gif ファイルなどの画像ファイルも同時に登録できます。ただし、登録時には各ファイルのサイズチェックだけを行い、ファイルの内容はチェックしませんので、必ず動作確認を行ってから HTML ファイルや画像ファイルを登録してください。

入れ替えることができる画面を次に示します。

[入れ替え可能な画面]

- ログイン画面
- ログアウト画面
- ログイン成功画面
- ログイン失敗画面
- ログアウト完了画面
- ログアウト失敗画面

なお、登録した Web 認証画面は運用コマンドで削除できます。削除したあとは、デフォルトの Web 認証画面に戻ります。

また、「表 10-6 認証エラーメッセージとエラー発生理由対応表」に示す認証エラーメッセージも入れ替えることができます。

さらに、Web ブラウザのお気に入りに表示するアイコン（favicon.ico）も入れ替えることができます。

各ファイルの詳細は、「11.3 Web 認証画面作成手順」を参照してください。

なお、Web 認証画面の登録中に次に示すような中断が起きた場合、登録した画面が表示されずにデフォルト画面が表示されます。このとき、運用コマンド `show web-authentication html-files` で Web 認証画面の登録情報を表示すると、登録が成功したかのように表示されることがあります。

- Web 認証画面登録中に [Ctrl] + [C] キーを押して、意図的に処理を中断させた場合
- telnet 経由でコンソールにログインし、Web 認証画面登録中に telnet が何らかの要因で切断された場合

Web 認証画面の登録中に中断が起きた場合は、再度 Web 認証画面を登録してください。

10.8 系切替時の引き継ぎ情報

系切替時には次の情報が引き継がれます。

内蔵 Web 認証 DB

[引き継ぎ契機]

- 運用コマンド `commit web-authentication` の実行時に待機系システムに反映されます。
- 運用コマンド `synchronize` の実行時に待機系システムに反映されます。

登録された Web 認証画面情報

[引き継ぎ契機]

- 運用コマンド `set web-authentication html-files` の実行時に待機系システムに反映されます。
- 運用コマンド `clear web-authentication html-files` の実行時に待機系システムに反映されます。

ログインユーザ情報

[引き継ぎ契機]

- 次の情報が、系切替時に新運用系システムに引き継がれます。
ユーザ ID, 認証後の VLAN ID, MAC アドレス, ログイン時間, 最大接続時間, 端末が接続されているポート番号

10.9 Web 認証使用時の注意事項

(1) 他機能との共存

他機能との共存については、「7.2 レイヤ 2 認証と他機能との共存について」を参照してください。

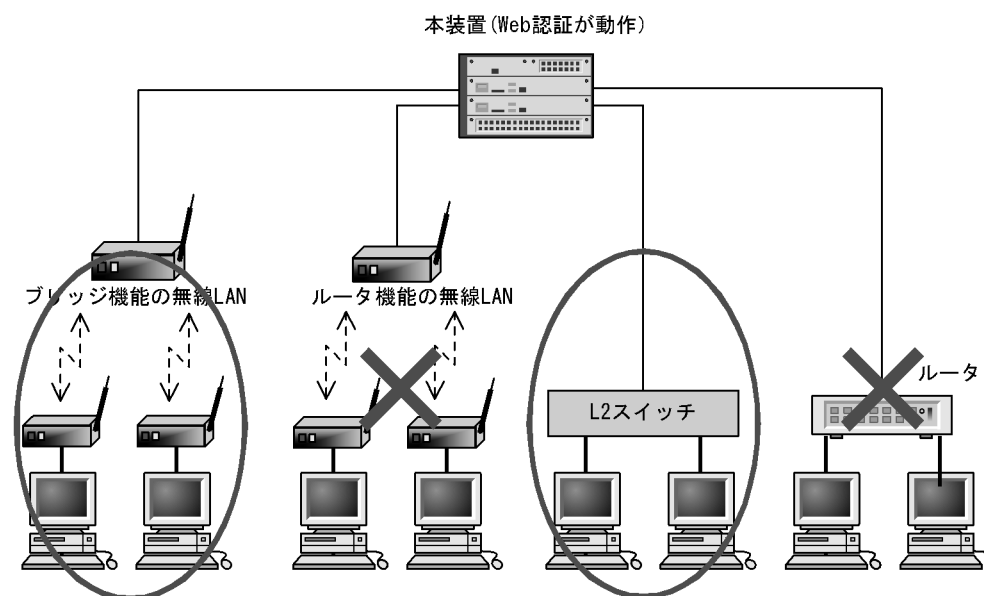
(2) 本装置と認証対象の端末間に接続する装置について

本装置の配下にはプロキシサーバやルータを接続しないでください。

本装置と認証端末との間の経路上に、クライアント端末の MAC アドレスを書き換えるもの（プロキシサーバやルータなど）が存在した場合、Web 認証が書き換えられた MAC アドレスを認証対象端末と認識してしまうために端末ごとの認証ができません。

また、本装置の配下にポート間遮断機能の無い HUB や無線 LAN を接続し、それに複数の PC が接続されている場合、認証済みでなくても PC 同士で通信ができてしまいますので注意が必要です。

図 10-22 本装置と端末間の接続

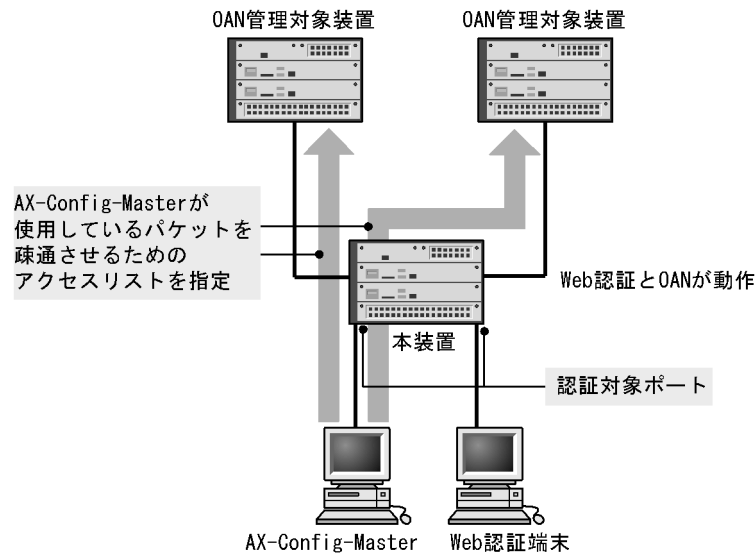


(3) OAN との共存について

Web 認証は OAN と共存できますが、次に示す条件があります。

- 本装置の認証対象ポートに AX-Config-Master を接続し、Web 認証を行わずに本装置で使用したい場合は、コンフィグレーションコマンド `web-authentication web-port` で OAN が使用する https ポート (832, 9698) を指定する必要があります。
- 認証対象ポートに AX-Config-Master を接続し、Web 認証を行わずに本装置の外部に接続された装置を管理する場合、次の図に示すようにアクセスリストで OAN が使用する IP パケットを通信させる設定が必要です。

図 10-23 OAN との共存



(4) VLAN 機能が再起動した場合の動作

運用コマンド `restart vlan` で VLAN 機能が再起動した場合、Web 認証は認証を解除しないで、認証された順に再登録をします。ただし、認証数が多い場合、登録に時間が掛かるため、登録が完了するまでの間通信ができなくなりますが、登録が完了した時点で通信ができます。

(5) Web 認証プログラムが再起動した場合

Web 認証デーモンが再起動した場合、認証中のユーザすべての認証が解除されます。この場合、再起動後に端末から手動で再度認証を行ってください。

(6) レガシーモードでの再認証時の認証後 VLAN について

レガシーモードで、認証済みの端末から認証済みのユーザ ID でログイン操作（再認証操作）を行って認証成功となった際、RADIUS サーバから送られてくる VLAN ID または内蔵 Web 認証 DB に設定された VLAN ID に変更があっても、すでに収容されている VLAN から変更はありません。

ローカル認証方式の場合も RADIUS 認証方式の場合も同様に、最初に認証成功となった時点で収容した認証後 VLAN からの変更は行いません。

11 Web 認証の設定と運用

Web 認証は、Web ブラウザを用いて認証されたユーザ単位に VLAN へのアクセス制御を行う機能です。この章では Web 認証のオペレーションについて解説します。

11.1 コンフィグレーション

11.2 オペレーション

11.3 Web 認証画面作成手順

11.1 コンフィグレーション

11.1.1 コンフィグレーションコマンド一覧

Web 認証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 11-1 コンフィグレーションコマンド一覧

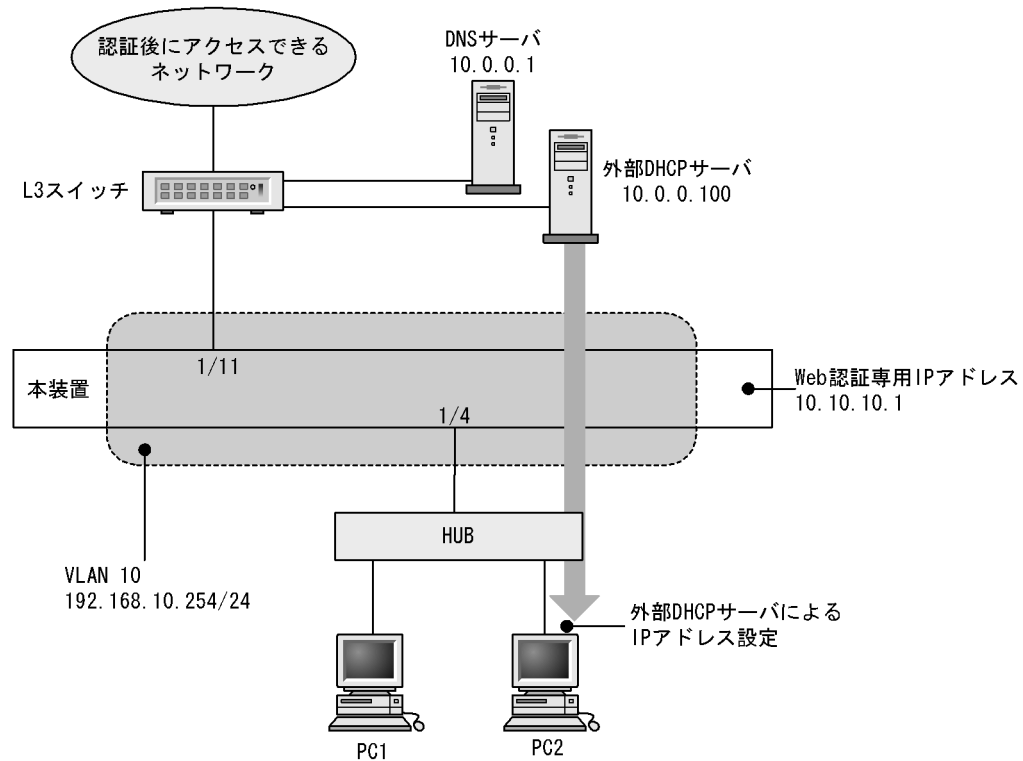
コマンド名	説明
aaa accounting web-authentication default start-stop group radius	アカウントサーバの使用設定をします。
aaa authentication web-authentication default group radius	RADIUS サーバの使用設定をします。
web-authentication auto-logout	MAC アドレス学習エージアウトによる強制ログアウト機能を設定します。
web-authentication ip address	固定 VLAN モード時およびダイナミック VLAN モード時の Web 認証専用 IP アドレスを指定します。
web-authentication jump-url	認証成功后、端末からアクセスする URL を指定します。
web-authentication logging enable	認証結果と動作ログの syslog サーバへの出力を開始します
web-authentication logout ping tos-windows	認証済み端末から送出される特殊 ping の TOS 値を指定します。
web-authentication logout ping ttl	認証済み端末から送出される特殊 ping の TTL 値を指定します。
web-authentication logout polling count	監視パケットに対する応答が無かった場合の再送する監視パケットの再送回数を指定します。
web-authentication logout polling enable	認証済み端末の動作を監視する接続監視機能を有効にします。
web-authentication logout polling interval	接続監視機能で使用する監視パケット (ARP) の送出時間を指定します。
web-authentication logout polling retry-interval	監視パケットに対する応答が無い場合に再送する監視パケットの時間間隔を指定します。
web-authentication max-timer	Web 認証の最大接続時間を指定します。
web-authentication max-user	Web 認証でダイナミック VLAN モードおよびレガシーモードの時に認証できる最大認証数を指定します。
web-authentication port	固定 VLAN モードおよびダイナミック VLAN モードの認証対象となるポートを指定します。
web-authentication redirect-mode	URL リダイレクト時、端末に表示するログイン操作のプロトコル (http または https) を指定します。
web-authentication redirect-vlan	ダイナミック VLAN モードを設定する MAC ポートのネイティブ VLAN を指定します。
web-authentication static-vlan max-user	固定 VLAN モードで認証できるユーザ数を指定します。
web-authentication system-auth-control	Web 認証を有効にします。
web-authentication vlan	レガシーモードで、Web 認証で切り替えを許可する切り替え後の VLAN を指定します。
web-authentication web-port	Web サーバへのアクセスポート番号を追加した場合に指定します。

11.1.2 固定 VLAN モードのコンフィグレーション

(1) ローカル認証方式の基本的な設定

ローカル認証方式を使用する上での基本的な設定を次の図に示します。

図 11-1 固定 VLAN モードのローカル認証方式の基本構成



(a) 認証ポートの設定

[設定のポイント]

Web 認証で使用するポートを設定します。

[コマンドによる設定]

1. `(config)# vlan 10`
`(config-vlan)# state active`
`(config-vlan)# exit`
2. `(config)# interface gigabitethernet 1/4`
`(config-if)# switchport mode access`
`(config-if)# switchport access vlan 10`
`(config-if)# web-authentication port`
`(config-if)# exit`

認証を行う端末が接続されているポートに VLAN ID と Web 認証を設定します。

3. `(config)# interface gigabitethernet 1/11`
`(config-if)# switchport mode access`
`(config-if)# switchport access vlan 10`
`(config-if)# exit`

認証後にアクセスするネットワークの L3 スイッチを接続するポートを指定します。

(b) VLAN インタフェースに IP アドレスを設定

[設定のポイント]

Web 認証で使用する VLAN に IP アドレスを設定します。

[コマンドによる設定]

1. (config)# interface vlan 10
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# exit

Web 認証で使用する VLAN ID 10 に IP アドレスを設定します。

(c) DHCP リレーの設定

[設定のポイント]

端末の認証に必要な外部 DHCP への DHCP リレー設定を設定します。

[コマンドによる設定]

1. (config)# interface vlan 10
(config-if)# ip helper-address 10.0.0.100
(config-if)# exit

外部 DHCP サーバ用の DHCP リレーを設定します。

(d) Web 認証の設定

[設定のポイント]

Web 認証のコンフィグレーションコマンドを設定して Web 認証を有効にします。

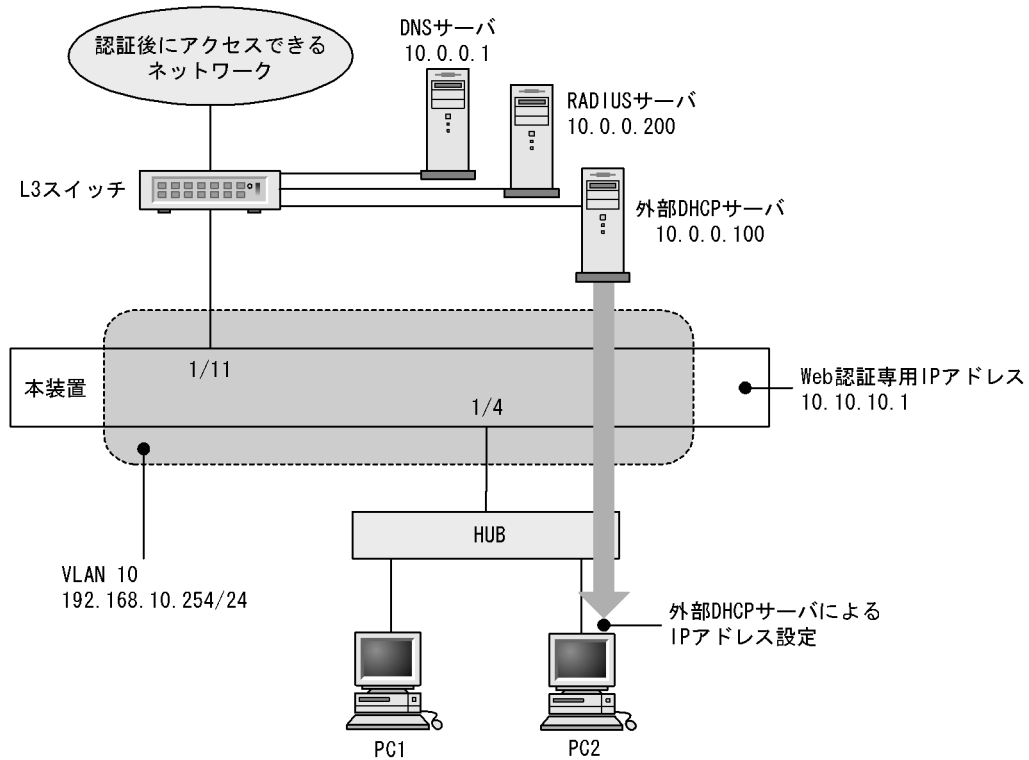
[コマンドによる設定]

1. (config)# web-authentication ip address 10.10.10.1
Web 認証専用の IP アドレス (IPv4 アドレス) を設定します。
2. (config)# web-authentication system-auth-control
Web 認証を起動します。

(2) RADIUS 認証方式の基本的な設定

RADIUS 認証方式を使用する上での基本的な設定を次の図に示します

図 11-2 固定 VLAN モードの RADIUS 認証方式の基本構成



(a) 認証ポートの設定

[設定のポイント]

Web 認証で使用するポートを設定します。

[コマンドによる設定]

1. (config)# vlan 10
(config-vlan)# state active
(config-vlan)# exit
2. (config)# interface gigabitethernet 1/4
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# web-authentication port
(config-if)# exit

認証を行う端末が接続されているポートに VLAN ID と Web 認証を設定します。

3. (config)# interface gigabitethernet 1/11
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# exit

認証後にアクセスするネットワークの L3 スイッチを接続するポートを指定します。

(b) VLAN インタフェースに IP アドレスを設定

[設定のポイント]

Web 認証で使用する VLAN に IP アドレスを設定します。

[コマンドによる設定]

1. (config)# interface vlan 10
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# exit

Web 認証で使用する VLAN ID 10 に IP アドレスを設定します。

(c) DHCP リレーの設定

[設定のポイント]

端末の認証に必要な外部 DHCP への DHCP リレー設定を設定します。

[コマンドによる設定]

1. (config)# interface vlan 10
(config-if)# ip helper-address 10.0.0.100
(config-if)# exit

外部 DHCP サーバ用の DHCP リレーを設定します。

(d) Web 認証の設定

[設定のポイント]

Web 認証のコンフィグレーションコマンドを設定して Web 認証を有効にします。

[コマンドによる設定]

1. (config)# web-authentication ip address 10.10.10.1
Web 認証専用の IP アドレス (IPv4 アドレス) を設定します。
2. (config)# aaa authentication web-authentication default group radius
(config)# radius-server host 10.0.0.200 key "webauth"
ユーザ認証を RADIUS サーバで行うための IP アドレスと RADIUS 鍵を設定します。
3. (config)# web-authentication system-auth-control
Web 認証を起動します。

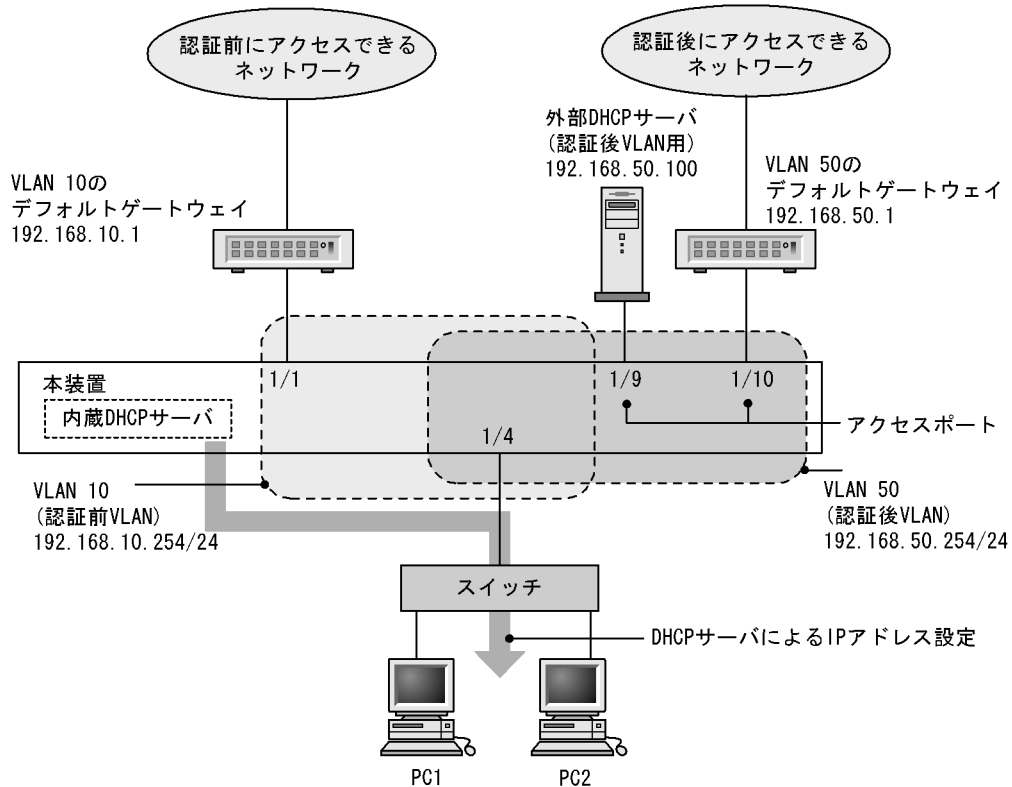
11.1.3 ダイナミック VLAN モードのコンフィグレーション

(1) ローカル認証方式の基本的な設定

ローカル認証方式を使用する際の基本的な設定を次の図に示します。なお、端末の IP アドレスは、認証前は本装置内 DHCP サーバから配布し、認証後は外部 DHCP サーバから配布します。

さらに、認証前 VLAN と認証後 VLAN 間の通信を禁止するフィルタを設定します。

図 11-3 ダイナミック VLAN モードのローカル認証方式の基本構成



(a) 認証ポートの設定

[設定のポイント]

Web 認証で使用するポートを設定します。

[コマンドによる設定]

- ```
(config)# interface gigabitethernet 1/4
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 50
(config-if)# switchport mac native vlan 10
(config-if)# web-authentication port
(config-if)# exit
```

認証を行う端末が接続されているポートに MAC VLAN と Web 認証を設定します。

- ```
(config)# interface range gigabitethernet 1/9-10
(config-if-range)# switchport mode access
(config-if-range)# switchport access vlan 50
(config-if-range)# exit
```

認証後にアクセスするネットワークのポートを指定します。

(b) VLAN インタフェースに IP アドレスを設定

[設定のポイント]

認証前 VLAN および認証後 VLAN に IP アドレスを設定します。

[コマンドによる設定]

1. (config)# interface vlan 10
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# exit
(config)# interface vlan 50
(config-if)# ip address 192.168.50.254 255.255.255.0
(config-if)# exit

認証前 VLAN と認証後 VLAN に各 IP アドレスを設定します。

(c) Web 認証の設定

[設定のポイント]

Web 認証のコンフィグレーションコマンドを設定して Web 認証を有効にします。

[コマンドによる設定]

1. (config)# web-authentication ip address 10.10.10.1
Web 認証専用の IP アドレス (IPv4 アドレス) を設定します。
2. (config)# web-authentication system-auth-control
Web 認証を起動します。

(2) RADIUS 認証方式の基本的な設定

RADIUS 認証方式を使用する際の基本的な設定を次の図に示します。なお、端末の IP アドレスは、認証前は本装置内 DHCP サーバから配布し、認証後は外部 DHCP サーバから配布します。

さらに、認証前 VLAN と認証後 VLAN 間の通信を禁止するフィルタを設定します。

[コマンドによる設定]

1. (config)# interface vlan 10
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# exit
(config)# interface vlan 50
(config-if)# ip address 192.168.50.254 255.255.255.0
(config-if)# exit

認証前 VLAN と認証後 VLAN に各 IP アドレスを設定します。

(c) Web 認証の設定

[設定のポイント]

Web 認証のコンフィグレーションコマンドを設定して Web 認証を有効にします。

[コマンドによる設定]

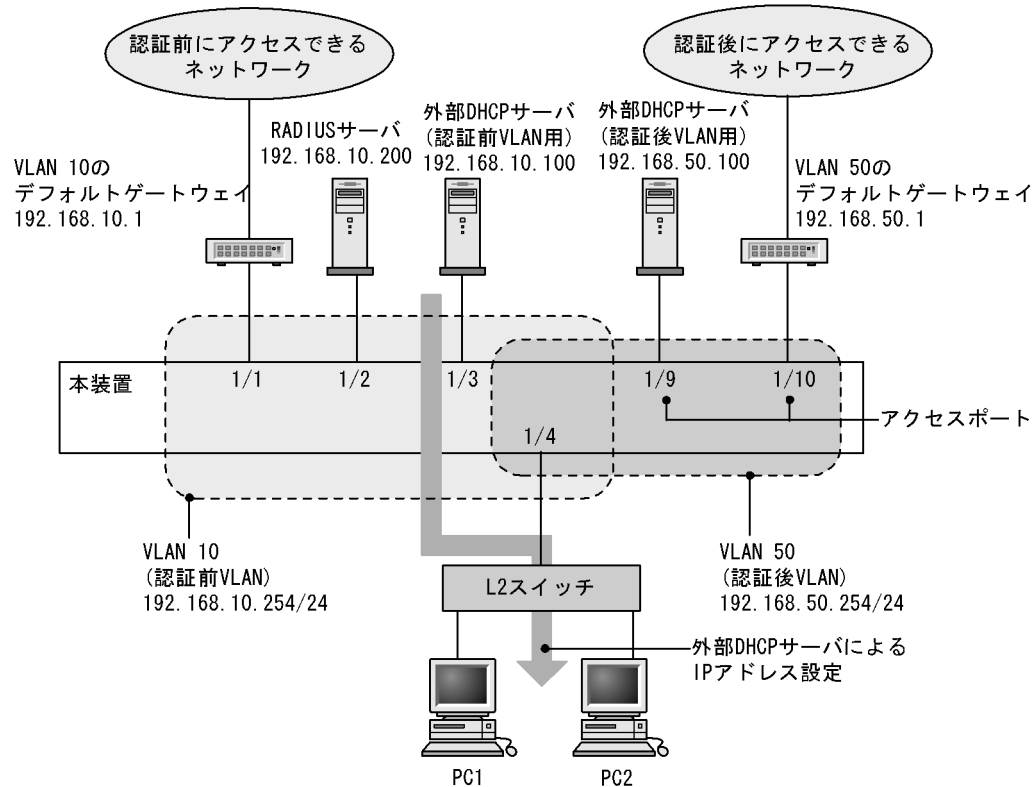
1. (config)# web-authentication ip address 10.10.10.1
Web 認証専用の IP アドレス (IPv4 アドレス) を設定します。
2. (config)# aaa authentication web-authentication default group radius
(config)# radius-server host 192.168.10.200 key "webauth"
ユーザ認証を RADIUS サーバで行うための IP アドレスと RADIUS 鍵を設定します。
3. (config)# web-authentication system-auth-control
Web 認証を起動します。

(3) RADIUS 認証方式 + 認証前に外部 DHCP サーバ使用時の設定

RADIUS 認証方式で認証前および認証後に、端末の IP アドレスをそれぞれの外部 DHCP サーバから配布する際の構成を次に示します。

さらに、認証前 VLAN と認証後 VLAN 間の通信を禁止するフィルタを設定します。

図 11-5 ダイナミック VLAN モードの RADIUS 認証方式 + 外部 DHCP サーバ使用時の構成



(a) 認証ポートの設定

[設定のポイント]

Web 認証で使用するポートを設定します。

[コマンドによる設定]

- ```
(config)# interface gigabitethernet 1/4
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 50
(config-if)# switchport mac native vlan 10
(config-if)# web-authentication port
(config-if)# exit
```

認証を行う端末が接続されているポートに MAC VLAN と Web 認証を設定します。

- ```
(config)# interface range gigabitethernet 1/9-10
(config-if-range)# switchport mode access
(config-if-range)# switchport access vlan 50
(config-if-range)# exit
```

認証後にアクセスするネットワークのポートを指定します。

(b) VLAN インタフェースに IP アドレスを設定

[設定のポイント]

認証前 VLAN および認証後 VLAN に IP アドレスを設定します。

[コマンドによる設定]

1. (config)# interface vlan 10
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# exit
(config)# interface vlan 50
(config-if)# ip address 192.168.50.254 255.255.255.0
(config-if)# exit

認証前 VLAN と認証後 VLAN に各 IP アドレスを設定します。

(c) Web 認証の設定

[設定のポイント]

Web 認証のコンフィグレーションコマンドを設定して Web 認証を有効にします。

[コマンドによる設定]

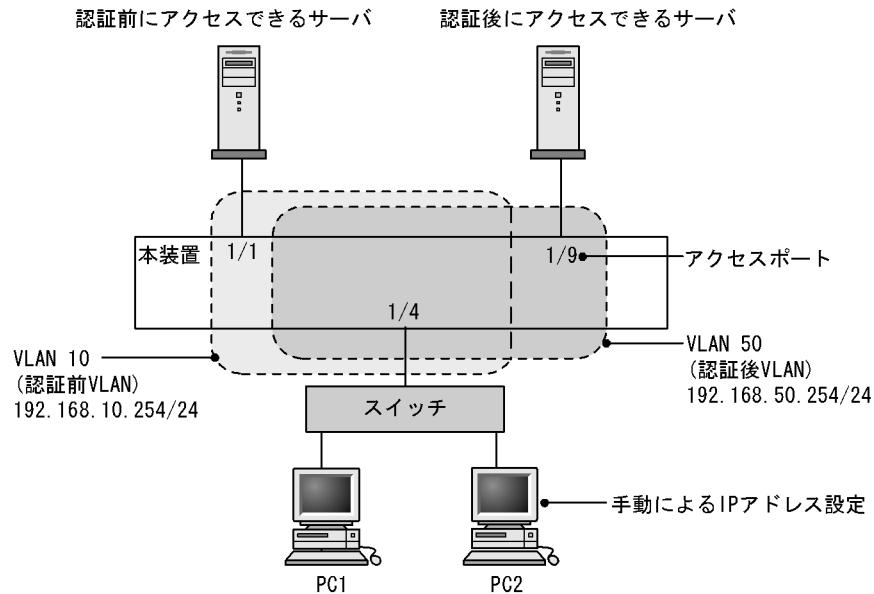
1. (config)# web-authentication ip address 10.10.10.1
Web 認証専用の IP アドレス (IPv4 アドレス) を設定します。
2. (config)# aaa authentication web-authentication default group radius
(config)# radius-server host 192.168.10.200 key "webauth"
ユーザ認証を RADIUS サーバで行うための IP アドレスと RADIUS 鍵を設定します。
3. (config)# web-authentication system-auth-control
Web 認証を起動します。

11.1.4 レガシーモードのコンフィグレーション

(1) ローカル認証方式の基本的な設定

ローカル認証方式を使用する上での基本的な設定を次の図に示します。なお、端末 (PC1, PC2) の IP アドレスは、端末側で認証前と認証後に手動で切り替えるものとします。

図 11-6 ローカル認証方式の構成例



認証前 VLAN と認証後 VLAN を設定し、アクセスリストの設定をしたあとに、Web 認証の設定をします。また、認証前 VLAN から認証後 VLAN に対して通信を許可しないよう、認証後 VLAN から認証前 VLAN に対して Web ブラウザとの通信だけを許可するアクセスリストを設定します。

(a) 認証ポートの設定

[設定のポイント]

Web 認証で使用するポートを設定します。

[コマンドによる設定]

1. (config)# interface gigabitethernet 1/4
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 50
(config-if)# switchport mac native vlan 10
(config-if)# exit

認証を行う端末が接続されているポートに認証前 VLAN と認証後 VLAN を指定します。

2. (config)# interface gigabitethernet 1/9
(config-if)# switchport mode access
(config-if)# switchport access vlan 50
(config-if)# exit

認証後に接続するサーバを接続するポートに認証後 VLAN を指定します。

(b) VLAN インタフェースに IP アドレスを設定

[設定のポイント]

認証前 VLAN および認証後 VLAN に IP アドレスを設定します。

[コマンドによる設定]

1. (config)# interface vlan 10

```
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# exit
(config)# interface vlan 50
(config-if)# ip address 192.168.50.254 255.255.255.0
(config-if)# exit
```

認証前 VLAN と認証後 VLAN に各 IP アドレスを設定します。

(c) アクセスリストの設定

[設定のポイント]

認証後 VLAN と認証前 VLAN のアクセスリストを設定します。

[コマンドによる設定]

```
1. (config)# ip access-list extended 100
   (config-ext-nacl)# permit ip 192.168.10.0 0.0.0.255 192.168.10.0 0.0.0.255
   (config-ext-nacl)# deny ip any any
   (config-ext-nacl)# exit
   (config)# interface vlan 10
   (config-if)# ip access-group 100 in layer3-forwarding
   (config-if)# exit
```

認証前 VLAN からは認証後 VLAN に対して通信を許可しないようアクセスリストを設定します。

```
2. (config)# ip access-list extended 150
   (config-ext-nacl)# permit tcp 192.168.50.0 0.0.0.255 host 192.168.10.254 eq
   http
   (config-ext-nacl)# permit ip 192.168.50.0 0.0.0.255 any
   (config-ext-nacl)# deny ip any any
   (config-ext-nacl)# exit
   (config)# interface vlan 50
   (config-if)# ip access-group 150 in layer3-forwarding
   (config-if)# exit
```

認証後 VLAN からは認証前 VLAN に対してアクセスリストを設定します。

(d) Web 認証の設定

[設定のポイント]

Web 認証のコンフィグレーションコマンドを設定して Web 認証を有効にします。

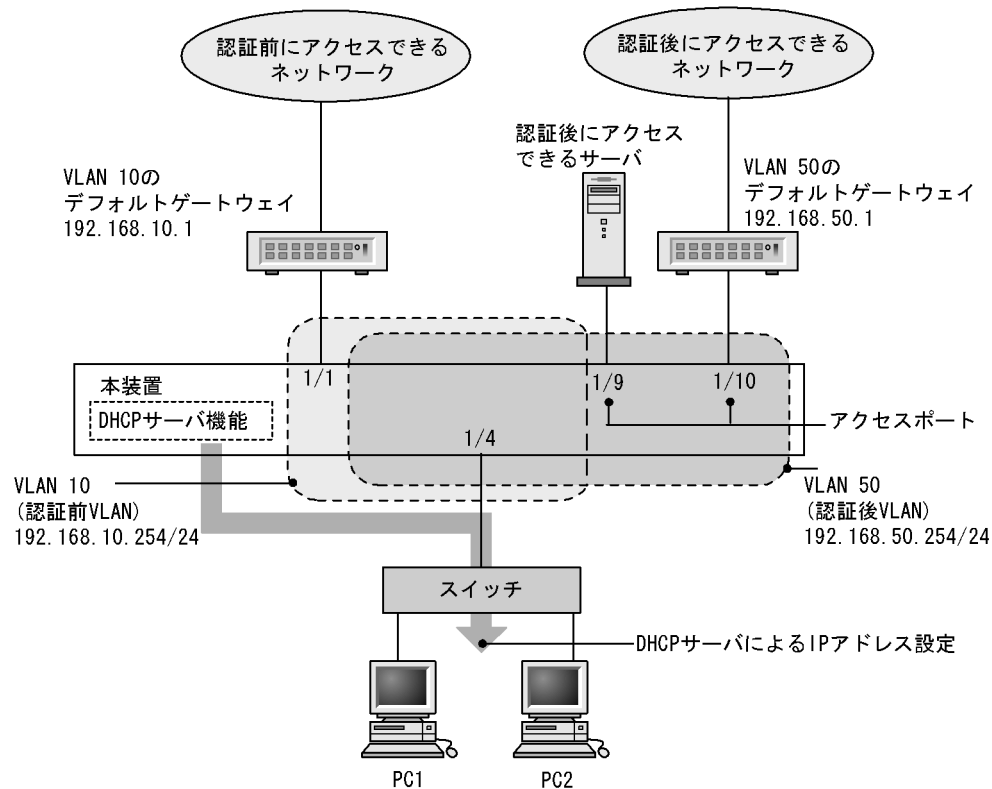
[コマンドによる設定]

1. (config)# web-authentication vlan 50
Web 認証の認証後 VLAN を設定するコンフィグレーションコマンドで VLAN ID を設定します。
2. (config)# web-authentication system-auth-control
Web 認証を起動します。

(2) ローカル認証方式 + 内蔵 DHCP サーバ使用時の構成

ローカル認証方式に内蔵 DHCP サーバを使用して Web 認証を構成した際の設定例を、次の図に示します。なお、端末 (PC1, PC2) の IP アドレスは、本装置内蔵の DHCP サーバ機能で割り当てるものとします。

図 11-7 ローカル認証方式 + 内蔵 DHCP 使用時の構成例



認証前 VLAN と認証後 VLAN を設定し、アクセスリスト、DHCP サーバの設定を行ったあとに、Web 認証の設定をします。また、認証前 VLAN からは認証後 VLAN に対して通信を許可しないよう、認証後 VLAN から認証前 VLAN に対して Web ブラウザとの通信だけを許可するアクセスリストを設定します。

(a) 認証ポートの設定

[設定のポイント]

Web 認証で使用するポートを設定します。

[コマンドによる設定]

- (config)# interface gigabitethernet 1/4
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 50
(config-if)# switchport mac native vlan 10
(config-if)# exit

認証を行う端末が接続されているポートに認証前 VLAN と認証後 VLAN を指定します。

- (config)# interface range gigabitethernet 1/9-10
(config-if-range)# switchport mode access
(config-if-range)# switchport access vlan 50

```
(config-if-range)# exit
```

認証後に接続するサーバを接続するポートに認証後 VLAN を指定します。

(b) VLAN インタフェースに IP アドレスを設定

[設定のポイント]

認証前 VLAN および認証後 VLAN に IP アドレスを設定します。

[コマンドによる設定]

```
1. (config)# interface vlan 10
   (config-if)# ip address 192.168.10.254 255.255.255.0
   (config-if)# exit
   (config)# interface vlan 50
   (config-if)# ip address 192.168.50.254 255.255.255.0
   (config-if)# exit
```

認証前 VLAN と認証後 VLAN に各 IP アドレスを設定します。

(c) アクセスリストの設定

[設定のポイント]

認証後 VLAN と認証前 VLAN のアクセスリストを設定します。

[コマンドによる設定]

```
1. (config)# ip access-list extended 100
   (config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 255.255.255.255 eq bootps
   (config-ext-nacl)# permit ip 192.168.10.0 0.0.0.255 192.168.10.0 0.0.0.255
   (config-ext-nacl)# deny ip any any
   (config-ext-nacl)# exit
   (config)# interface vlan 10
   (config-if)# ip access-group 100 in layer3-forwarding
   (config-if)# exit
```

認証前 VLAN からは認証後 VLAN に対して通信を許可しないよう、アクセスリストを設定します。

```
2. (config)# ip access-list extended 150
   (config-ext-nacl)# permit tcp 192.168.50.0 0.0.0.255 host 192.168.10.254 eq
   http
   (config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 255.255.255.255
   (config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.10.254
   (config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.50.254
   (config-ext-nacl)# permit ip 192.168.50.0 0.0.0.255 any
   (config-ext-nacl)# deny ip any any
   (config-ext-nacl)# exit
   (config)# interface vlan 50
   (config-if)# ip access-group 150 in layer3-forwarding
   (config-if)# exit
```

認証後 VLAN からは認証前 VLAN に対し、Web ブラウザからの通信だけ中継を許可するよう、アクセスリストを設定します。

(d) DHCP サーバの設定

[設定のポイント]

端末に IP アドレスを配布するための DHCP サーバを設定します。

[コマンドによる設定]

1. (config)# service dhcp vlan 10
 (config)# ip dhcp excluded-address 192.168.10.1
 (config)# ip dhcp excluded-address 192.168.10.254
 (config)# ip dhcp pool POOL10
 (dhcp-config)# network 192.168.10.0/24
 (dhcp-config)# lease 0 0 1
 (dhcp-config)# default-router 192.168.10.1
 (dhcp-config)# exit

DHCP サーバに認証前 VLAN 用の設定をします (端末認証に使用する IP アドレスの配布を設定します。デフォルトルータの IP アドレス 192.168.10.1 を設定します。)

2. (config)# service dhcp vlan 50
 (config)# ip dhcp excluded-address 192.168.50.1
 (config)# ip dhcp excluded-address 192.168.50.254
 (config)# ip dhcp pool POOL50
 (dhcp-config)# network 192.168.50.0/24
 (dhcp-config)# lease 0 0 1
 (dhcp-config)# default-router 192.168.50.1
 (dhcp-config)# exit

DHCP サーバに認証後 VLAN 用の設定をします (認証された端末で使用する IP アドレスの配布を設定します。デフォルトルータの IP アドレス 192.168.50.1 を設定します。)

(e) Web 認証の設定

[設定のポイント]

Web 認証のコンフィグレーションコマンドを設定して Web 認証を有効にします。

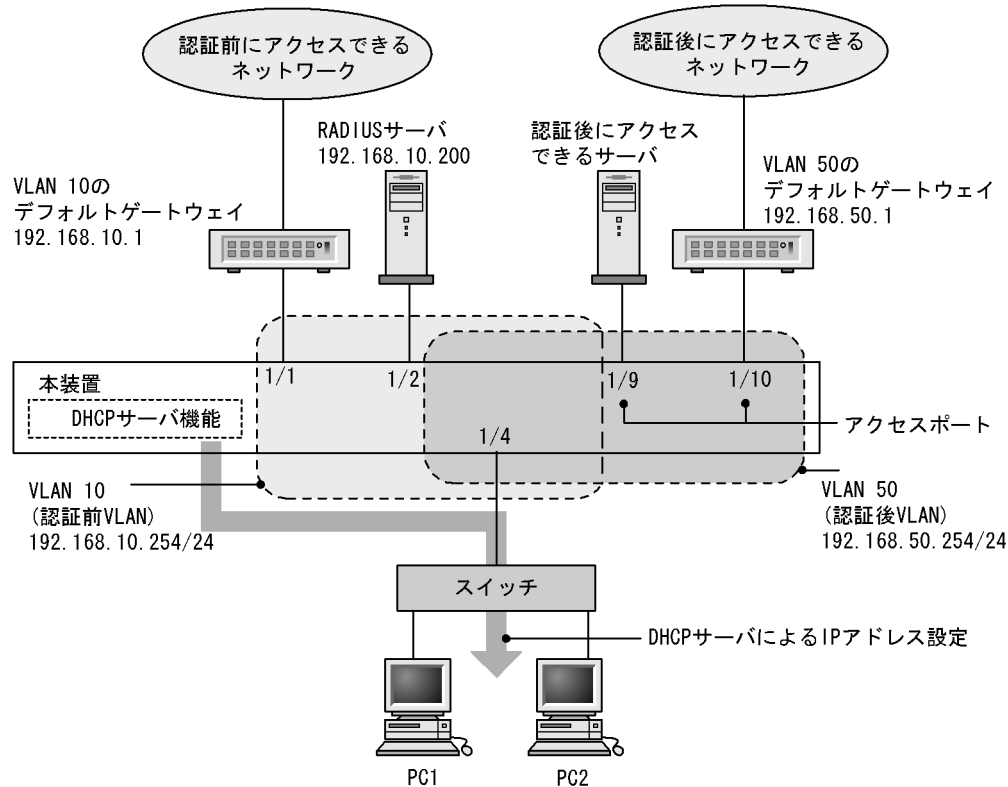
[コマンドによる設定]

1. (config)# web-authentication vlan 50
 Web 認証の認証後 VLAN を設定するコンフィグレーションコマンドで VLAN ID を設定します。
2. (config)# web-authentication system-auth-control
 Web 認証を起動します。

(3) RADIUS 認証方式 + 内蔵 DHCP サーバ使用時の構成

RADIUS 認証方式と内蔵 DHCP サーバを使用して Web 認証を構成した際の設定例を、次の図に示します。なお、端末 (PC1 , PC2) の IP アドレスは、本装置内蔵の DHCP サーバ機能で割り当てるものとします。

図 11-8 Web 認証の RADIUS 認証方式 + 内蔵 DHCP 使用時の構成例



認証前 VLAN と認証後 VLAN を設定し、アクセスリスト、DHCP サーバの設定を行ったあとに、Web 認証の設定をします。また、認証前 VLAN からは認証後 VLAN に対して通信を許可しないよう、認証後 VLAN から認証前 VLAN に対して Web ブラウザとの通信だけを許可するアクセスリストを設定します。

(a) 認証ポートの設定

[設定のポイント]

Web 認証で使用するポートを設定します。

[コマンドによる設定]

1. (config)# interface gigabitethernet 1/4
 (config-if)# switchport mode mac-vlan
 (config-if)# switchport mac vlan 50
 (config-if)# switchport mac native vlan 10
 (config-if)# exit

認証を行う端末が接続されているポートに認証前 VLAN と認証後 VLAN を指定します。

2. (config)# interface range gigabitethernet 1/9-10
 (config-if-range)# switchport mode access
 (config-if-range)# switchport access vlan 50
 (config-if-range)# exit

認証後に接続するサーバを接続するポートに認証後 VLAN を指定します。

(b) VLAN インタフェースに IP アドレスを設定

[設定のポイント]

認証前 VLAN および認証後 VLAN に IP アドレスを設定します。

[コマンドによる設定]

```
1. (config)# interface vlan 10
   (config-if)# ip address 192.168.10.254 255.255.255.0
   (config-if)# exit
   (config)# interface vlan 50
   (config-if)# ip address 192.168.50.254 255.255.255.0
   (config-if)# exit
```

認証前 VLAN と認証後 VLAN に各 IP アドレスを設定します。

(c) アクセスリストの設定

[設定のポイント]

認証後 VLAN と認証前 VLAN のアクセスリストを設定します。

[コマンドによる設定]

```
1. (config)# ip access-list extended 100
   (config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 255.255.255.255 eq bootps
   (config-ext-nacl)# permit ip 192.168.10.0 0.0.0.255 192.168.10.0 0.0.0.255
   (config-ext-nacl)# deny ip any any
   (config-ext-nacl)# exit
   (config)# interface vlan 10
   (config-if)# ip access-group 100 in layer3-forwarding
   (config-if)# exit
```

認証前 VLAN からは認証後 VLAN に対して通信を許可しないよう、アクセスリストを設定します。

```
2. (config)# ip access-list extended 150
   (config-ext-nacl)# permit tcp 192.168.50.0 0.0.0.255 host 192.168.10.254 eq
   http
   (config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 255.255.255.255
   (config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.10.254
   (config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.50.254
   (config-ext-nacl)# permit ip 192.168.50.0 0.0.0.255 any
   (config-ext-nacl)# deny ip any any
   (config-ext-nacl)# exit
   (config)# interface vlan 50
   (config-if)# ip access-group 150 in layer3-forwarding
   (config-if)# exit
```

認証後 VLAN からは認証前 VLAN に対し、Web ブラウザからの通信だけ中継を許可するよう、アクセスリストを設定します。

(d) DHCP サーバの設定

[設定のポイント]

端末に IP アドレスを配布するための DHCP サーバを設定します。

[コマンドによる設定]

```
1. (config)# service dhcp vlan 10
   (config)# ip dhcp excluded-address 192.168.10.1
   (config)# ip dhcp excluded-address 192.168.10.254
   (config)# ip dhcp pool POOL10
   (dhcp-config)# network 192.168.10.0/24
   (dhcp-config)# lease 0 0 1
   (dhcp-config)# default-router 192.168.10.1
   (dhcp-config)# exit
```

DHCP サーバに認証前 VLAN 用の設定をします (端末認証に使用する IP アドレス配布を設定します。デフォルトルータの IP アドレス 192.168.10.1 を設定します。)

```
2. (config)# service dhcp vlan 50
   (config)# ip dhcp excluded-address 192.168.50.1
   (config)# ip dhcp excluded-address 192.168.50.254
   (config)# ip dhcp pool POOL50
   (dhcp-config)# network 192.168.50.0/24
   (dhcp-config)# lease 0 0 1
   (dhcp-config)# default-router 192.168.50.1
   (dhcp-config)# exit
```

DHCP サーバに認証後 VLAN 用の設定をします (認証された端末で使用する IP アドレスの配布を設定します。デフォルトルータの IP アドレス 192.168.50.1 を設定します。)

(e) Web 認証の設定

[設定のポイント]

Web 認証のコンフィグレーションコマンドを設定して Web 認証を有効にします。

[コマンドによる設定]

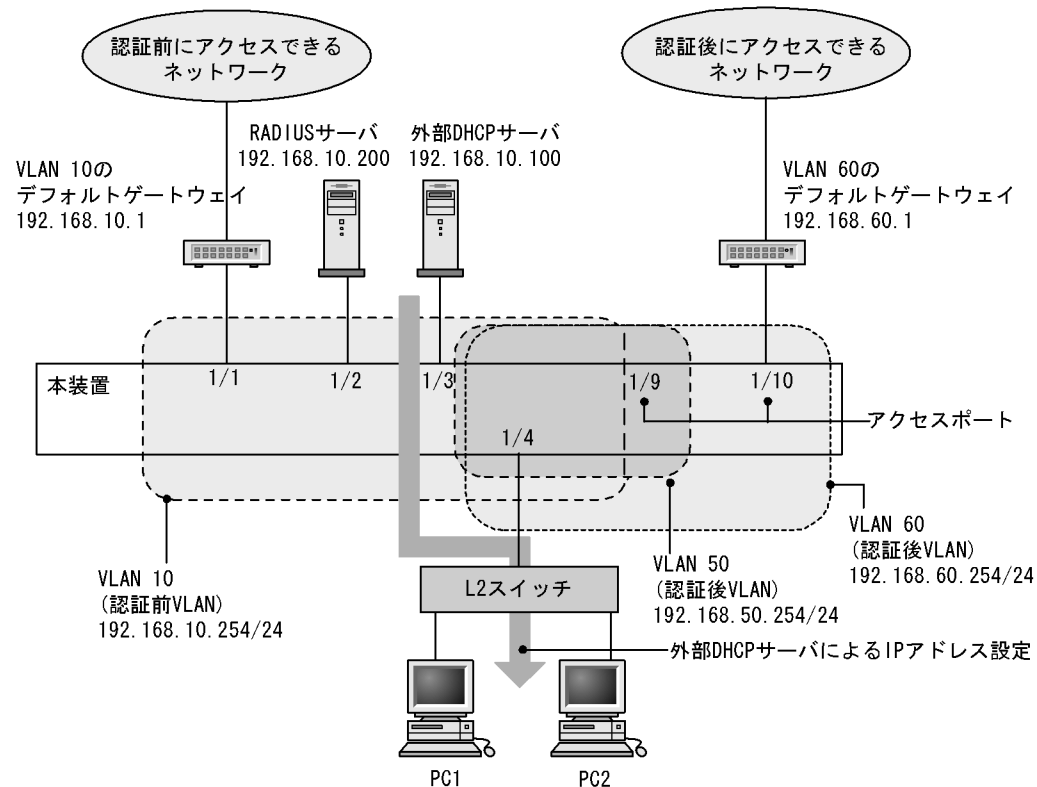
1. (config)# web-authentication vlan 50
Web 認証の認証後 VLAN を設定するコンフィグレーションコマンドで VLAN ID を設定します。
2. (config)# aaa authentication web-authentication default group radius
(config)# radius-server host 192.168.10.200 key "webauth"
ユーザ認証を RADIUS サーバで行うための IP アドレスと RADIUS 鍵を設定します。
3. (config)# web-authentication system-auth-control
Web 認証を起動します。

(4) RADIUS 認証方式 + 外部 DHCP サーバ + 複数の認証後 VLAN 使用時の構成

RADIUS 認証方式と外部 DHCP サーバを使用し、複数の認証後 VLAN を設定する場合の Web 認証設定

例を次の図に示します。なお、端末 (PC1, PC2) の IP アドレスは、外部 DHCP サーバによって割り当てられるものとします。

図 11-9 Web 認証の RADIUS 認証方式 + 外部 DHCP サーバ + 複数認証後 VLAN 使用時の構成例



認証前 VLAN と認証後 VLAN を設定し、アクセスリスト、DHCP サーバの設定をしたあとに、Web 認証の設定をします。また、認証前 VLAN からは認証後 VLAN に対して通信を許可しないよう、認証後 VLAN から認証前 VLAN に対して Web ブラウザとの通信だけを許可するアクセスリストを設定します。

また、認証後 VLAN 同士は通信を許可しないようにアクセスリストを設定します。

(a) 認証ポートの設定

[設定のポイント]

Web 認証で使用するポートを設定します。

[コマンドによる設定]

1.

```
(config)# interface gigabitethernet 1/4
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 50,60
(config-if)# switchport mac native vlan 10
(config-if)# exit
```

認証を行う端末が接続されているポートに認証前 VLAN と認証後 VLAN を指定します。

2.

```
(config)# interface gigabitethernet 1/9
(config-if)# switchport mode access
(config-if)# switchport access vlan 50
```

```
(config-if)# exit
```

認証後に接続するサーバを接続するポートに認証後 VLAN を指定します。

3. (config)# interface gigabitethernet 1/10

```
(config-if)# switchport mode access
```

```
(config-if)# switchport access vlan 60
```

```
(config-if)# exit
```

認証後に接続するサーバを接続するポートに認証後 VLAN を指定します。

(b) VLAN インタフェースに IP アドレスを設定

[設定のポイント]

認証前 VLAN および認証後 VLAN に IP アドレスを設定します。

[コマンドによる設定]

1. (config)# interface vlan 10

```
(config-if)# ip address 192.168.10.254 255.255.255.0
```

```
(config-if)# exit
```

```
(config)# interface vlan 50
```

```
(config-if)# ip address 192.168.50.254 255.255.255.0
```

```
(config-if)# exit
```

```
(config)# interface vlan 60
```

```
(config-if)# ip address 192.168.60.254 255.255.255.0
```

```
(config-if)# exit
```

認証前 VLAN と認証後 VLAN に各 IP アドレスを設定します。

(c) アクセスリストの設定

[設定のポイント]

認証後 VLAN と認証前 VLAN のアクセスリストを設定します。

[コマンドによる設定]

1. (config)# ip access-list extended 100

```
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 255.255.255.255 eq bootps
```

```
(config-ext-nacl)# permit ip 192.168.10.0 0.0.0.255 192.168.10.0 0.0.0.255
```

```
(config-ext-nacl)# deny ip any any
```

```
(config-ext-nacl)# exit
```

```
(config)# interface vlan 10
```

```
(config-if)# ip access-group 100 in layer3-forwarding
```

```
(config-if)# exit
```

認証前 VLAN からは認証後 VLAN に対して通信を許可しないよう、アクセスリストを設定します。

2. (config)# ip access-list extended 150

```
(config-ext-nacl)# permit tcp 192.168.50.0 0.0.0.255 host 192.168.10.254 eq http
```

```
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 255.255.255.255
```

```
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.10.254
```

```
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.50.254
(config-ext-nacl)# permit ip 192.168.50.0 0.0.0.255 any
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface vlan 50
(config-if)# ip access-group 150 in layer3-forwarding
(config-if)# exit
```

認証後 VLAN (VLAN ID 50) からは認証前 VLAN に対し、Web ブラウザからの通信だけ中継を許可し、他の認証後 VLAN (VLAN ID 60) への通信は許可しないよう、アクセスリストを設定します。

```
3. (config)# ip access-list extended 160
   (config-ext-nacl)# permit tcp 192.168.60.0 0.0.0.255 host 192.168.10.254 eq
   http
   (config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 255.255.255.255
   (config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.10.254
   (config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.60.254
   (config-ext-nacl)# permit ip 192.168.60.0 0.0.0.255 any
   (config-ext-nacl)# deny ip any any
   (config-ext-nacl)# exit
   (config)# interface vlan 60
   (config-if)# ip access-group 160 in layer3-forwarding
   (config-if)# exit
```

認証後 VLAN (VLAN ID 60) からは認証前 VLAN に対し、Web ブラウザからの通信だけ中継を許可し、他の認証後 VLAN (VLAN ID 50) への通信は許可しないよう、アクセスリストを設定します。

(d) DHCP リレーエージェントの設定

[設定のポイント]

端末に IP アドレスを配布するための DHCP リレーエージェントを設定します。

[コマンドによる設定]

```
1. (config)# interface vlan 10
   (config-if)# ip address 192.168.10.254 255.255.255.0
   (config-if)# ip helper-address 192.168.10.100
   (config-if)# exit
```

認証前 VLAN の DHCP リレーエージェントの設定をします。

```
2. (config)# interface vlan 50
   (config-if)# ip address 192.168.50.254 255.255.255.0
   (config-if)# ip helper-address 192.168.10.100
   (config-if)# exit
```

認証後 VLAN (VLAN ID 50) の DHCP リレーエージェントの設定をします。

```
3. (config)# interface vlan 60
   (config-if)# ip address 192.168.60.254 255.255.255.0
   (config-if)# ip helper-address 192.168.10.100
```

```
(config-if)# exit
```

認証後 VLAN (VLAN ID 60) の DHCP リレーエージェントの設定をします。

(e) Web 認証の設定

[設定のポイント]

Web 認証のコンフィグレーションコマンドを設定して Web 認証を有効にします。

[コマンドによる設定]

1. (config)# web-authentication vlan 50

```
(config)# web-authentication vlan 60
```

Web 認証の認証後 VLAN を設定するコンフィグレーションコマンドで VLAN ID を設定します。

2. (config)# aaa authentication web-authentication default group radius

```
(config)# radius-server host 192.168.10.200 key "webauth"
```

ユーザ認証を RADIUS サーバで行うための IP アドレスと RADIUS 鍵を設定します。

3. (config)# web-authentication system-auth-control

Web 認証を起動します。

11.1.5 Web 認証のパラメータ設定

Web 認証で可能なパラメータ設定を説明します。

(1) 認証最大時間の設定

[設定のポイント]

認証済みの端末を強制的にログアウトする時間を設定します。

[コマンドによる設定]

1. (config)# web-authentication max-timer 60

強制ログアウト時間を 60 分に設定します。

(2) 認証ユーザ数の設定 (固定 VLAN モード)

[設定のポイント]

Web 認証の固定 VLAN モードで認証できるユーザ数を設定します。

[コマンドによる設定]

1. (config)# web-authentication static-vlan max-user 100

Web 認証の固定 VLAN モードで認証できるユーザ数を 100 ユーザに設定します。

(3) 認証ユーザ数の設定 (ダイナミック VLAN モード, レガシーモード)

[設定のポイント]

Web 認証のダイナミック VLAN モードまたはレガシーモードで認証できるユーザ数を設定します。

[コマンドによる設定]

1. (config)# web-authentication max-user 5
Web 認証で認証できるユーザ数を 5 ユーザに設定します。

(4) RADIUS サーバの設定

[設定のポイント]

RADIUS 認証方式で使用する RADIUS サーバを設定します。

[コマンドによる設定]

1. (config)# aaa authentication web-authentication default group radius
RADIUS サーバでユーザ認証を行うように設定します。

[注意事項]

各 RADIUS サーバの radius-server コマンドで設定された応答待ち時間（再送回数 × 応答タイムアウト時間）の合計が 60 秒を超える場合、RADIUS サーバへ認証要求している途中で認証失敗となることがあります。なお、Web 認証で使用する radius-server コマンドの設定は、ログイン認証、コマンド承認、および IEEE802.1X でも共通して使用するため、応答待ち時間の設定には注意してください。

(5) アカウンティングの設定

[設定のポイント]

Web 認証のアカウンティング集計を行うよう設定します。

[コマンドによる設定]

1. (config)# aaa accounting web-authentication default start-stop group radius
RADIUS サーバにアカウンティング集計を行うよう設定します。

(6) Web 認証専用 IP アドレスの設定（固定 VLAN モード，ダイナミック VLAN モード）

[設定のポイント]

Web 認証専用の IP アドレスを設定します。

[コマンドによる設定]

1. (config)# web-authentication ip address 10.10.10.1
Web 認証専用の IP アドレス（10.10.10.1）を設定します。

[注意事項]

- 設定を行った場合は、運用コマンド restart web-authentication web-server で Web サーバを再起動してください。認証途中のユーザは再度ログイン操作が必要です。
- レガシーモードの状態（web-authentication port コマンドが設定されていない状態）で、本コマンドを設定したあとに web-authentication port コマンドを設定した場合は、運用コマンド restart web-authentication web-server で Web サーバを再起動してください。

(7) Web 認証専用 IP アドレスと FQDN の設定 (固定 VLAN モード, ダイナミック VLAN モード)

[設定のポイント]

Web 認証専用の IP アドレスと FQDN を設定します。

[コマンドによる設定]

1. (config)# **web-authentication ip address 10.10.10.1 fqdn host.example.com**
Web 認証専用の IP アドレス (10.10.10.1) と FQDN (host.example.com) を設定します。

[注意事項]

- 設定を行った場合は, 運用コマンド `restart web-authentication web-server` で Web サーバを再起動してください。認証途中のユーザは再度ログイン操作が必要です。
- レガシーモードの状態 (web-authentication port コマンドが設定されていない状態) で, 本コマンドを設定したあとに web-authentication port コマンドを設定した場合は, 運用コマンド `restart web-authentication web-server` で Web サーバを再起動してください。

(8) URL リダイレクト機能の設定 (ダイナミック VLAN モード)

[設定のポイント]

Web 認証の URL リダイレクト機能を設定します。

[コマンドによる設定]

1. (config)# **web-authentication redirect-vlan 10**
Web 認証の URL リダイレクト機能を有効にして, 認証前 VLAN として VLAN 10 を設定します。

[注意事項]

設定を行った場合は, 運用コマンド `restart web-authentication web-server` で Web サーバを再起動してください。認証途中のユーザは再度ログイン操作が必要です。

(9) URL リダイレクト機能時のログイン操作プロトコルの設定 (ダイナミック VLAN モード)

[設定のポイント]

Web 認証の URL リダイレクト機能時にログインを操作させるプロトコルを設定します。

[コマンドによる設定]

1. (config)# **web-authentication redirect-mode https**
Web 認証の URL リダイレクト機能で https を用います。

[注意事項]

設定を行った場合は, 運用コマンド `restart web-authentication web-server` で Web サーバを再起動してください。認証途中のユーザは再度ログイン操作が必要です。

(10) syslog サーバへの出力設定

[設定のポイント]

認証結果と動作ログを syslog サーバに出力する設定をします。

[コマンドによる設定]

1. (config)# web-authentication logging enable
(config)# logging event-kind aut
Web 認証の結果と動作ログを syslog サーバに出力する設定をします。

(11) 接続監視機能の設定 (固定 VLAN モード)

[設定のポイント]

認証済み端末の動作を監視する接続監視機能を設定します。

[コマンドによる設定]

1. (config)# web-authentication logout polling enable
接続監視機能を有効に設定します。
2. (config)# web-authentication logout polling interval 300
動作監視パケットの送出時間間隔を 300 秒に設定します。
3. (config)# web-authentication logout polling retry-interval 10
動作監視パケットの再送出時間間隔を 10 秒に設定します。
4. (config)# web-authentication logout polling count 5
動作監視パケットの送出回数を 5 回に設定します。

(12) 接続監視機能の無効設定 (固定 VLAN モード)

[設定のポイント]

認証済み端末の動作を監視する接続監視機能を無効に設定します。

[コマンドによる設定]

1. (config)# no web-authentication logout polling enable
接続監視機能を無効に設定します。

(13) Web サーバへのアクセスポート番号設定

[設定のポイント]

Web 認証で使用している Web サーバのサービスポート番号を設定します (デフォルトの http=80 番 , https=443 番以外に追加する場合に使用します)。

また , OAN と共存する場合は , OAN が使用するサービスポート番号 (832 と 9698) を設定します。この場合 , OAN が使用するサービスポート番号では Web 認証のログイン操作およびログアウト操作はできません。

[コマンドによる設定]

1. (config)# web-authentication web-port http 8080
Web サーバの http ポートとして 80 番のほかに 8080 番も設定します。
2. (config)# web-authentication web-port https 8443

Web サーバの https ポートとして 443 番のほかに 8443 番も設定します。

[注意事項]

設定を行った場合は、Web サーバを再起動してください。認証途中のユーザは再度ログイン操作が必要です。

(14) 認証成功後の URL 設定

[設定のポイント]

認証成功後に端末がアクセスする URL を設定します。

[コマンドによる設定]

1. (config)# web-authentication jump-url "http://www.example.com/"
認証成功後に http://www.example.com/ の画面を表示させます。

11.1.6 認証除外の設定方法

Web 認証で認証対象外とするための設定を説明します。

(1) 固定 VLAN モードの認証除外ポートの設定

固定 VLAN モードで、認証しないで通信を許可するポートを次のように設定します。

[設定のポイント]

認証を除外するポートに対しては、認証ポートを設定しません。

[コマンドによる設定]

1. (config)# vlan 10
(config-vlan)# state active
(config-vlan)# exit
(config)# interface gigabitethernet 1/4
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# web-authentication port
(config-if)# exit
(config)# interface gigabitethernet 1/10
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# exit

固定 VLAN モードで扱う VLAN ID 10 を設定したポート 1/4 は認証対象ポートとして設定します。また、ポート 1/10 には認証しないで通信を許可する設定をします。

(2) 固定 VLAN モードの認証除外端末の設定

固定 VLAN モードで、認証しないで通信を許可する端末の MAC アドレスを次のように設定します。

[設定のポイント]

認証を除外する端末の MAC アドレスを MAC アドレステーブルに登録します。

[コマンドによる設定]

1. `(config)# vlan 10`
`(config-vlan)# exit`
`(config)# mac-address-table static 0012.e212.3456 vlan 10 interface`
`gigabitethernet 1/10`
VLAN ID 10 のポート 1/10 に、認証しないで通信を許可する端末の MAC アドレスを設定します。

(3) ダイナミック VLAN モードの認証除外ポートの設定

ダイナミック VLAN モードで、認証しないで通信を許可するポートを次のように設定します。

[設定のポイント]

認証を除外するポートをアクセスポートとして設定し、認証対象ポートを設定しません。

[コマンドによる設定]

1. `(config)# vlan 50 mac-based`
`(config-vlan)# state active`
`(config-vlan)# exit`
`(config)# interface gigabitethernet 1/10`
`(config-if)# switchport mode access`
`(config-if)# switchport access vlan 50`
`(config-if)# exit`
MAC VLAN ID 50 のポート 1/10 に対して、認証しないで通信を許可する設定をします。

(4) ダイナミック VLAN モードの認証除外端末の設定

ダイナミック VLAN モードで、認証しないで通信を許可する端末の MAC アドレスを次のように設定します。

[設定のポイント]

認証を除外する端末の MAC アドレスを、MAC VLAN と MAC アドレステーブルに登録します。

[コマンドによる設定]

1. `(config)# vlan 50 mac-based`
`(config-vlan)# mac-address 0012.e212.3456`
`(config-vlan)# exit`
`(config)# mac-address-table static 0012.e212.3456 vlan 50 interface`
`gigabitethernet 1/10`
MAC VLAN ID 50 のポート 1/10 に、認証しないで通信を許可する端末の MAC アドレスを設定します。

(5) レガシーモードの認証除外ポートの設定

レガシーモードで、認証しないで通信を許可するポートを次のように設定します。

[設定のポイント]

認証を除外するポートをアクセスポートとして設定します。

[コマンドによる設定]

```
1. (config)# vlan 50 mac-based
   (config-vlan)# state active
   (config-vlan)# exit
   (config)# interface gigabitethernet 1/10
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 50
   (config-if)# exit
```

MAC VLAN ID 50 のポート 1/10 に対して、認証しないで通信を許可する設定をします。

(6) レガシーモードの認証除外端末の設定

レガシーモードで、認証しないで通信を許可する端末の MAC アドレスを次のように設定します。

[設定のポイント]

認証を除外する端末の MAC アドレスを、MAC VLAN に登録します。

[コマンドによる設定]

```
1. (config)# vlan 50 mac-based
   (config-vlan)# mac-address 0012.e212.3456
   (config-vlan)# exit
```

VLAN ID 50 の MAC VLAN に、認証しないで通信を許可する端末の MAC アドレスを設定します。

11.2 オペレーション

11.2.1 運用コマンド一覧

Web 認証の運用コマンド一覧を次の表に示します。

表 11-2 運用コマンド一覧

コマンド名	説明
set web-authentication user	Web 認証で使用するユーザ ID を追加します。
set web-authentication passwd	登録したユーザのパスワードを変更します。
set web-authentication vlan	登録したユーザの VLAN ID を変更します。
remove web-authentication user	登録したユーザ ID を削除します。
commit web-authentication	追加, 変更した内容を内蔵 Web 認証 DB に反映します。
store web-authentication	内蔵 Web 認証 DB のバックアップファイルを作成します。
load web-authentication	バックアップファイルから内蔵 Web 認証 DB を復元します。
show web-authentication user	内蔵 Web 認証 DB の登録内容, または追加, 変更途中の情報を表示します。
clear web-authentication auth-state	認証済みユーザの強制ログアウトを行います。
show web-authentication login	認証済のアカウントログを表示します。
show web-authentication	Web 認証のコンフィギュレーションを表示します。
show web-authentication statistics	Web 認証の統計情報を表示します。
clear web-authentication statistics	統計情報をクリアします。
show web-authentication logging	Web 認証の動作ログを表示します。
clear web-authentication logging	Web 認証の動作ログをクリアします。
set web-authentication html-files	指定された Web 認証画面ファイルを登録します。
clear web-authentication html-files	登録した Web 認証画面ファイルを削除します。
show web-authentication html-files	登録した Web 認証画面ファイルのファイル名, ファイルサイズと登録日時を表示します。
restart web-authentication	Web 認証プログラムを再起動します。
dump protocols web-authentication	Web 認証のダンプ情報を収集します。

11.2.2 Web 認証の設定情報表示

show web-authentication コマンドで Web 認証の設定情報が表示されます。

(1) 固定 VLAN モードで、認証方式が RADIUS 認証の場合

図 11-10 Web 認証の設定情報表示 (固定 VLAN モードの RADIUS 認証)

```
# show web-authentication
Date 2010/04/15 10:52:49 UTC
web-authentication Information:
  Authentic-mode      : Static-VLAN
  Authentic-method    : RADIUS           Accounting-state : disable
  Max-timer           : 60               Max-user        : 256
  VLAN Count         : -                 Auto-logout     : -
  Syslog-send         : enable
  Alive-detection     : enable
  timer               : 60               interval-timer  : 3       count : 3
  Jump-URL            : http://www.example.com/
  Web-IP-address      : 10.10.10.1
  FQDN                : aaa.example.com
  Web-port            : http  : 80, 8080   https : 443, 8443
  Access-list-No     : 100

      Port          : 1/1
      VLAN ID       : 5,10,15

      Port          : 1/2
      VLAN ID       : 15-16
```

(2) ダイナミック VLAN モードで、認証方式がローカル認証の場合

図 11-11 Web 認証の設定情報表示 (ダイナミック VLAN モードのローカル認証)

```
# show web-authentication
Date 2010/04/15 10:52:49 UTC
web-authentication Information:
  Authentic-mode      : Dynamic-VLAN
  Authentic-method    : Local           Accounting-state : disable
  Max-timer           : 60               Max-user        : 256
  VLAN Count         : -                 Auto-logout     : disable
  Syslog-send         : enable
  URL-redirect        : enable          Protocol        : http
  Jump-URL            : http://www.example.com/
  Web-IP-address      : 192.168.1.1
  FQDN                : aaa.example.com
  Web-port            : http  : 80, 8080   https : 443, 8443
  Redirect-vlan       : 10
  Access-list-No     : 100

      Port          : 1/10
      VLAN ID       : 1000,1500
      Native VLAN   : 10

      Port          : 1/12
      VLAN ID       : 1000,1500
      Native VLAN   : 10
```


(3) ダイナミック VLAN モードで、認証方式が RADIUS 認証の場合

図 11-12 Web 認証の設定情報表示 (ダイナミック VLAN モードの RADIUS 認証)

```
# show web-authentication
Date 2010/04/15 10:52:49 UTC
web-authentication Information:
  Authentic-mode       : Dynamic-VLAN
  Authentic-method    : RADIUS           Accounting-state : enable
  Max-timer           : 60               Max-user       : 256
  VLAN Count         : -                 Auto-logout    : disable
  Syslog-send        : enable
  URL-redirect       : enable           Protocol       : http
  Jump-URL           : http://www.example.com/
  Web-IP-address     : 192.168.1.1
  FQDN               : aaa.example.com
  Web-port           : http : 80, 8080   https : 443, 8443
  Redirect-vlan     : 10
  Access-list-No    : 100

      Port           : 1/10
      VLAN ID       : 1000,1500
      Native VLAN   : 10

      Port           : 1/12
      VLAN ID       : 1000,1500
      Native VLAN   : 10
```

(4) レガシーモードで VLAN が登録されていて、認証方式がローカル認証の場合

図 11-13 Web 認証の設定情報表示 (ローカル認証)

```
# show web-authentication
Date 2010/04/15 10:52:49 UTC
web-authentication Information:
  Authentic-mode       : Legacy
  Authentic-method    : Local           Accounting-state : disable
  Max-timer           : 60               Max-user       : 256
  VLAN Count         : 16                 Auto-logout    : disable
  Syslog-send        : enable
  Jump-URL           : http://www.example.com/
  Web-port           : http : 80         https : 443

VLAN Information:
  VLAN ID : 5,10,15,20,25,30,35,40,1000-1007
```

(5) レガシーモードで VLAN が登録されていて、認証方式が RADIUS 認証の場合

図 11-14 Web 認証の設定情報表示 (RADIUS 認証)

```
# show web-authentication
Date 2010/04/15 10:52:49 UTC
web-authentication Information:
  Authentic-mode       : Legacy
  Authentic-method    : RADIUS           Accounting-state : disable
  Max-timer           : 60               Max-user       : 256
  VLAN Count         : 16                 Auto-logout    : disable
  Syslog-send        : enable
  Jump-URL           : http://www.example.com/
  Web-port           : http : 80         https : 443

VLAN Information:
  VLAN ID : 5,10,15,20,25,30,35,40,1000-1007
```

11.2.3 Web 認証の状態表示

show web-authentication statistics コマンドで Web 認証の状態および RADIUS との通信状況が表示され

ます。

図 11-15 Web 認証の表示

```
# show web-authentication statistics
Date 2006/08/12 11:10:49 UTC
web-authentication Information:
  Authentication Request Total :      100
  Authentication Current Count :       10
  Authentication Error Total   :       30
RADIUS web-authentication Information:
[RADIUS frames]
  TxTotal   :      10 TxAccReq :      10 TxError   :      0
  RxTotal   :      30 RxAccAccpt:     10 RxAccRejct:    10
                RxAccChllg:     10 RxInvalid :      0
Account web-authentication Information:
[Account frames]
  TxTotal   :      10 TxAccReq :      10 TxError   :      0
  RxTotal   :      20 RxAccResp :     10 RxInvalid :      0
```

11.2.4 Web 認証の認証状態表示

show web-authentication login コマンドで Web 認証の認証状態が表示されます。

(1) 固定 VLAN モードの場合

図 11-16 Web 認証の認証状態表示 (固定 VLAN モード)

```
# show web-authentication login
Date 2010/04/15 10:52:49 UTC
Total user counts:2
Username
VLAN   MAC address      Port  IP address
Login time      Limit time
USER00123456789
  3     0012.e200.9166   1/5   192.168.0.1
2010/04/15 09:58:04 UTC 00:10:20
USER01
4094   0012.e268.7527   1/6   192.168.1.10
2010/04/15 10:10:23 UTC 00:20:35
```

(2) ダイナミック VLAN モードの場合

図 11-17 Web 認証の認証状態表示 (ダイナミック VLAN モード)

```
# show web-authentication login
Date 2010/04/15 10:52:49 UTC
Total user counts:2
Username
VLAN   MAC address      Login time      Limit time
USER00123456789
  3     0012.e200.9166   2010/04/15 09:58:04 UTC 00:10:20
USER01
4094   0012.e268.7527   2010/04/15 10:10:23 UTC 00:20:35
```

(3) レガシーモードの場合

図 11-18 Web 認証の認証状態表示 (レガシーモード)

```
# show web-authentication login
Date 2010/04/15 10:52:49 UTC
Total user counts:2
Username
VLAN    MAC address      Login time          Limit time
USER00123456789
   3     0012.e200.9166   2010/04/15 09:58:04 UTC  00:10:20
USER01
4094    0012.e268.7527   2010/04/15 10:10:23 UTC  00:20:35
```

11.2.5 内蔵 Web 認証 DB の作成

Web 認証システムの環境設定およびコンフィギュレーションの設定が完了したあとに、内蔵 Web 認証 DB の作成を行います。また、すでに内蔵 Web 認証 DB に登録されているユーザ情報の修正を行います。

(1) ユーザの登録

認証対象のユーザごとに `set web-authentication user` コマンドで、ユーザ ID、パスワード、VLAN ID を登録します。次の例では、USER01 ~ USER05 の 5 ユーザ分を登録します。

[コマンド入力]

```
# set web-authentication user USER01 PAS0101 100
# set web-authentication user USER02 PAS0200 100
# set web-authentication user USER03 PAS0300 100
# set web-authentication user USER04 PAS0320 100
# set web-authentication user USER05 PAS0400 100
```

(2) ユーザ情報変更と削除

登録済みユーザのパスワード、VLAN ID の変更およびユーザの削除は次の手順で行います。

(a) パスワード変更

[コマンド入力]

```
# set web-authentication passwd USER01 PAS0101 PPP4321
```

ユーザ ID (USER01) のパスワードを PAS0101 から PPP4321 に変更します。

```
# set web-authentication passwd USER02 PAS0200 BBB1234
```

ユーザ ID (USER02) のパスワードを PAS0200 から BBB1234 に変更します。

(b) VLAN ID 変更

[コマンド入力]

```
# set web-authentication vlan BBB1234 200
```

ユーザ ID (BBB1234) の VLAN ID を 200 に変更します。

(c) ユーザ削除

[コマンド入力]

```
# remove web-authentication user PPP4321
```

ユーザ ID (P P P P 4 3 2 1) を削除します。

(3) 内蔵 Web 認証 DB への反映

set web-authentication コマンドおよび remove web-authentication コマンドで登録・変更したユーザ情報を内蔵 Web 認証 DB に反映します。

[コマンド入力]

```
# commit web-authentication
```

11.2.6 内蔵 Web 認証 DB のバックアップ

内蔵 Web 認証 DB のバックアップおよびバックアップファイルからの復元を示します。

(1) 内蔵 Web 認証 DB のバックアップ

内蔵 Web 認証 DB から運用コマンド store web-authentication でバックアップファイル (次の例では backupfile) を作成します。

[コマンド入力]

```
# store web-authentication backupfile
Backup web-authentication user data. Are you sure? (y/n): y
#
```

(2) 内蔵 Web 認証 DB の復元

バックアップファイル (次の例では backupfile) から運用コマンド load web-authentication で内蔵 Web 認証 DB を作成します。

[コマンド入力]

```
# load web-authentication backupfile
Restore web-authentication user data. Are you sure? (y/n): y
#
```

11.2.7 Web 認証画面の登録

Web 認証画面の登録は次の手順で行います。

1. 各 Web 認証画面のファイルを外部装置 (PC など) で作成します。
2. 本装置へログインし、カレントディレクトリに Web 認証画面を格納するディレクトリを作成します。
3. 画面ファイルを 2. で作成したディレクトリ配下に、ファイル転送または MC 経由で格納します。
4. set web-authentication html-files コマンドで Web 認証画面を登録します。

図 11-19 Web 認証画面の登録

```
# mkdir docs ...1
# set web-authentication html-files docs
Would you wish to install new html-files ? (y/n):y
executing...
Install complete.
#
```

1. ディレクトリ docs を作成し、配下に、登録するファイルを置きます。

11.2.8 登録した Web 認証画面の削除

set web-authentication html-files コマンドで登録した Web 認証画面を clear web-authentication html-files コマンドで削除します。

図 11-20 Web 認証画面の削除

```
# clear web-authentication html-files
Would you wish to clear registered html-files and initialize? (y/n):y
Clear complete.
#
```

11.2.9 Web 認証画面の情報表示

show web-authentication html-files コマンドで、登録した Web 認証画面の情報を表示します。

図 11-21 Web 認証画面の情報表示

```
# show web-authentication html-files
Date 2007/04/01 10:07:04 UTC
TOTAL SIZE      :      60974
-----
                SIZE      DATE
login.html      :      2049    2007/03/30 14:05
loginOK.html    :      1046    2007/03/30 14:05
loginNG.html    :       985    2007/03/30 14:05
logout.html     :       843    2007/03/30 14:05
logoutOK.html   :       856    2007/03/30 14:05
logoutNG.html   :       892    2007/03/30 14:05
webauth.msg     :       104    2007/03/30 14:05
favicon.ico     :       199    2007/03/30 14:05
the other files :     54000    2007/03/30 14:05
#
```

11.3 Web 認証画面作成手引き

Web 認証画面入れ替え機能で入れ替えができる画面と対応するファイル名を次に示します。

- ログイン画面 (ファイル名: login.html)
- ログアウト画面 (ファイル名: logout.html)
- ログイン成功画面 (ファイル名: loginOK.html)
- ログイン失敗画面 (ファイル名: loginNG.html)
- ログアウト完了画面 (ファイル名: logoutOK.html)
- ログアウト失敗画面 (ファイル名: logoutNG.html)

各 Web 認証画面ファイルは HTML 形式で作成してください。

HTML 上には, JavaScript のようにクライアント端末上だけで動作する言語は使用可能ですが, サーバへアクセスするような言語は使用できません。また, perl などの CGI も指定しないでください。

ただし, ログイン画面, ログアウト画面では, Web 認証とのインタフェース用の記述が必要です。ログイン画面, ログアウト画面については, 「11.3.1 ログイン画面 (login.html)」, 「11.3.2 ログアウト画面 (logout.html)」を参照してください。

また, 「表 10-6 認証エラーメッセージとエラー発生理由対応表」に示した認証エラーメッセージも置き換えることができます。使用できるファイル名は次のとおりです。ファイルの作成方法については, 「11.3.3 認証エラーメッセージファイル (webauth.msg)」を参照してください。

- 認証エラーメッセージ (ファイル名: webauth.msg)

さらに, Web ブラウザのお気に入りに表示するアイコンも入れ替えることができます。

- Web ブラウザのお気に入りに表示するアイコン (ファイル名: favicon.ico)

注意

入れ替え可能な画面および認証エラーメッセージのファイル名は, 必ず上記に示したファイル名と一致させてください。

11.3.1 ログイン画面 (login.html)

Web 認証にログインする際, ユーザ ID とパスワードの入力をクライアントに対し要求する画面です。

(1) 設定条件

ログイン画面の HTML ファイルを作成する際は, 次の表に示す記述を必ず入れてください。

表 11-3 ログイン画面に必要な設定

記述内容	意味
<code><form name="Login" method="post" action="/cgi-bin/Login.cgi"></form></code>	ログイン操作を Web 認証に指示するための記述です。この記述は変更しないでください。
<code><input type="text" name="uid" size="40" maxlength="32" autocomplete="OFF" /></code>	ユーザ ID を指定するための記述です。size と maxlength 以外の記述は変更しないでください。上記 <code><form></form></code> の内部に設定してください。また, maxlength は必ず 6 以上の数字を設定してください。

記述内容	意味
<code><input type="password" name="pwd" size="40" maxlength="32" autocomplete="OFF" /></code>	パスワードを指定するための記述です。size と maxlength 以外の記述は変更しないでください。上記 <code><form></form></code> の内部に設定してください。また、maxlength は必ず 6 以上の数字を設定してください。
<code><input type="submit" value="Login" /></code>	Web 認証にログイン要求を行うために記述です。この記述は変更しないでください。上記 <code><form></form></code> の内部に設定してください。

注意

login.html ファイルに、ほかのファイルに関連付ける場合は、関連付けするファイル名の先頭に `"/` (スラッシュ) を記述してください。
 (例) ``

(2) 設定例

ログイン画面 (login.html) のソース例を次の図に示します。

図 11-22 ログイン画面 (login.html) のソース例

```

<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
<title>&nbsp;&nbsp;&nbsp;</title>
</head>
<body>
<!-- ===== Body ===== -->
<center>
<br />
<table width="100%">
<tr><td align="center" bgcolor="#2b1872">
<font color="#ffffff"><b>LOGIN</b></font>
</td></tr></table>
<br />
Please enter your ID and password.<br />
<br />
<form name="Login" method="post" action="/cgi-bin/Login.cgi">
<table><tr>
<td>user ID</td>
<td><input type="text" name="uid" size="40" maxlength="32" autocomplete="OFF" /></td>
</tr><tr>
<td>password</td>
<td><input type="password" name="pwd" size="40" maxlength="32"
autocomplete="OFF" /></td>
</tr></table>
<br />
<input type="submit" value="Login" />
</form>
<br /><br /><br /><br /><br />
</center>
<!-- ===== Footer ===== -->
<hr>
</body>
</html>

```

ログイン操作をWeb認証に指示するための記述

ユーザID指定のための記述

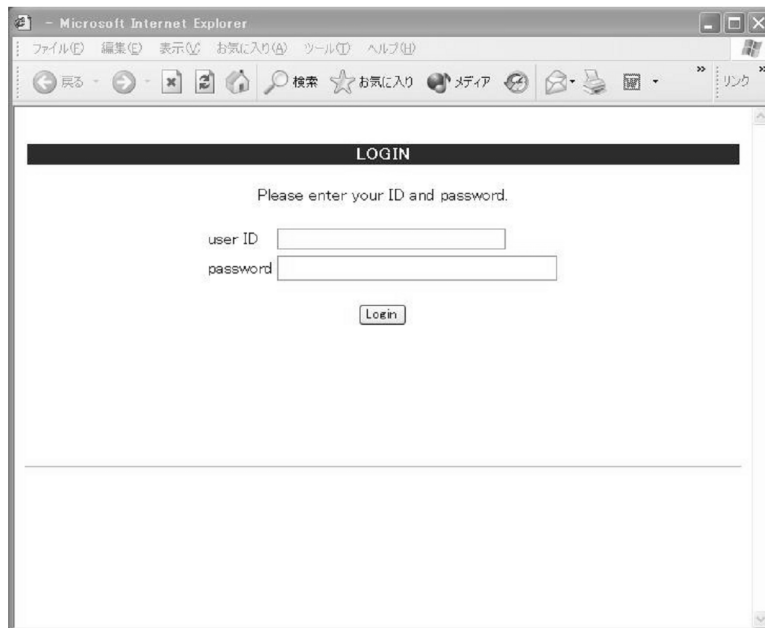
パスワード指定のための記述

Web認証にログイン要求を行うための記述

(3) ログイン画面表示例

ログイン画面の表示例を次の図に示します。

図 11-23 ログイン画面の表示例



11.3.2 ログアウト画面 (logout.html)

Web 認証機能でログインしているクライアントがログアウトを要求するための画面です。

(1) 設定条件

ログアウト画面の HTML ファイルを作成する際は、次の表に示す記述を必ず入れてください。

表 11-4 ログアウト画面に必要な設定

記述内容	意味
<code><form name="Logout" method="post" action="/cgi-bin/Logout.cgi"></form></code>	ログアウト操作を Web 認証に指示するための記述です。この記述は変更しないでください。
<code><input type="submit" value="Logout" /></code>	Web 認証にログアウト要求を行うために記述です。この記述は変更しないでください。上記 <code><form></form></code> の内部に設定してください。

注意

logout.html ファイルに、ほかのファイルを関連付ける場合は、関連付けするファイル名の先頭に "/" (スラッシュ) を記述してください。
(例) ``

(2) 設定例

ログアウト画面 (logout.html) のソース例を次の図に示します。

図 11-24 ログアウト画面 (logout.html) のソース例

```

<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
<title>&nbsp;</title>
</head>
<body>
<!-- ===== Body ===== -->
<center>
<br />
<form name="Logout" method="post" action="/cgi-bin/Logout.cgi">
<table width="100%">
<tr><td align="center" bgcolor="#2b1872">
<font color="#ffffff"><b>LOGOUT</b></font>
</td></tr></table>
<br />
Please push the following button.<br />
<br />
<input type="submit" value="Logout" />
</form>
<br /><br /><br /><br /><br /><br />
</center>
<!-- ===== Footer ===== -->
<br>
</body>
</html>

```

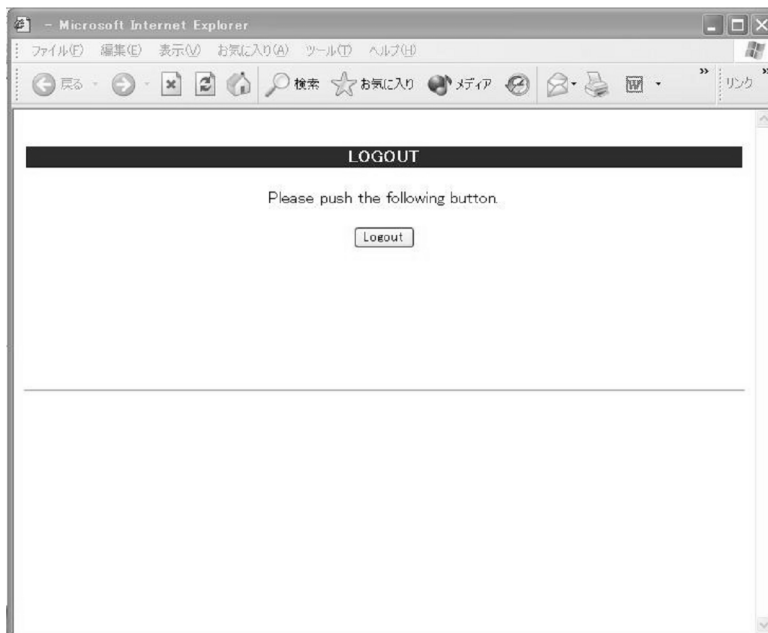
ログアウト操作をWeb認証に指示するための記述

Web認証にログアウト要求を行うための記述

(3) ログアウト画面表示例

ログアウト画面の表示例を次の図に示します。

図 11-25 ログアウト画面の表示例



11.3.3 認証エラーメッセージファイル (webauth.msg)

認証エラーメッセージファイル (webauth.msg) は、Web 認証ログインまたは Web 認証ログアウトの失敗時に応答画面で表示するメッセージ群を格納したファイルです。

デフォルト設定の認証エラーメッセージを入れ替える際は、次の表に示す 9 行のメッセージを格納した認証エラーメッセージファイルを作成してください。

表 11-5 認証エラーメッセージファイルの各行の内容

行番号	内容
1 行目	ログイン時、ユーザ ID またはパスワード記述を誤った場合、もしくは Web 認証 DB による認証エラーとなった場合に出力するメッセージ。 [デフォルトメッセージ] " User ID or password is wrong. Please enter correct user ID and password. "
2 行目	Radius による認証エラーとなった場合に出力するメッセージ。 [デフォルトメッセージ] " RADIUS: Authentication reject. "
3 行目	コンフィグレーション上、Radius 認証の設定となっているが、Radius サーバと本装置との接続が確立していない場合に出力するメッセージ。 [デフォルトメッセージ] " RADIUS: No authentication response. "
4 行目	本装置のコンフィグレーションの設定誤り、または他機能との競合のためにログインできない場合に出力するメッセージ。 [デフォルトメッセージ] " You cannot login by this machine. "
5 行目	プログラムの軽度の障害が発生した場合に出力するメッセージ。 [デフォルトメッセージ] " Sorry, you cannot login just now. Please try again after a while. "
6 行目	プログラムの中度の障害が発生した場合に出力するメッセージ。 [デフォルトメッセージ] " The system error occurred. Please contact the system administrator. "
7 行目	プログラムの重度の障害が発生した場合に出力するメッセージ。 [デフォルトメッセージ] " A fatal error occurred. Please inform the system administrator. "
8 行目	ログアウト処理で CPU 高負荷などによって、ログアウトが失敗した場合に出力するメッセージ。 [デフォルトメッセージ] " Sorry, you cannot logout just now. Please try again after a while. "
9 行目	ログインしていないユーザがログアウトした場合に出力するメッセージ。 [デフォルトメッセージ] " The client PC is not authenticated. "

(1) 設定条件

- 改行だけの行があった場合は、デフォルトのエラーメッセージを表示します。
- ファイル保存時は、改行コードを " CR+LF " または " LF " のどちらからで保存してください。
- 1 行に書き込めるメッセージ長は、半角 512 文字 (全角 256 文字) までです。ここで示している文字数には html タグ、改行タグ "
 " も含まれます。なお、半角 512 文字を超えた文字については無視します。
- 認証エラーメッセージファイルが 10 行以上あった場合は、10 行目以降の内容は無視します。

(2) 認証エラーメッセージファイル作成のポイント

- 認証エラーメッセージファイル上に記述したテキストは、そのまま HTML テキストとして使用します。したがって、認証エラーメッセージ上に HTML のタグを記述すると、そのタグの動作を行います。

- 1メッセージは1行で記述する必要があるため、エラーメッセージの表示イメージに改行を入れたい場合は、改行したい個所に HTML の改行タグ "
 " を挿入してください。

(3) 設定例

認証エラーメッセージファイル (webauth.msg) のソース例を次の図に示します。

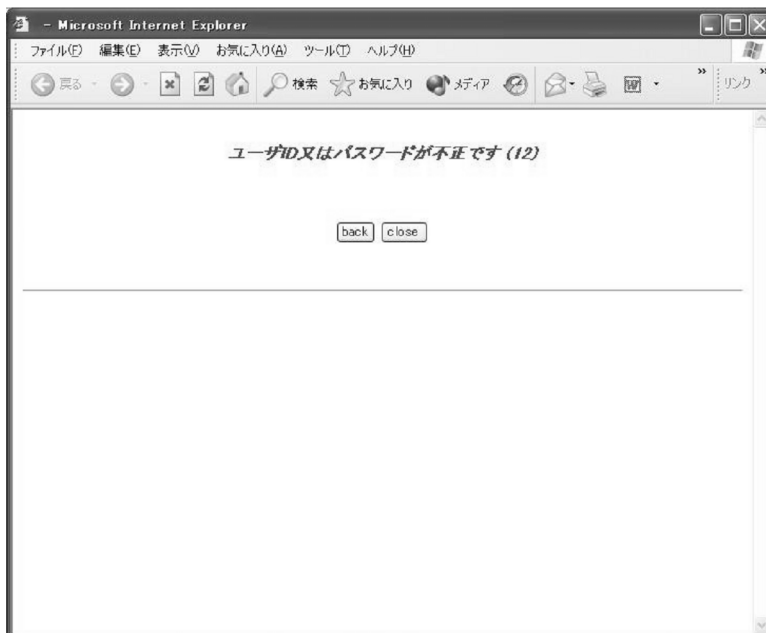
図 11-26 認証エラーメッセージファイル (webauth.msg) のソース例

```
ユーザID又はパスワードが不正です  
パスワードが不正です  
認証サーバが見つかりません<BR>システム管理者にお問い合わせください。  
システムの設定に誤りがあります<BR>システム管理者にお問い合わせください。  
システム障害発生 (minor) <BR>しばらくしてから再度ログインをしてください。  
システム障害発生 (major) <BR>システム管理者にお問い合わせください。  
システム障害発生 (critical) <BR>システム管理者にお問い合わせください。  
システムが高負荷状態です<BR>しばらくしてからログアウトしてください。  
ログインしていません
```

(4) 表示例

上記の認証エラーメッセージファイルを使用し、パスワード長不正により、ログインに失敗したときのログイン失敗画面の表示例を次の図に示します。

図 11-27 ログイン失敗画面の表示例 (パスワード長不正)



11.3.4 Web 認証固有タグ

Web 認証画面の HTML ファイルに Web 認証固有タグを書き込むことで、認証画面上にログイン時刻やエラーメッセージを表示できます。

設定可能な画面と Web 認証固有タグの組み合わせを次の表に示します。

表 11-6 特殊タグ一覧

タグ表記	画面に表示 する内容	ログイン 画面	ログアウト 画面	ログイン 成功画面	ログイン 失敗画面	ログアウト 完了画 面	ログアウト 失敗画 面
<!-- Login_Time -->	ログイン時刻 ¹	-	-		-	-	-
<!-- Logout_Time -->	ログアウト時刻 ²	-	-		-		-
<!-- After_Vlan -->	認証後 VLAN ID ³	-	-		-	-	-
<!-- Error_Message -->	エラーメッ セージ ⁴	-	-	-		-	
<!-- Redirect_URL -->	なし	-	-	- ⁵	-	-	-

(凡例) : 画面上に表示する。 - : 画面上空欄となる。

注 1 ログインが成功した時刻。

注 2 表示画面によって意味が異なります。

ログイン成功画面：自動ログアウトする時刻。

ログアウト完了画面：ログアウト動作が完了した時刻。

注 3 ログイン成功後、ユーザが通信を行う VLAN ID。

注 4 ログインまたはログアウトが失敗した場合のエラー要因。

注 5 画面上に表示しませんが、認証成功後のジャンプ先 URL を保持します。

設定例については、「11.3.5 その他の画面サンプル」を参照してください。

11.3.5 その他の画面サンプル

Web 認証画面 (loginOK.html, logoutOK.html, loginNG.html, logoutNG.html) のサンプルソースを示します。

(1) ログイン成功画面 (loginOK.html)

ログイン成功画面のソース例および表示例を次の図に示します。

図 11-28 ログイン成功画面のソース例 (loginOK.html)

```

<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
<title>&nbsp;&nbsp;&nbsp;</title>
</head>
<body oncontextmenu="return false;">
<!-- ===== Body ===== -->
<center>
Login success
<br /><br />
<Table Border="0">
<Tr>
<Td Align="left">
Login Time
</Td>
<Td Align="left">
---
</Td>
<Td Align="left">
<b><!-- Login_Time --></b> ログイン時刻表示タグ
</Td>
</Tr>
<Tr>
<Td Align="left">
Logout Time
</Td>
<Td Align="left">
---
</Td>
<Td Align="left">
<b><!-- Logout_Time --></b> ログアウト時刻表示タグ
</Td>
</Tr>
</Table>
<b><!-- Redirect_URL --></b> 認証成功後のジャンプ先URLタグ
<br /><br />

<form>
<input type="button" value="close" onClick="window.close()" />
</form>
<br /><br />
</center>
<br /><br />
<!-- ===== Footer ===== -->
<hr>
</body>
</html>

```

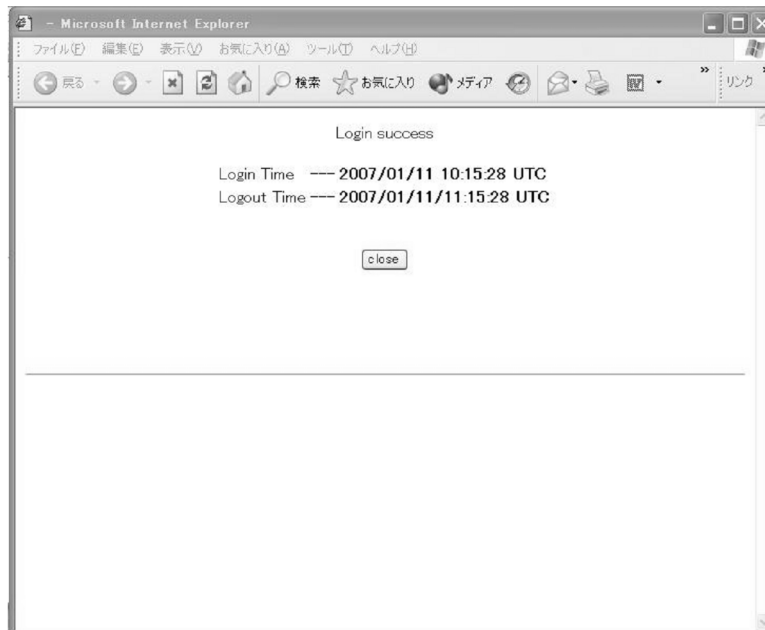
注意

loginOK.html ファイルに、ほかのファイルに関連付ける場合は、関連付けするファイル名の先頭に ” / ” (スラッシュ) を記述してください。

(例)

なお、ダイナミック VLAN モードまたはレガシーモードでは、loginOK.html ファイルにほかのファイルに関連付けると、ログイン成功画面が正常に表示されないことがあります。

図 11-29 ログイン成功画面の表示例



(2) ログアウト完了画面 (logoutOK.html)

ログアウト完了画面のソース例および表示例を次の図に示します。

図 11-30 ログアウト完了画面のソース例 (logoutOK.html)

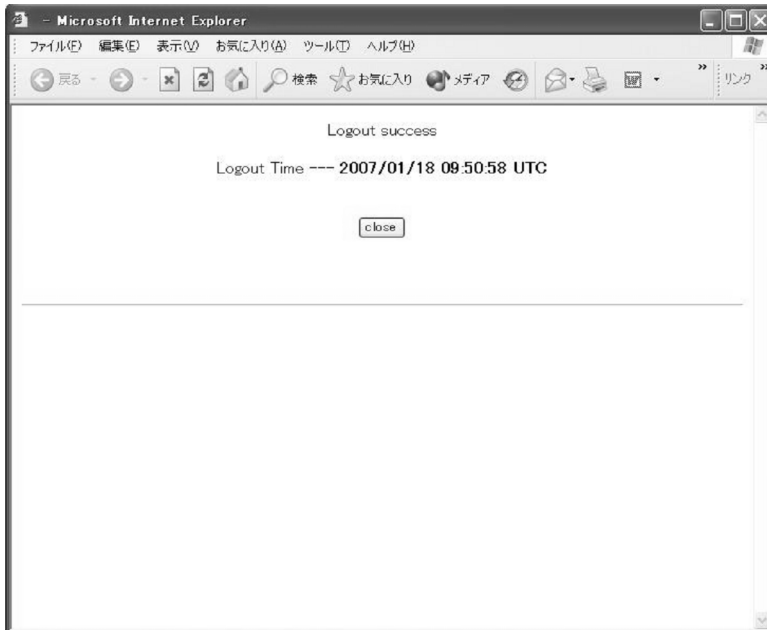
```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
<title>&nbsp;</title>
</head>
<body oncontextmenu="return false;">
<!-- ===== Body ===== -->
<center>
Logout success
<br /><br />
Logout Time --- <b>!-- Logout Time --> ログアウト時刻表示タグ
<br /><br /><br />
<form>
<input type="button" value="close" onClick="window.close()" />
</form>
<br /><br />
</center>
<!-- ===== Footer ===== -->
<hr>
</body>
</html>
```

注意

logoutOK.html ファイルに、ほかのファイルに関連付ける場合は、関連付けるファイル名の先頭に "/" (スラッシュ) を記述してください。

(例)

図 11-31 ログアウト完了画面の表示例



(3) ログイン / ログアウト失敗画面 (loginNG.html / logoutNG.html)

ログイン / ログアウト失敗画面のソース例および表示例を次の図に示します。

図 11-32 ログイン / ログアウト失敗画面のソース例 (loginNG.html / logoutNG.html)

```

<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
<title>&nbsp;</title>
</head>
<body oncontextmenu="return false;">
<!-- ===== Body ===== -->
<center>
<br>
<i style="color:red"><b><!-- Error Message --></b></i>
<br /><br /><br /><br />
<form>
<input type="button" value="back" onClick="history.back()" />
<input type="button" value="close" onClick="window.close()" />
</form>
<br />
</center>
<!-- ===== Footer ===== -->
<hr>
</body>
</html>

```

エラーメッセージ表示タグ
↓

注意

loginNG.html , logoutNG.html ファイルに、ほかのファイルに関連付ける場合は、関連付けるファイル名の先頭に "/" (スラッシュ) を記述してください。

(例)

図 11-33 ログイン/ログアウト失敗画面の表示例



12 MAC 認証の解説

MAC 認証は、受信したフレームの送信元 MAC アドレスを認証し、VLAN へのアクセス制御を行う機能です。この章では MAC 認証について解説します。

12.1 概要

12.2 システム構成例

12.3 認証機能

12.4 内蔵 MAC 認証 DB および RADIUS サーバの準備

12.5 MAC 認証使用時の注意事項

12.1 概要

ユーザ ID、パスワードを入力できる PC のような機器では IEEE802.1X や Web 認証を利用できますが、MAC 認証はユーザ ID、パスワードを入力できないプリンタなどの機器でも認証を行うための機能です。

指定されたポートに受信するフレームの送信元 MAC アドレスで認証し、認証された MAC アドレスを持つフレームだけが通信を許可されます。

なお、DHCP snooping が設定された場合、MAC 認証の対象となる端末から送信された ARP パケットと DHCP パケットは、MAC 認証と DHCP snooping の両方の対象になります。

(1) 認証モード

本装置は次に示す認証モードをサポートしています。

- 固定 VLAN モード
認証が成功した端末の MAC アドレスを MAC アドレステーブルに登録して、VLAN へ通信できるようにします。
- ダイナミック VLAN モード
認証が成功したあと、MAC アドレスを MAC VLAN に登録して、認証前のネットワークと認証後のネットワークを分離します。

ダイナミック VLAN モードの記述で、認証前の端末が所属する VLAN を認証前 VLAN と呼びます。また、認証後の VLAN を認証後 VLAN と呼びます。

(2) 認証方式

本装置は、固定 VLAN モード、ダイナミック VLAN モードのどちらの認証モードでも、次に示すローカル認証方式または RADIUS 認証方式のどちらかの方式を選択できます。

- ローカル認証方式
本装置に内蔵した認証用 DB (内蔵 MAC 認証 DB と呼びます) に MAC アドレスを登録しておき、受信したフレームの MAC アドレスとの一致を確認して認証する方式です。ネットワーク内に RADIUS サーバを置かない小規模ネットワークに適しています。
- RADIUS 認証方式
ネットワーク内に設置した RADIUS サーバを用いて認証する方式です。比較的規模の大きなネットワークに適しています。

12.2 システム構成例

12.2.1 固定 VLAN モード

認証対象端末が認証前のときは、MAC アドレステーブルに登録されず、接続された VLAN 内へ通信できない状態です。認証が成功すると、端末の MAC アドレスを MAC アドレステーブルに登録し、VLAN 内へ通信できるようになります。

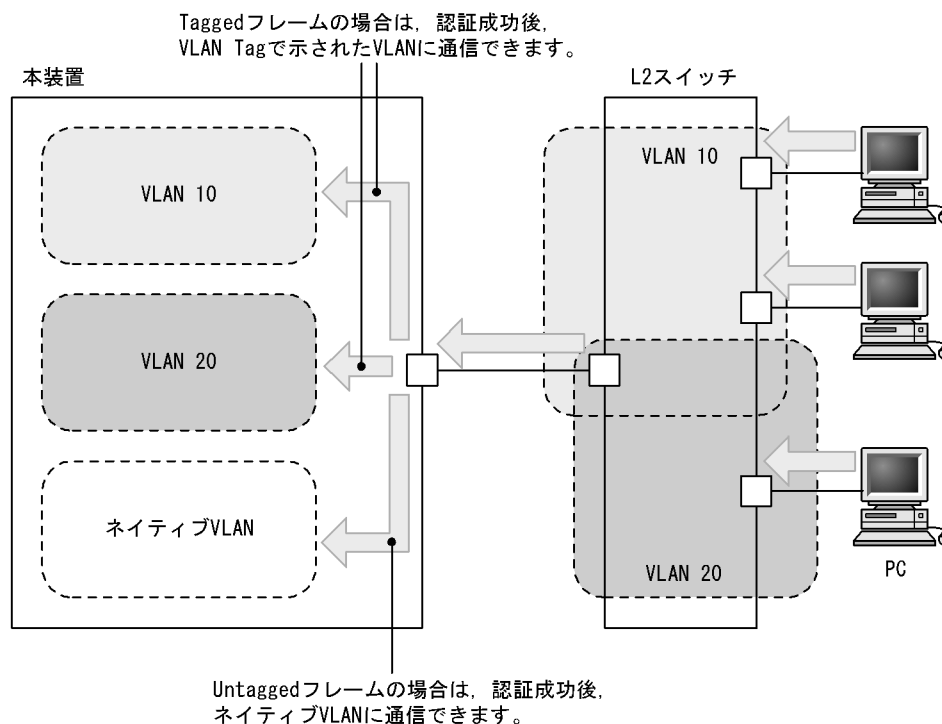
本装置では、認証ポートとして次のポートを設定できます。

- アクセスポート
- トランクポート

なお、トランクポートに入ってきた Tagged フレームおよび Untagged フレームの扱いは次のようになります。

- 認証時のフレームが Tagged フレームの場合、認証成功後、VLAN Tag で示された VLAN に通信できます。
- 認証時のフレームが Untagged フレームの場合、認証成功後、ネイティブ VLAN に通信できます。

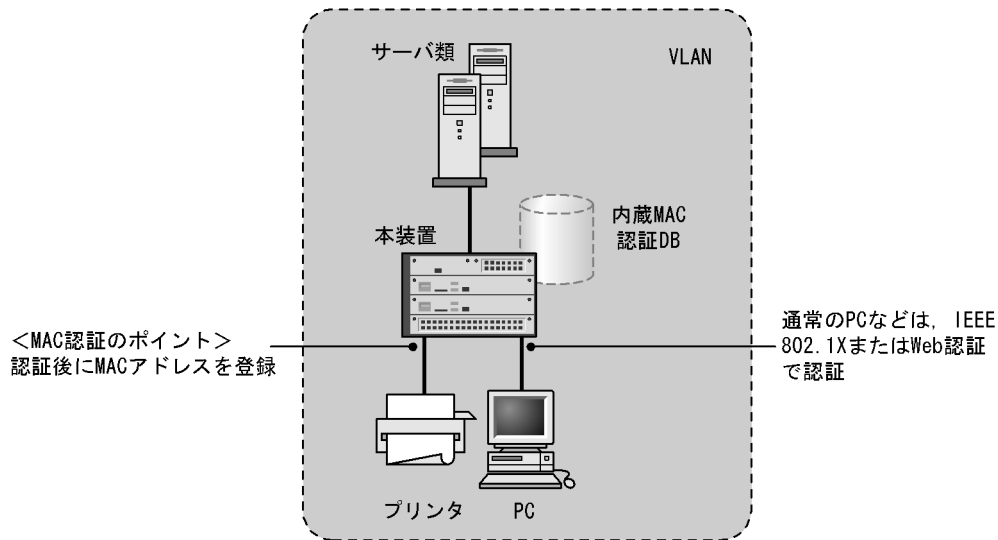
図 12-1 Tagged フレームおよび Untagged フレームの扱い



(1) ローカル認証方式

ローカル認証方式は、MAC 認証の対象となるポートで受信したフレームの送信元 MAC アドレスと、内蔵 MAC 認証 DB に登録されている MAC アドレスとを照合し、一致していれば認証成功として通信を許可する方式です。

図 12-2 固定 VLAN モードのローカル認証方式の構成



なお、ローカル認証方式には、MAC アドレスだけで照合する方法と、MAC アドレスと VLAN ID との組み合わせで照合する方法があります。これらの方法は、コンフィグレーションコマンド `mac-authentication vlan-check` で選択できます。

MAC アドレスと VLAN ID による照合時の設定条件を次の表に示します。

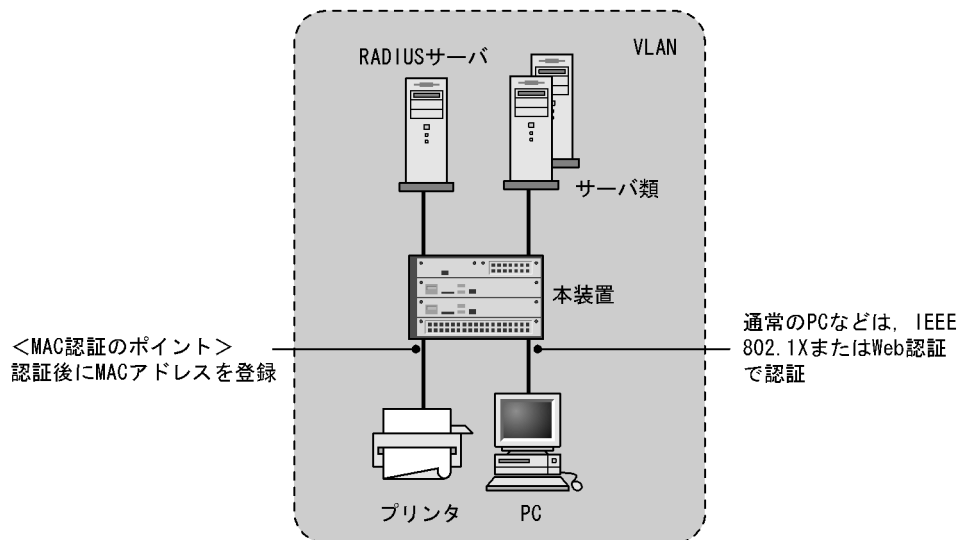
表 12-1 固定 VLAN モードのローカル認証方式の VLAN ID 照合

コンフィグレーション コマンド設定	内蔵 MAC 認証 DB の VLAN ID 設定	
	有り	無し
有り	MAC アドレスと VLAN ID で照合します。	MAC アドレスだけで照合します。
無し	MAC アドレスだけで照合します。	MAC アドレスだけで照合します。

(2) RADIUS 認証方式

RADIUS 認証方式は、MAC 認証の対象となるポートで受信したフレームの送信元 MAC アドレスと、RADIUS サーバに登録されている MAC アドレスとを照合し、一致していれば認証成功として通信を許可する方式です。

図 12-3 固定 VLAN モードの RADIUS 認証方式の構成



なお、RADIUS 認証方式には、MAC アドレスだけで照合する方法と、MAC アドレスと VLAN ID との組み合わせで照合する方法があります。これらの方法は、コンフィギュレーションコマンド `mac-authentication vlan-check` で選択できます。

MAC アドレスと VLAN ID による照合時の設定条件を次の表に示します。

表 12-2 固定 VLAN モードの RADIUS 認証方式の VLAN ID 照合

コンフィギュレーション コマンド設定	動作
有り	MAC アドレスと VLAN ID で照合します。
無し	MAC アドレスだけで照合します。

また、RADIUS への問い合わせに用いるパスワードは、コンフィギュレーションコマンド `mac-authentication password` で設定できます。なお、コンフィギュレーションコマンド `mac-authentication password` が設定されていない場合は、認証を行う MAC アドレスをパスワードとして用います。

12.2.2 ダイナミック VLAN モード

ダイナミック VLAN モードでは、認証前 VLAN に収容されていた認証対象端末を、認証成功後、内蔵 MAC 認証 DB または RADIUS に登録されている VLAN ID を使用して、MAC VLAN と MAC アドレステーブルに登録して認証後 VLAN への通信を許可します。このため、次に示す設定が必要になります。

- MAC VLAN が設定されている MAC ポートを認証ポートとして設定

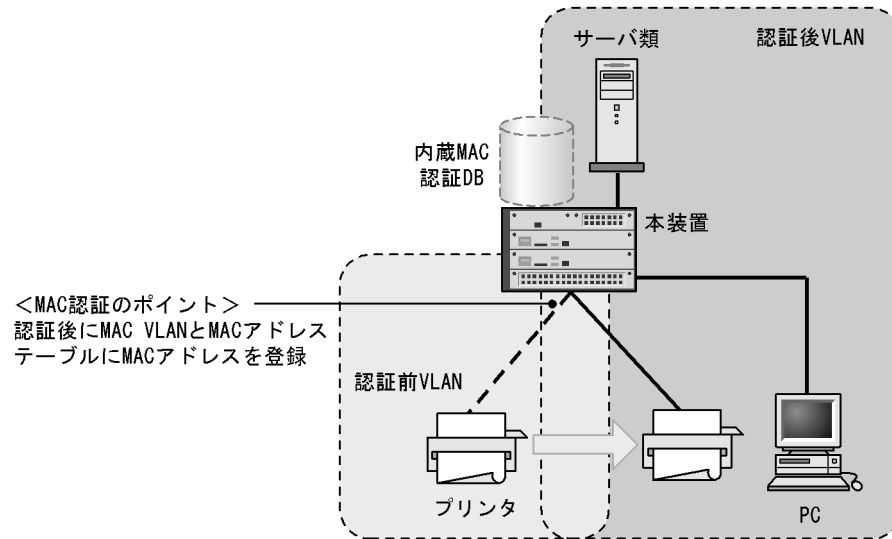
また、認証前 VLAN 内で通信したい場合は、認証専用 IPv4 アクセスリストで通信に必要なフィルタ条件を設定する必要があります。

(1) ローカル認証方式

ローカル認証方式は、MAC 認証の対象となるポートで受信したフレームの送信元 MAC アドレスと、内蔵 MAC 認証 DB に登録されている MAC アドレスとを照合し、一致していれば認証成功として内蔵 MAC 認

証 DBに登録されている VLAN ID を使用して、MAC VLAN と MAC アドレステーブルに登録し、認証後 VLAN への通信を許可する方式です。

図 12-4 ダイナミック VLAN モードのローカル認証方式の構成

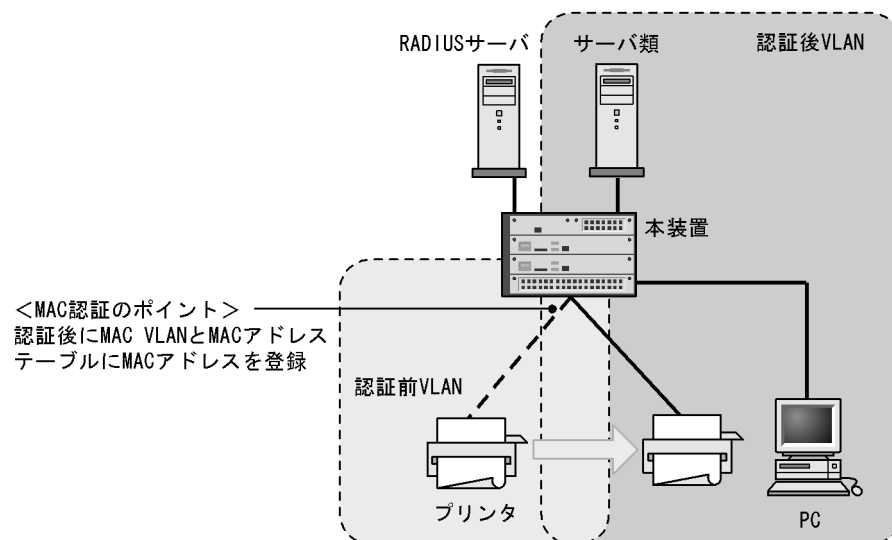


(2) RADIUS 認証方式

RADIUS 認証方式は、MAC 認証の対象となるポートで受信したフレームの送信元 MAC アドレスと、RADIUS サーバに登録されている MAC アドレスとを照合し、一致していれば RADIUS に登録されている VLAN ID を使用して、MAC VLAN と MAC アドレステーブルに登録して認証後 VLAN への通信を許可する方式です。

また、RADIUS への問い合わせに使用するパスワードは、コンフィグレーションコマンド `mac-authentication password` で設定できます。コンフィグレーションコマンド `mac-authentication password` が設定されていない場合は、認証する MAC アドレスをパスワードとして使用します。

図 12-5 ダイナミック VLAN モードの RADIUS 認証方式の構成



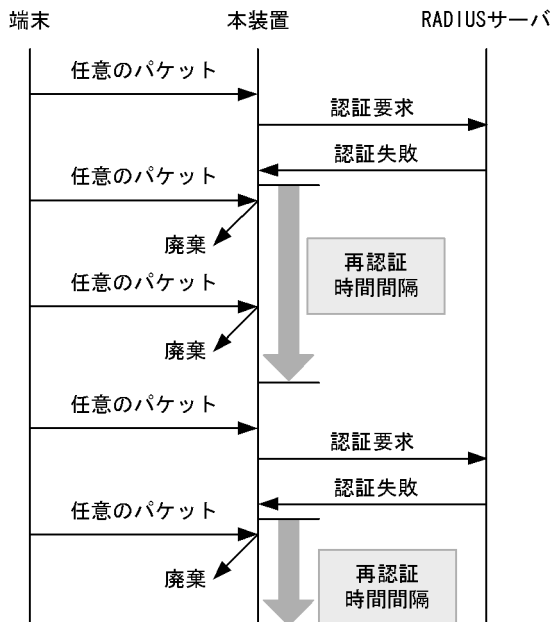
12.3 認証機能

12.3.1 認証失敗後の動作

端末の認証に失敗した場合、一定時間（再認証時間間隔と呼びます）は、MAC 認証での認証をしません。再認証時間間隔経過後、改めて認証処理を行います。

なお、コンフィグレーションコマンド `mac-authentication auth-interval-timer` によって再認証時間間隔を設定できます。設定された再認証時間間隔を超過してから 1 分以内に改めて認証処理を行います。

図 12-6 認証失敗後の動作シーケンス



12.3.2 認証解除方式

端末の認証解除方式を次の表に示します。

表 12-3 認証モードごとの認証解除方式

認証解除方式	固定 VLAN モード	ダイナミック VLAN モード
最大接続時間超過時の認証解除		
運用コマンドによる認証解除		
認証端末接続ポートのリンクダウンによる認証解除		-
認証済み端末の MAC アドレステーブルエージングによる認証解除		
VLAN 設定変更による認証解除		
認証方式の切り替えによる認証解除		
認証モードの切り替えによる認証解除		
MAC 認証の停止による認証解除		

(凡例) : サポート - : 該当なし

(1) 最大接続時間超過時の認証解除

コンフィグレーションコマンド `mac-authentication max-timer` で設定された最大接続時間を超えた場合に、強制的に認証状態を解除します。この際に設定された最大接続時間を経過してから 1 分以内で認証解除が行われます。

なお、コンフィグレーションコマンド `mac-authentication max-timer` で最大接続時間を短縮したり、延長したりした場合、現在認証中の端末には適用されず、次回認証時から設定が有効となります。

(2) 運用コマンドによる認証解除

運用コマンド `clear mac-authentication auth-state` で MAC アドレス単位に、強制的に認証解除ができます。なお、同一 MAC アドレスで複数の VLAN ID に認証を行っている場合は、同じ MAC アドレスを持つ認証をすべて解除します。

(3) 認証済み端末接続ポートのリンクダウンによる認証解除

認証済み端末が接続しているポートのリンクダウンを検出した際に、該当するポートに接続された端末の認証を解除します。

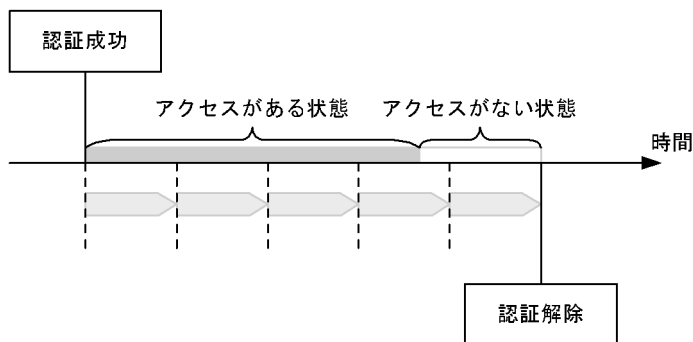
(4) 認証済み端末の MAC アドレステーブルエージングによる認証解除

認証済み端末に対し、MAC アドレステーブルを周期的に監視し、端末からのアクセスがあるかをチェックしています。該当する端末からのアクセスがない状態が続いた場合に、強制的に MAC 認証の認証状態を解除し、認証前の VLAN ID に収容を変更します。ただし、回線の瞬断などの影響で認証が解除されてしまうことを防ぐために、MAC アドレステーブルのエージング時間経過後、該当する MAC アドレスを持つ端末からのアクセスがない状態が続いた場合に、認証状態を解除します。

MAC アドレステーブルのエージング時間と、MAC アドレステーブルエージングによるログアウトの関係を次の図に示します。

なお、MAC アドレステーブルのエージング時間はデフォルト値を使用するか、またはデフォルト値より大きな値を設定してください。

図 12-7 認証済み端末の MAC アドレステーブルエージングによるログアウト



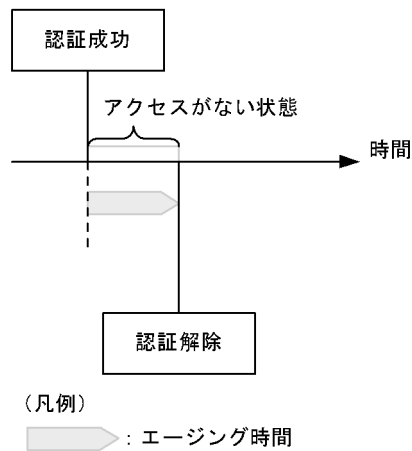
(凡例)

➡ : エージング時間

また、認証成功直後に端末からのアクセスがないと、MAC アドレステーブルエージングに合わせて、強制的に認証を解除します。

認証成功直後からアクセスがない場合のログアウトを次の図に示します。

図 12-8 認証成功直後からアクセスがない場合のログアウト



なお、この機能はコンフィグレーションコマンド `no mac-authentication auto-logout` で無効にできます (アクセスがない状態が続いた場合でも強制的にログアウトしない設定が可能)。

(5) VLAN 設定変更による認証解除

コンフィグレーションコマンドで認証端末が含まれる VLAN の設定を変更した場合、変更された VLAN に含まれる端末の認証を解除します。

[コンフィグレーションの変更内容]

- VLAN を削除した場合
- VLAN を停止 (suspend) した場合

(6) 認証方式の切り替えによる認証解除

認証方式が RADIUS 認証方式からローカル認証方式に切り替わった場合、またはローカル認証方式から RADIUS 認証方式に切り替わった場合、すべての端末の認証を解除します。

(7) 認証モードの切り替えによる認証解除

`copy` コマンドでコンフィグレーションを変更して、認証モードが切り替わる設定をした場合、すべての端末の認証を解除します。

(8) MAC 認証の停止による認証解除

コンフィグレーションコマンドで MAC 認証の定義が削除されて MAC 認証が停止した場合、すべての端末の認証を解除します。

12.3.3 認証済み端末のポート間移動

認証済み端末がポート間を移動した場合については、「7.3 レイヤ 2 認証共通の機能」を参照してください。

12.3.4 アカウント機能

認証結果は次のアカウント機能によって記録されます。

(1) アカウントログ

認証結果は本装置の MAC 認証のアカウントログに記録されます。記録されたアカウントログは、運用コマンド `show mac-authentication logging` で表示できます。

出力される認証結果を次の表に示します。

表 12-4 出力される認証結果

事象	時刻	MAC アドレス	VLAN ID	ポート番号	メッセージ
認証成功	認証成功時刻				成功メッセージ
認証解除	認証解除時刻				解除メッセージ
認証失敗	認証失敗時刻				失敗要因メッセージ

(凡例) : 記録する

注 メッセージによっては出力されない場合があります。

本装置の MAC 認証のアカウントログは、最大 2100 行まで記録できます。2100 行を超えた場合、古い順に記録が削除され、最新のアカウント情報が追加記録されていきます。

(2) RADIUS サーバのアカウント機能への記録

コンフィグレーションコマンド `aaa accounting mac-authentication` で、RADIUS サーバのアカウント機能を使用できます。アカウント機能には次の情報が記録されます。

- 認証情報 : 認証成功時に次の情報が記録されます。
サーバに記録された時刻, MAC アドレス, VLAN ID
- 認証解除情報 : 認証解除時に次の情報が記録されます。
サーバに記録された時刻, MAC アドレス, VLAN ID, 認証成功から認証解除までの経過時間

(3) RADIUS サーバへの認証情報記録

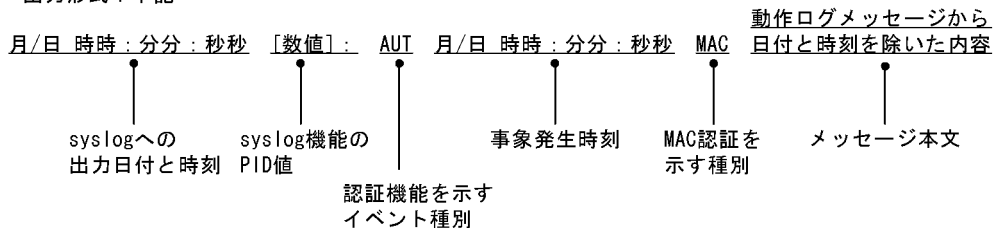
RADIUS 認証方式の場合は、RADIUS サーバが持っている機能によって、認証成功 / 認証失敗が記録されます。ただし、使用する RADIUS サーバによって記録される情報が異なることがありますので、詳細は RADIUS サーバの説明書を参照してください。

(4) syslog サーバへの動作ログ記録

MAC 認証の動作ログを syslog サーバに出力できます。また、動作ログは MAC 認証のアカウントログを含みます。syslog サーバへの出力形式を次の図に示します。

図 12-9 syslog サーバ出力形式

- イベント種別 : AUT
- 出力形式 : 下記



また、コンフィグレーションコマンド `mac-authentication logging enable` および `logging event-kind aut`

によって、出力の開始および停止ができます。

12.4 内蔵 MAC 認証 DB および RADIUS サーバの準備

12.4.1 内蔵 MAC 認証 DB の準備

MAC 認証のローカル認証方式を使用するに当たって、事前に内蔵 MAC 認証 DB を作成する必要があります。また、本装置の内蔵 MAC 認証 DB はバックアップおよび復元できます。

(1) 内蔵 MAC 認証 DB の作成

運用コマンド `set mac-authentication mac-address` で MAC アドレスおよび VLAN ID を内蔵 MAC 認証 DB に登録します。運用コマンド `remove mac-authentication mac-address` で登録した MAC アドレスの削除もできます。

登録・変更された内容は、運用コマンド `commit mac-authentication` が実行された時点で、内蔵 MAC 認証 DB に反映されます。

なお、運用コマンド `commit mac-authentication` で内蔵 MAC 認証 DB への反映を行った場合、現在認証中の端末には適用されず、次回認証時から有効となります。

注意

内蔵 MAC 認証 DB をダイナミック VLAN モードで使用する場合は、登録時に次の点に注意する必要があります。

- MAC アドレス登録時に必ず VLAN ID を指定してください。VLAN ID が省略されている場合は、その MAC アドレスは認証エラーとなります。
- 同じ MAC アドレスを複数の VLAN ID で登録した場合、最も数字の小さい VLAN ID が VLAN 切り替えに使用されます。
- VLAN ID に 1 を指定しないでください。MAC VLAN で使用できない VLAN ID のために認証エラーとなります。

(2) 内蔵 MAC 認証 DB のバックアップ

運用コマンド `store mac-authentication` で、ローカル認証用に作成した内蔵 MAC 認証 DB のバックアップを取ることができます。

(3) 内蔵 MAC 認証 DB の復元

運用コマンド `load mac-authentication` で、ローカル認証用に作成したバックアップファイルから、内蔵 MAC 認証 DB の復元ができます。ただし、復元を実行すると、直前に運用コマンド `set mac-authentication mac-address` で登録・更新していた内容は廃棄されて、復元された内容に置き換わりますので、注意が必要です。

12.4.2 RADIUS サーバの準備

MAC 認証の RADIUS 認証方式を使用するに当たっては、事前に MAC アドレスとパスワードを RADIUS サーバに設定する必要があります。

また、本装置の MAC 認証機能が使用する RADIUS の属性を示します。

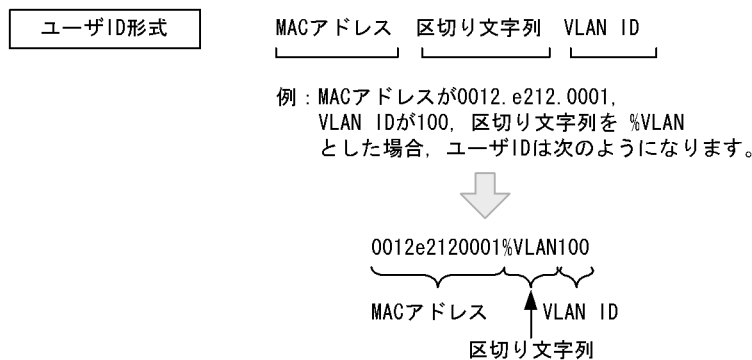
(1) ユーザ ID の登録

MAC アドレスの照合用として RADIUS のユーザ ID に MAC アドレスを登録します。MAC アドレスは

16 進文字列で半角英数字（英字は a ~ f の小文字）を用い、12 文字で指定します。

また、固定 VLAN モードで、RADIUS での照合時に MAC アドレスだけでなく VLAN ID も照合したい場合は、次に示す形式で MAC アドレスと VLAN ID を表す文字列とをつないだものをユーザ ID として登録してください。

図 12-10 MAC アドレス +VLAN ID 登録形式



(2) パスワードの登録

次のどちらかをパスワードとして設定します。

- ユーザ ID に登録した MAC アドレスと同一の MAC アドレス
- ユーザ ID に共通の文字列

(3) 認証後 VLAN の設定

ダイナミック VLAN モードで認証成功後に切り替える認証後 VLAN を次のように設定します。

1. Tunnel-Type に Virtual LANs (VLAN) を設定 (値 13) します。
2. Tunnel-Medium-Type に 6 を設定します。
3. Tunnel-Private-Group-ID に VLAN ID を次の形式で設定します。

- 数字文字で設定
例：VLAN ID が 2048 の場合、文字列で 2048 を設定
- 文字列 " VLAN " に続いて VLAN ID を数字文字で設定
例：VLAN ID が 2048 の場合、VLAN2048 を設定

(4) MAC 認証機能が使用する RADIUS サーバの属性

認証方式として PAP を設定します。また、MAC 認証が使用する RADIUS の属性を次の表に示します。なお、RADIUS サーバの詳細な設定方法については、使用する RADIUS サーバの説明書を参照してください。

表 12-5 MAC 認証で使用する属性名 (その 1 Access-Request)

属性名	Type 値	説明
User-Name	1	MAC アドレス、または「図 12-10 MAC アドレス +VLAN ID 登録形式」で生成した値を指定します。
User-Password	2	MAC アドレス、またはコンフィギュレーションコマンドで設定されたパスワードを指定します。

属性名	Type 値	説明
NAS-IP-Address	4	ループバックインタフェースの IP アドレス指定時はループバックインタフェースの IP アドレスを格納し、指定されていない場合は RADIUS サーバと通信するインタフェースの IP アドレスを格納します。
Service-Type	6	Framed(2) を設定します。
Calling-Station-Id	31	認証端末の MAC アドレス（小文字 ASCII，“-”区切り）を指定します。 例：00-12-e2-01-23-45
NAS-Identifier	32	固定 VLAN モードでは、認証端末を収容している VLAN ID を数字文字列で指定します。 例：VLAN ID 100 の場合 100 ダイナミック VLAN モードでは、コンフィグレーションコマンド hostname で指定された装置名を指定します。
NAS-Port-Type	61	Virtual(5) を設定します
NAS-IPv6-Address	95	ループバックインタフェースの IPv6 アドレス指定時はループバックインタフェースの IPv6 アドレスを格納し、指定されていない場合は RADIUS サーバと通信するインタフェースの IPv6 アドレスを格納します。ただし、IPv6 リンクローカルアドレスで通信する場合は、ループバックインタフェースの IPv6 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を格納します。

表 12-6 MAC 認証で使用する属性名（その 2 Access-Accept）

属性名	Type 値	説明
Service-Type	6	Framed(2) が返却される：MAC 認証ではチェックしません。
Reply-Message	18	（未使用）
Tunnel-Type	64	ダイナミック VLAN モード時に使用します。 VLAN を示す 13 であるかをチェックします。 固定 VLAN モード時は使用しません。
Tunnel-Medium-Type	65	ダイナミック VLAN モード時に使用します。 IEEE802.1X と同様の値 6 の Tunnel-Medium-Type であるかをチェックします。 固定 VLAN モード時は使用しません。
Tunnel-Private-Group-Id	81	ダイナミック VLAN モード時に使用します。 VLAN を表す数字文字列または “VLANxx” xx は VLAN ID を表します。 ただし、先頭の 1 オクテットの内容が 0x00 ~ 0x1f の場合は、Tag を表しているため、この場合は 2 オクテット目からの値が VLAN を表します。先頭の 1 オクテットの内容が 0x20 以上の場合は、先頭から VLAN を表します。 固定 VLAN モード時は使用しません。

表 12-7 RADIUS Accounting で使用する属性名

属性名	Type 値	説明
User-Name	1	MAC アドレス、または「図 12-10 MAC アドレス +VLAN ID 登録形式」で生成した値を指定します。
NAS-IP-Address	4	NAS の IP アドレスを格納します。 ループバックインタフェースの IP アドレス設定時は、ループバックインタフェースの IP アドレスを格納します。なお、これ以外は、サーバと通信するインタフェースの IP アドレスを格納します。
Service-Type	6	Framed(2) を設定します。

属性名	Type 値	説明
Calling-Station-Id	31	端末の MAC アドレス (小文字 ASCII, “-” 区切り) を設定します。 例: 00-12-e2-01-23-45
NAS-Identifier	32	固定 VLAN モードでは, 認証端末を収容している VLAN ID を数字文字列で設定します。 例: VLAN ID 100 の場合 100 ダイナミック VLAN モードでは, コンフィグレーションコマンド hostname で指定された装置名を指定します。
Acct-Status-Type	40	認証成功時に Start(1), 認証解除時に Stop(2) を格納します。
Acct-Delay-Time	41	イベント発生時から送信するまでに要した時間 (秒) を格納します。
Acct-Session-Id	44	プロセス ID を格納します。(認証成功, 認証解除に関しては同じ値です)
Acct-Authentic	45	認証方式を示す RADIUS, Local のどちらかを格納します。
Acct-Session-Time	46	認証解除するまでの時間 (秒) を格納します。
NAS-Port-Type	61	Virtual(5) を設定します。
NAS-IPv6-Address	95	NAS の IPv6 アドレスを格納します。 ループバックインタフェースの IPv6 アドレス設定時は, ループバックインタフェースの IPv6 アドレスを格納します。なお, 上記以外は, サーバと通信するインタフェースの IPv6 アドレスを格納します。ただし, IPv6 リンクローカルアドレスで通信する場合は, ループバックインタフェースの IPv6 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を格納します。

12.5 MAC 認証使用時の注意事項

(1) 他機能との共存

他機能との共存については、「7.2 レイヤ 2 認証と他機能との共存について」を参照してください。

(2) MAC 認証プログラムが再起動した場合

MAC 認証プログラムが再起動した場合、認証中のすべての認証が解除されます。この場合、再起動後に再度認証を行ってください。

13

MAC 認証の設定と運用

MAC 認証は、受信したフレームの送信元 MAC アドレスを認証し、VLAN へのアクセス制御を行う機能です。この章では MAC 認証のオペレーションについて説明します。

13.1 コンフィグレーション

13.2 オペレーション

13.1 コンフィグレーション

13.1.1 コンフィグレーションコマンド一覧

MAC 認証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 13-1 コンフィグレーションコマンド一覧

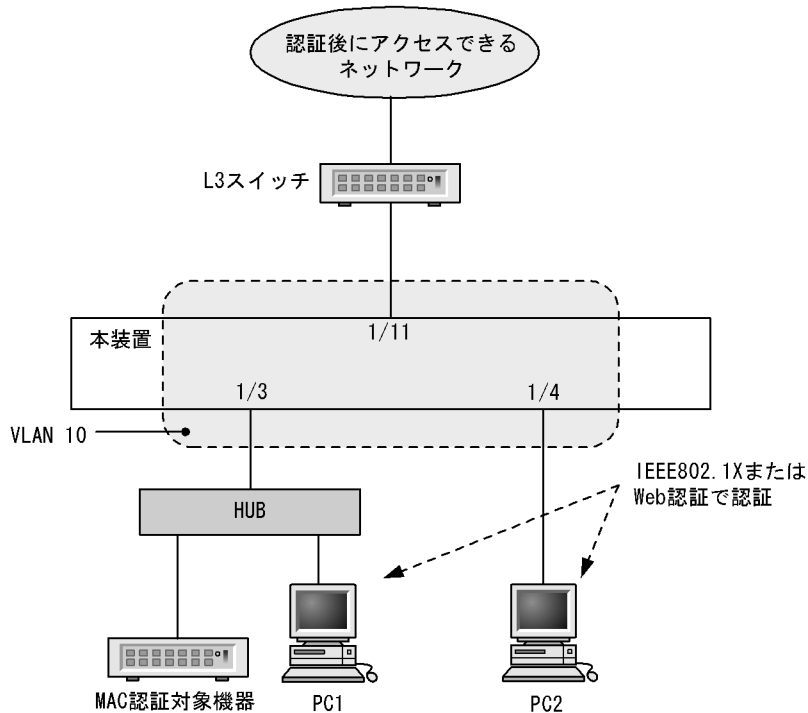
コマンド名	説明
aaa accounting mac-authentication default start-stop group radius	RADIUS Accounting を使用することを設定します。
aaa authentication mac-authentication default group radius	RADIUS 認容方式で認証することを設定します。
mac-authentication auth-interval-timer	認証失敗後、次の認証が行われるまでの再認証時間間隔を指定します。
mac-authentication auto-logout	端末からのアクセスがない状態が続いていることを検出して認証解除する動作を無効にします。
mac-authentication dynamic-vlan max-user	ダイナミック VLAN モードで認証できる MAC アドレス数を指定します。
mac-authentication logging enable	動作ログの syslog サーバへの出力を設定します。
mac-authentication max-timer	認証最大時間を指定します。
mac-authentication password	RADIUS サーバへの問い合わせ時に使用するパスワードを指定します。
mac-authentication port	MAC 認証を行うポートを設定します。
mac-authentication radius-server host	MAC 認証専用 RADIUS サーバの IP アドレスなどを指定します。
mac-authentication static-vlan max-user	固定 VLAN モードで認証できる MAC アドレス数を指定します。
mac-authentication system-auth-control	MAC 認証デーモンを起動します。
mac-authentication vlan-check	認証時に MAC アドレスに加え、VLAN ID も照合することを設定します。

13.1.2 固定 VLAN モードのコンフィグレーション

(1) ローカル認証方式の基本的な設定

ローカル認証方式を使用する上での基本的な設定を次の図に示します。

図 13-1 固定 VLAN モードのローカル認証方式の基本構成



(a) 認証ポートの設定

[設定のポイント]

MAC 認証で使用するポートを設定します。

[コマンドによる設定]

1. (config)# interface gigabitethernet 1/3
 (config-if)# switchport mode access
 (config-if)# switchport access vlan 10
 (config-if)# mac-authentication port
 (config-if)# exit

認証を行う端末が接続されているポートに MAC 認証を設定します。

(b) MAC 認証の設定

[設定のポイント]

MAC 認証のコンフィギュレーションコマンドを設定して MAC 認証を有効にします。

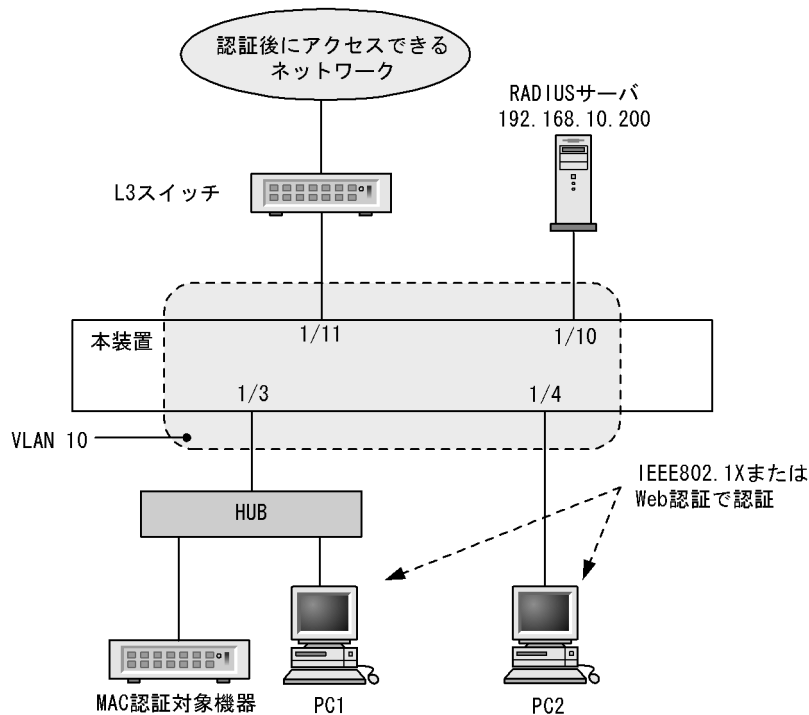
[コマンドによる設定]

1. (config)# mac-authentication system-auth-control
 MAC 認証を起動します。

(2) RADIUS 認証方式の基本的な設定

RADIUS 認証方式を使用する上での基本的な設定を次の図に示します。

図 13-2 固定 VLAN モードの RADIUS 認証方式の基本構成



(a) 認証ポートの設定

[設定のポイント]

MAC 認証で使用するポートを設定します。

[コマンドによる設定]

1. (config)# interface gigabitethernet 1/3
 (config-if)# switchport mode access
 (config-if)# switchport access vlan 10
 (config-if)# mac-authentication port
 (config-if)# exit

認証を行う端末が接続されているポートに MAC 認証を設定します。

(b) MAC 認証の設定

[設定のポイント]

MAC 認証のコンフィギュレーションコマンドを設定して MAC 認証を有効にします。

[コマンドによる設定]

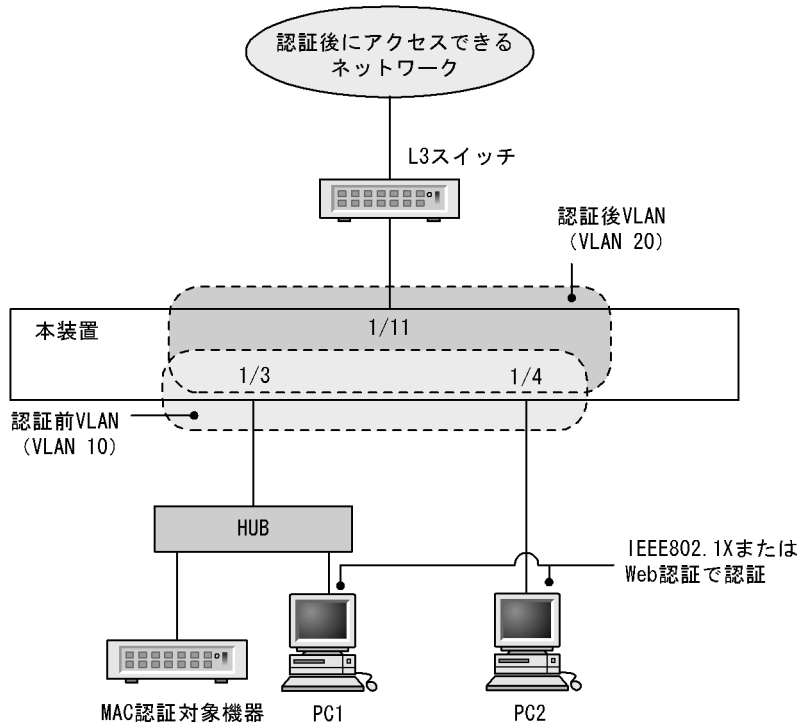
1. (config)# aaa authentication mac-authentication default group radius
 (config)# mac-authentication radius-server host 192.168.10.200 key "macauth"
 認証を RADIUS サーバにするために、IP アドレスと RADIUS 鍵を設定します。
2. (config)# mac-authentication system-auth-control
 MAC 認証を起動します。

13.1.3 ダイナミック VLAN モードのコンフィギュレーション

(1) ローカル認証方式の基本的な設定

ダイナミック VLAN モードで、ローカル認証方式を使用する上での基本的な設定を次の図に示します。

図 13-3 ダイナミック VLAN モードのローカル認証方式の基本構成



(a) 認証ポートの設定

[設定のポイント]

MAC 認証で使用するポートを設定します。

[コマンドによる設定]

1. (config)# interface range gigabitethernet 1/3-4
- (config-if-range)# switchport mode mac-vlan
- (config-if-range)# switchport mac vlan 20
- (config-if-range)# switchport mac native vlan 10
- (config-if-range)# mac-authentication port
- (config-if-range)# exit

認証を行う端末が接続されているポートに MAC 認証を設定します。

(b) MAC 認証の設定

[設定のポイント]

MAC 認証のコンフィギュレーションコマンドを設定して MAC 認証を有効にします。

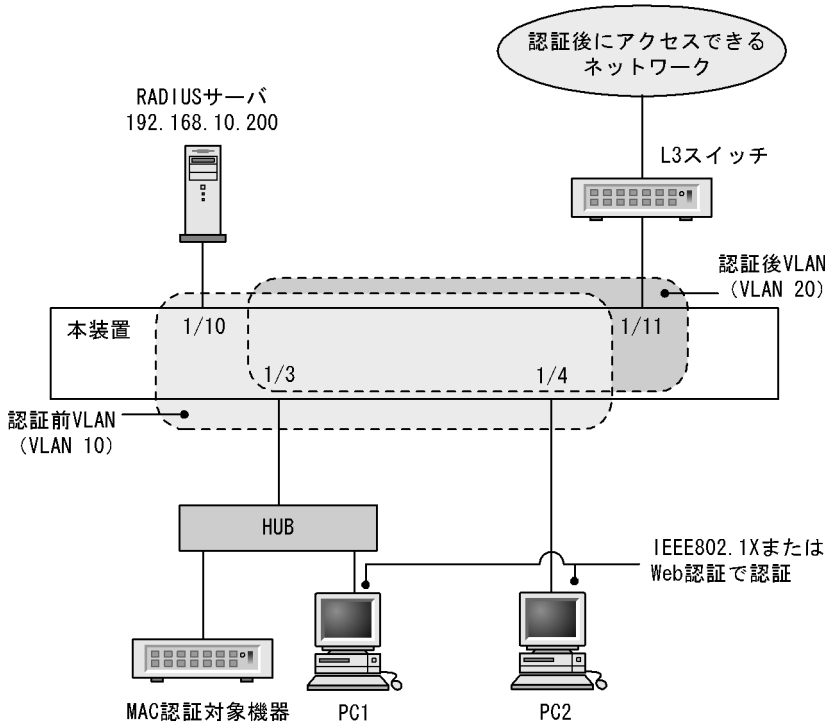
[コマンドによる設定]

1. (config)# mac-authentication system-auth-control
MAC 認証を起動します。

(2) RADIUS 認証方式の基本的な設定

ダイナミック VLAN モードで、RADIUS 認証方式を使用する上での基本的な設定を次の図に示します。

図 13-4 ダイナミック VLAN モードの RADIUS 認証方式の基本構成



(a) 認証ポートの設定

[設定のポイント]

MAC 認証で使用するポートを設定します。

[コマンドによる設定]

1. (config)# interface range gigabitethernet 1/3-4
(config-if-range)# switchport mode mac-vlan
(config-if-range)# switchport mac vlan 20
(config-if-range)# switchport mac native vlan 10
(config-if-range)# mac-authentication port
(config-if-range)# exit
認証を行う端末が接続されているポートに MAC 認証を設定します。

(b) MAC 認証の設定

[設定のポイント]

MAC 認証のコンフィギュレーションコマンドを設定して MAC 認証を有効にします。

[コマンドによる設定]

1. (config)# aaa authentication mac-authentication default group radius
(config)# mac-authentication radius-server host 192.168.10.200 key "macauth"
認証を RADIUS サーバであるために、IP アドレスと RADIUS 鍵を設定します。
2. (config)# mac-authentication system-auth-control
MAC 認証を起動します。

13.1.4 MAC 認証のパラメータ設定

MAC 認証で設定できるパラメータの設定方法を説明します。

(1) 認証最大時間の設定

[設定のポイント]

認証済みの端末を強制的に認証解除する時間を設定します。

[コマンドによる設定]

1. (config)# mac-authentication max-timer 60
強制的に認証解除する時間を 60 分に設定します。

(2) 固定 VLAN モードの認証数の設定

[設定のポイント]

固定 VLAN モードで認証できる MAC アドレス数を設定します。

[コマンドによる設定]

1. (config)# mac-authentication static-vlan max-user 20
MAC 認証の固定 VLAN モードで認証できる MAC アドレスの数を 20 個に設定します。

(3) RADIUS サーバの設定

[設定のポイント]

RADIUS 認証方式で使用する RADIUS サーバを設定します。

[コマンドによる設定]

1. (config)# aaa authentication mac-authentication default group radius
RADIUS サーバで認証するように設定します。

(4) アカウンティングの設定

[設定のポイント]

アカウンティング集計をするように設定します。

[コマンドによる設定]

1. (config)# aaa accounting mac-authentication default start-stop group radius

RADIUS サーバにアカウント集計をするように設定します。

(5) syslog サーバへの出力設定

[設定のポイント]

認証結果と動作ログを syslog サーバに出力する設定をします。

[コマンドによる設定]

1. (config)# mac-authentication logging enable
(config)# logging event-kind aut

MAC 認証の結果と動作ログを syslog サーバに出力する設定をします。

(6) 認証時に VLAN ID も照合する設定

[設定のポイント]

認証時に、MAC アドレスだけでなく VLAN ID も照合する場合に設定します。

[コマンドによる設定]

1. (config)# mac-authentication vlan-check key "@@VLAN"

認証時に VLAN ID も照合します。

また、RADIUS 認証方式で、MAC アドレスと VLAN ID とを "@@VLAN" の文字でつなげた文字列で RADIUS へ問い合わせます。

(7) RADIUS 問い合わせパスワードの設定

[設定のポイント]

RADIUS への照合の際に使用するパスワードを設定します。

[コマンドによる設定]

1. (config)# mac-authentication password pakapaka

RADIUS への照合時のパスワードとして "pakapaka" を設定します。

(8) 認証失敗後の再認証時間間隔設定

[設定のポイント]

認証失敗後の次回認証までの再認証時間間隔を設定します。

[コマンドによる設定]

1. (config)# mac-authentication auth-interval-timer 10

認証失敗後、10 分間経過後に再度認証を行うよう設定します。

(9) 認証専用 IPv4 アクセスリストの設定

[設定のポイント]

認証前状態の端末から特定のバケットを本装置外へ転送するよう設定します。

[コマンドによる設定]

1. (config)# ip access-list extended 100
 (config-ext-nacl)# permit udp any host 255.255.255.255 eq bootps
 (config-ext-nacl)# permit udp any host 192.168.10.100 eq bootps
 (config-ext-nacl)# exit
 (config)# authentication ip access-group 100
 認証前の端末から DHCP パケットだけ 192.168.10.100 へのアクセスを許可する IPv4 アクセスリストを設定します。

(10) ダイナミック VLAN モードの認証数の設定

[設定のポイント]

ダイナミック VLAN モードで認証できる MAC アドレス数を設定します。

[コマンドによる設定]

1. (config)# mac-authentication dynamic-vlan max-user 20
 MAC 認証のダイナミック VLAN モードで認証できる MAC アドレスの数を 20 個に設定します。

(11) 端末からのアクセスがない状態を検出して認証解除する動作を無効に設定

[設定のポイント]

認証済み MAC アドレスを持つ端末からのアクセスがない状態が続いても認証を解除しないように設定します。

[コマンドによる設定]

1. (config)# no mac-authentication auto-logout
 認証済み MAC アドレスを持つ端末からのアクセスがない状態が続いても認証解除させない設定をします。

13.1.5 認証除外の設定方法

MAC 認証で認証対象外とするための設定を説明します。

(1) 固定 VLAN モードの認証除外ポートの設定

固定 VLAN モードで、認証しないで通信を許可するポートを次のように設定します。

[設定のポイント]

認証を除外するポートに対しては、認証ポートを設定しません。

[コマンドによる設定]

1. (config)# vlan 10
 (config-vlan)# state active
 (config-vlan)# exit
 (config)# interface gigabitethernet 1/4
 (config-if)# switchport mode access
 (config-if)# switchport access vlan 10
 (config-if)# mac-authentication port

```
(config-if)# exit
(config)# interface gigabitethernet 1/10
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# exit
```

VLAN ID 10 を設定したポート 1/4 には認証ポートを設定します。また、ポート 1/10 には認証しないで通信を許可する設定をします。

(2) 固定 VLAN モードの認証除外端末の設定

固定 VLAN モードで、認証しないで通信を許可する端末の MAC アドレスを次のように設定します。

[設定のポイント]

認証を除外する端末の MAC アドレスを MAC アドレステーブルに登録します。

[コマンドによる設定]

```
1. (config)# vlan 10
   (config-vlan)# state active
   (config-vlan)# exit
   (config)# mac-address-table static 0012.e212.3456 vlan 10 interface
   gigabitethernet 1/10
```

VLAN ID 10 のポート 1/10 に、認証しないで通信を許可する端末の MAC アドレスを設定します。

(3) ダイナミック VLAN モードの認証除外ポートの設定

ダイナミック VLAN モードで、認証しないで通信を許可するポートを次のように設定します。

[設定のポイント]

認証を除外するポートに対しては、認証ポートを設定しません。

[コマンドによる設定]

```
1. (config)# vlan 20 mac-based
   (config-vlan)# state active
   (config-vlan)# exit
   (config)# interface gigabitethernet 1/4
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac vlan 20
   (config-if)# switchport mac native vlan 10
   (config-if)# mac-authentication port
   (config-if)# exit
   (config)# interface gigabitethernet 1/10
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 20
   (config-if)# exit
```

ダイナミック VLAN モードで扱う MAC VLAN ID 20 を設定したポート 1/4 には認証ポートを設定します。また、ポート 1/10 には認証しないで通信を許可する設定をします。

(4) ダイナミック VLAN モードの認証除外端末の設定

ダイナミック VLAN モードで、認証しないで通信を許可する端末の MAC アドレスを次のように設定します。

[設定のポイント]

認証を除外する端末の MAC アドレスを、MAC VLAN と MAC アドレステーブルに登録します。

[コマンドによる設定]

```
1. (config)# vlan 20 mac-based
   (config-vlan)# mac-address 0012.e212.3456
   (config-vlan)# exit
   (config)# mac-address-table static 0012.e212.3456 vlan 20 interface
   gigabitethernet 1/10
```

MAC VLAN ID 20 のポート 1/10 に、認証しないで通信を許可する端末の MAC アドレスを設定します。

13.2 オペレーション

13.2.1 運用コマンド一覧

MAC 認証の運用コマンド一覧を次の表に示します。

表 13-2 運用コマンド一覧

コマンド名	説明
show mac-authentication login	MAC 認証で認証済みの MAC アドレスを表示します。
show mac-authentication logging	MAC 認証の動作ログ情報を表示します。
show mac-authentication	MAC 認証のコンフィグレーションを表示します。
show mac-authentication statistics	統計情報を表示します。
clear mac-authentication auth-state mac-address	認証済み端末を強制的に認証解除します。
clear mac-authentication logging	動作ログ情報をクリアします。
clear mac-authentication statistics	統計情報をクリアします。
set mac-authentication mac-address	内蔵 MAC 認証 DB へ MAC アドレスを登録します。
remove mac-authentication	内蔵 MAC 認証 DB から MAC アドレスを削除します。
commit mac-authentication	内蔵 MAC 認証 DB をフラッシュメモリに保存します。
show mac-authentication mac-address	内蔵 MAC 認証 DB に登録された情報を表示します。
store mac-authentication	内蔵 MAC 認証 DB をバックアップします。
load mac-authentication	バックアップファイルから内蔵 MAC 認証 DB を復元します。
restart mac-authentication	MAC 認証プログラムを再起動します。
dump protocols mac-authentication	MAC 認証のダンプ情報を収集します。

13.2.2 MAC 認証の設定情報表示

show mac-authentication コマンドで MAC 認証の設定情報が表示されます。

図 13-5 MAC 認証の設定情報表示

```
# show mac-authentication
Date 2010/04/15 10:52:49 UTC
mac-authentication Information:
  Authentic-method : RADIUS           Accounting-state : disable
  Syslog-send      : enable

  Authentic-mode   : Static-VLAN
    Max-timer      : 60                 Max-terminal   : 256
    Port Count     : 1                 Auto-logout    : enable
  VLAN-check      : enable
    Vid-key        : %VLAN
  Access-list-No  : 100

  Authentic-mode   : Dynamic-VLAN
    Max-timer      : 60                 Max-terminal   : 256
    Port Count     : 1                 Auto-logout    : enable
  Access-list-No  : 100

Port Information:
  Port             : 1/2
  Dynamic-VLAN     :
  VLAN ID         : 1300-1310
  Native VLAN     : 1000

  Port             : 1/10
  Static-VLAN      :
  VLAN ID         : 300,305
```

13.2.3 MAC 認証の統計情報表示

show mac-authentication statistics コマンドで MAC 認証の状態および RADIUS との通信状況が表示されます。

図 13-6 MAC 認証の表示

```
# show mac-authentication statistics
Date 2010/04/15 11:10:49 UTC
mac-authentication Information:
  Authentication Request Total : 100
  Authentication Current Count : 10
  Authentication Error Total   : 30
RADIUS mac-authentication Information:
[RADIUS frames]
  TxTotal   : 130 TxAccReq : 130 TxError   : 0
  RxTotal   : 130 RxAccAccpt: 100 RxAccRejct: 30
  RxAccChllg: 0 RxInvalid : 0
Account mac-authentication Information:
[Account frames]
  TxTotal   : 100 TxAccReq : 100 TxError   : 0
  RxTotal   : 100 RxAccResp : 100 RxInvalid : 0
```

13.2.4 MAC 認証の認証状態表示

show mac-authentication login コマンドで MAC 認証の認証状態が表示されます。

図 13-7 MAC 認証の認証状態表示

```
# show mac-authentication login
Date 2010/04/15 10:52:49 UTC
Total client counts:2
MAC address   Port   VLAN   Login time                               Limit time   Mode
0012.e200.0001 1/1    3      2010/04/15 09:58:04 UTC                 00:10:20    Static
0012.e200.0002 1/10   4094   2010/04/15 10:10:23 UTC                 00:20:35    Dynamic
```

13.2.5 内蔵 MAC 認証 DB の作成

MAC 認証システムの環境設定およびコンフィグレーションの設定が完了したあとに、内蔵 MAC 認証 DB を作成します。また、すでに内蔵 MAC 認証 DB に登録されている内容を修正します。

(1) MAC アドレスの登録

set mac-authentication mac-address コマンドで、認証対象の MAC アドレスごとに MAC アドレス、VLAN ID を登録します。MAC アドレスを五つ登録する例を次に示します。

[コマンド入力]

```
# set mac-authentication mac-address 0012.e200.1234 100
# set mac-authentication mac-address 0012.e200.5678 100
# set mac-authentication mac-address 0012.e200.9abc 100
# set mac-authentication mac-address 0012.e200.def0 100
# set mac-authentication mac-address 0012.e200.0001 100
```

(2) MAC アドレス情報削除

登録済み MAC アドレスを削除します。

[コマンド入力]

```
# remove mac-authentication mac-address 0012.e200.1234
```

MAC アドレス (0012.e200.1234) を削除します。

(3) 内蔵 MAC 認証 DB への反映

commit mac-authentication コマンドで、set mac-authentication mac-address コマンドおよび remove mac-authentication mac-address コマンドで登録・削除した情報を、内蔵 MAC 認証 DB に反映します。

[コマンド入力]

```
# commit mac-authentication
```

13.2.6 内蔵 MAC 認証 DB のバックアップ

内蔵 MAC 認証 DB のバックアップ方法、およびバックアップファイルからの復元方法を次に示します。

(1) 内蔵 MAC 認証 DB のバックアップ

内蔵 MAC 認証 DB から store mac-authentication コマンドでバックアップファイル (次の例では backupfile) を作成します。

[コマンド入力]

```
# store mac-authentication backupfile
Backup mac-authentication MAC address data. Are you sure? (y/n): y
#
```

(2) 内蔵 MAC 認証 DB の復元

バックアップファイル (次の例では backupfile) から load mac-authentication コマンドで内蔵 MAC 認証 DB を作成します。

[コマンド入力]

```
# load mac-authentication backupfile
Restore mac-authentication MAC address data. Are you sure? (y/n): y
#
```


14 認証 VLAN 【OP-VAA】

認証 VLAN は、専用の認証サーバと連携してユーザ単位に VLAN へのアクセス制御を行う VLANAccessAgent と呼ばれる機能です。
この章では、認証 VLAN の解説と操作方法について説明します。

14.1 解説

14.2 コンフィグレーション

14.3 オペレーション

14.1 解説

認証 VLAN は、専用の認証サーバと連携してユーザ単位に VLAN へのアクセス制御を行う VLANaccessAgent と呼ばれる機能です。本装置配下に接続された端末から認証サーバに対してログインを行い、ユーザ認証が行われた結果、認証情報が本装置に通知されます。本装置は、送られてきた情報中の MAC アドレスを用いて、所定の VLAN に組み込むことによって、所属する VLAN の収容切り替えを行います。

また、本装置での認証有無にかかわらず、認証サーバから通知された認証情報をすべて登録する「通常モード」と、本装置で認証された MAC アドレスだけを登録する「スイッチ間非同期モード」があります。

認証 VLAN は、NEC 統合システム運用管理製品（WebSAM）の VLANaccess と呼ばれる認証 VLAN 専用ソフトウェアをインストールした 1 台以上の認証サーバと本装置とで構成されます。

また、認証を行う端末には、認証 VLAN ログオンと Windows ドメインログオンを SingleSignOn することができる VLANaccessClient と呼ばれる PC 上の専用クライアントソフトウェアを使用します。なお、専用クライアントソフトウェアを使用しないで、Web ブラウザで認証を行うこともできます。ただし、スイッチ間非同期モードを使用する場合は Web ブラウザとして Internet Explorer 6.0 を使用してください。

認証サーバにインストールされているソフトウェアを次の表に示します。

表 14-1 認証サーバにインストールされているソフトウェア

ソフトウェア名称		概説	接続可能な装置の動作モード	
			通常モード	スイッチ間非同期モード
VLANaccess2.0	NEC VitalQIP	統合的な IP アドレス管理を行います（運用管理機能、DNS サーバ、DHCP サーバを含みます）。		×
	NEC VitalQIP Registration Manager	DHCP 環境での Web によるユーザアクセス認証を行います。		
	VLANaccessController	VLANaccessAgent との通信および認証 Web アドオン機能で構成されています。		
VLANaccessController Ver.3.0 以降		Windows 2000 Server SP4 または、Windows 2003 Server の Active Directory と連携して、VLANaccessAgent との通信を行います。		

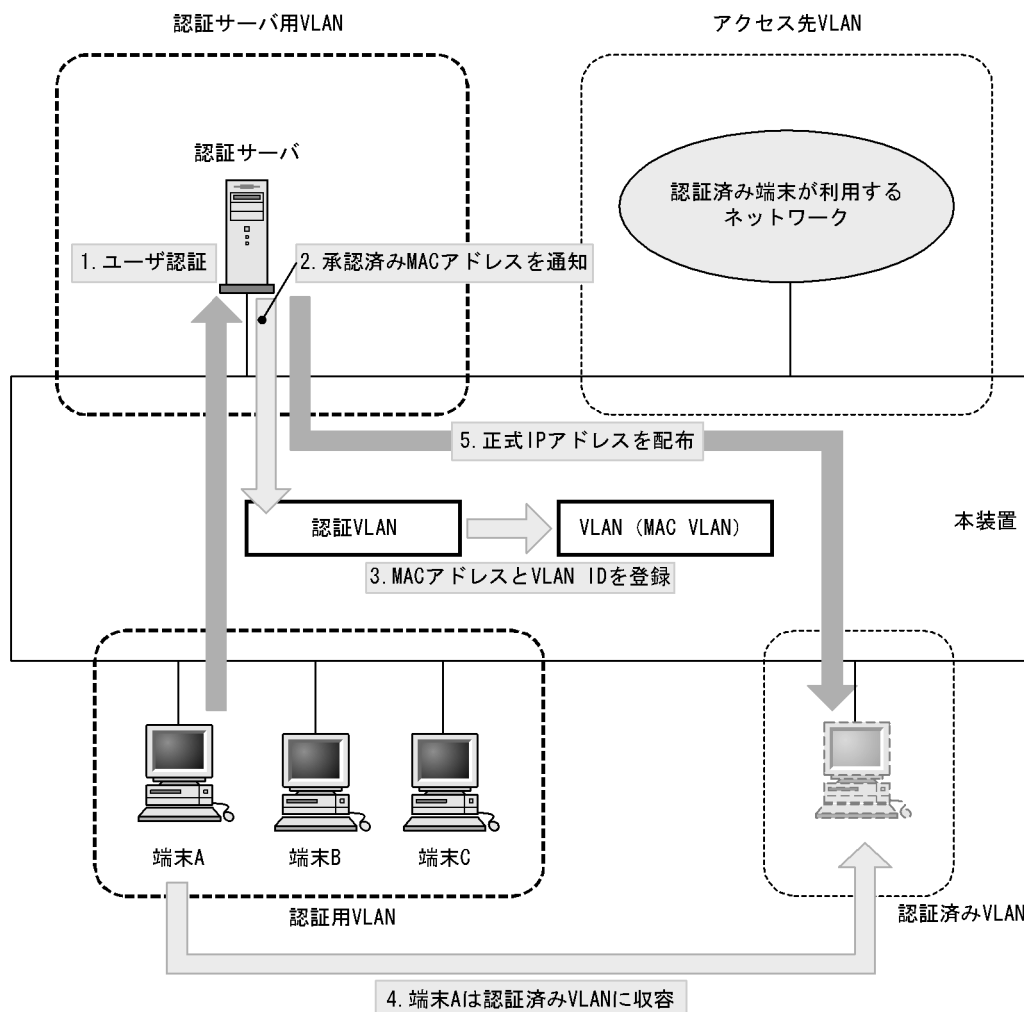
（凡例） : 接続可能 × : 接続不可

認証 VLAN は、本装置の配下に一般の L2 スイッチが使用でき、システム構築に自由度があります。冗長化機能である VRRP と連携して冗長構成を構築することもでき、小規模から大規模な認証システムの構築にも対応します。

14.1.1 機能概要

本装置を使った認証 VLAN の基本構成を次の図に示します。

図 14-1 認証 VLAN 基本構成



(凡例)

- 認証用VLAN : 未承認のユーザ端末に割り当てるVLAN
- 認証済みVLAN : ユーザ認証が完了したあとに端末に割り当てるVLAN
- 認証サーバ用VLAN : 認証サーバを接続するVLAN
- アクセス先VLAN : 認証後に端末が実際にアクセスするVLAN

14.1.2 認証手順

認証は、「図 14-1 認証 VLAN 基本構成」に示した手順で行われます。

1. ユーザ認証
認証を受ける端末は事前に DHCP クライアントの設定を行います。認証サーバ内の DHCP サーバ機能から認証サーバとの接続に使用する IP アドレスが端末に配布され、認証サーバで認証を受けることができます。
2. 認証済み MAC アドレス通知
認証完了後、認証サーバから MAC アドレスと VLAN 情報が本装置に通知されます。
3. MAC アドレスと VLAN ID を登録
認証サーバから通知された端末の MAC アドレスを、指定された VLAN に登録します。

4. 認証済み VLAN に收容

該当する MAC アドレスを持つ端末を認証済み VLAN に收容します。

5. 端末に正式 IP アドレス配布

認証サーバ内の DHCP サーバ機能から正式な IP アドレスが端末に配布されます。

また、ユーザがログアウトを行うと認証サーバのログアウト処理で MAC アドレスが本装置に通知され、認証用 VLAN に收容を戻します。

14.1.3 認証 VLAN で使用する VLAN

認証 VLAN を使用するために必要な設定を「表 14-2 認証 VLAN に必要な VLAN 設定」に示します。

なお、認証を行う端末が接続されているポートには、ポート VLAN のコンフィグレーションと MAC VLAN のコンフィグレーションの両方が必要です。

表 14-2 認証 VLAN に必要な VLAN 設定

種別	VLAN 設定	用途
認証用 VLAN	ポート VLAN	認証対象で認証を受ける端末を收容する VLAN
認証済み VLAN	MAC VLAN	認証後に收容する VLAN
認証サーバ用 VLAN	ポート VLAN	認証サーバを收容する VLAN
アクセス先 VLAN	ポート VLAN	端末が実際にアクセスするネットワークの VLAN

また、認証 VLAN を使用するにあたっては、VLAN 間で次のフィルタ設定が必要となります。

認証用 VLAN と認証済み VLAN 間：

全 IP 通信ができないようにフィルタを設定します。

認証用 VLAN と認証サーバ用 VLAN 間：

HTTP、DHCP、ICMP の通信だけ中継するようにフィルタを設定します。

認証用 VLAN とアクセス先 VLAN 間：

全 IP 通信ができないようにフィルタを設定します。

認証済み VLAN と認証サーバ用 VLAN 間：

HTTP、DHCP、ICMP の通信だけ中継するようにフィルタを設定します。

認証済み VLAN とアクセス先 VLAN 間：

フィルタ設定を行いません（すべての IP 通信を許可します）。

認証サーバ用 VLAN とアクセス先 VLAN 間：

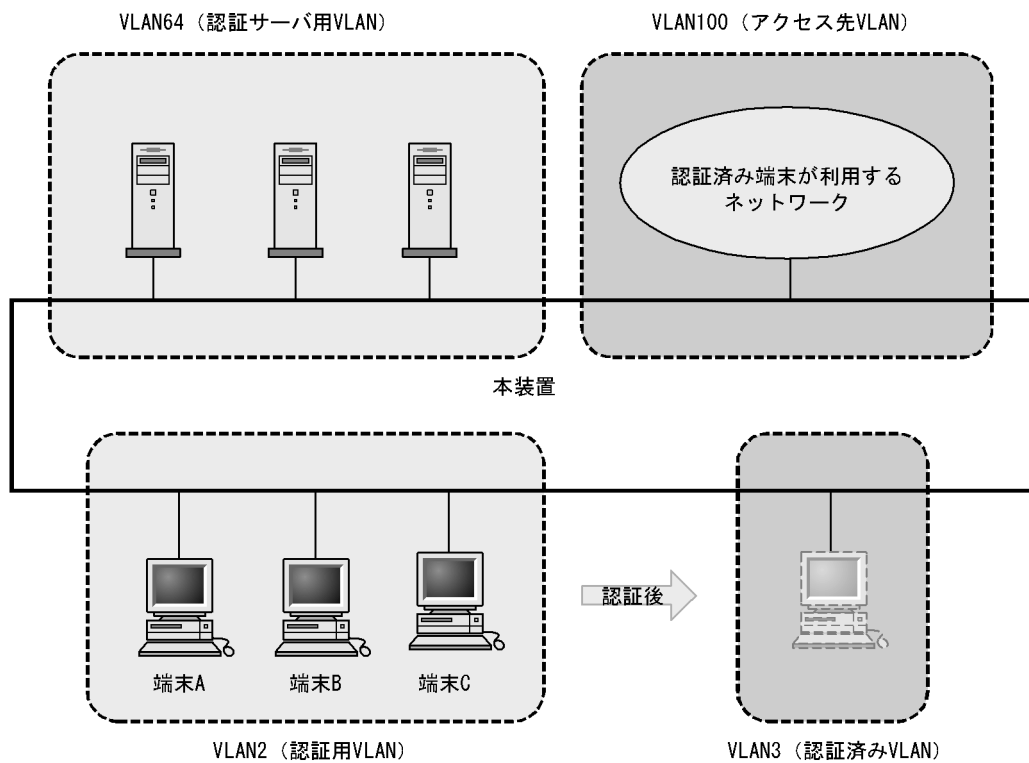
全 IP 通信ができないようにフィルタを設定します。

14.1.4 認証 VLAN の応用構成

(1) 認証サーバの複数台構成

認証サーバは 10 台まで設定できます。複数の認証サーバを設定することによって、認証時のサーバの負荷を分散できます。認証サーバを複数台使用した認証 VLAN の構成例を次の図に示します。

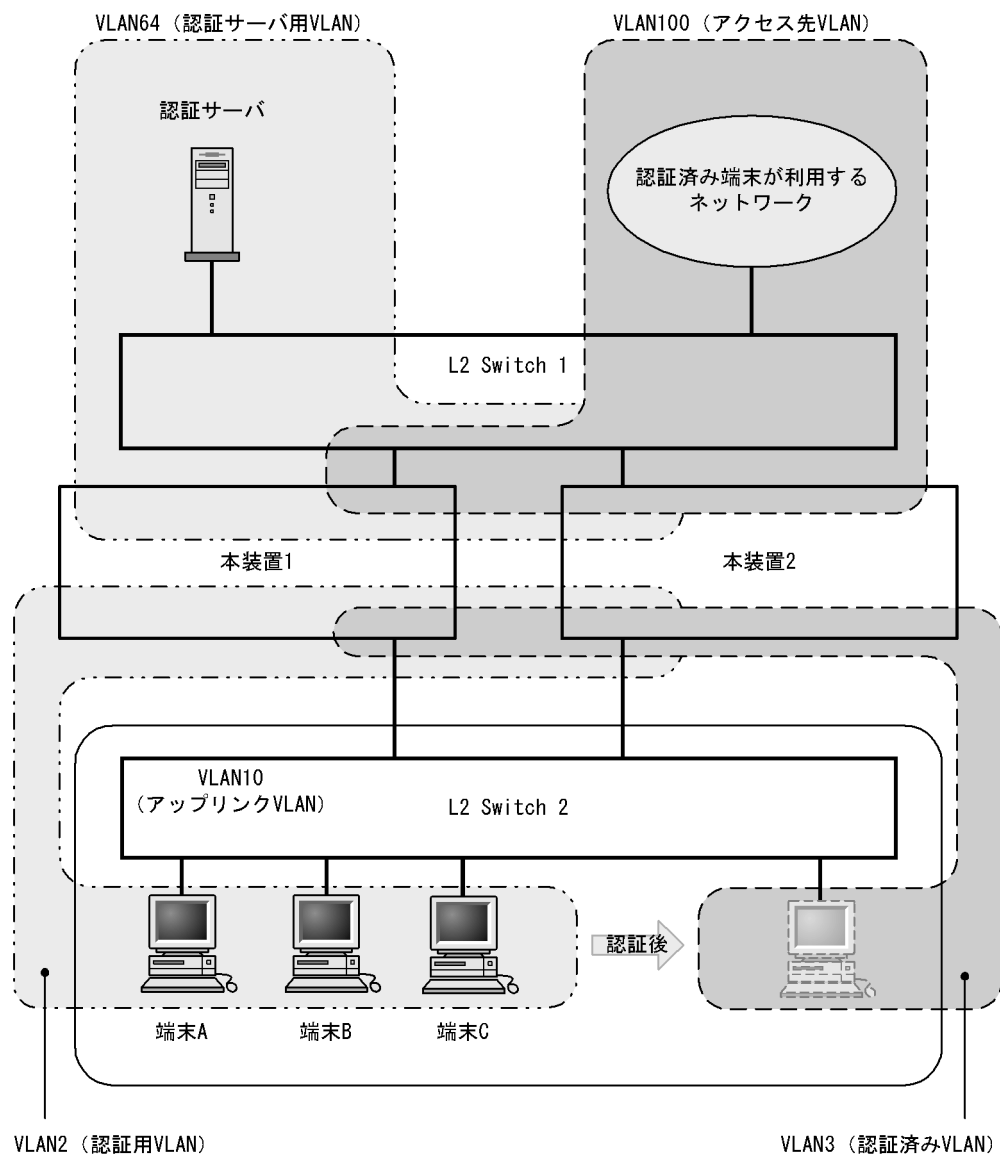
図 14-2 認証サーバ複数台構成



(2) 冗長構成

VRRP と認証 VLAN を使用して冗長構成の設定ができます。この構成は、エッジのレイヤ 2 スイッチで VLANAccessAgent をサポートしていない場合に有効です。本装置を使用した認証 VLAN の冗長構成を次の図に示します。

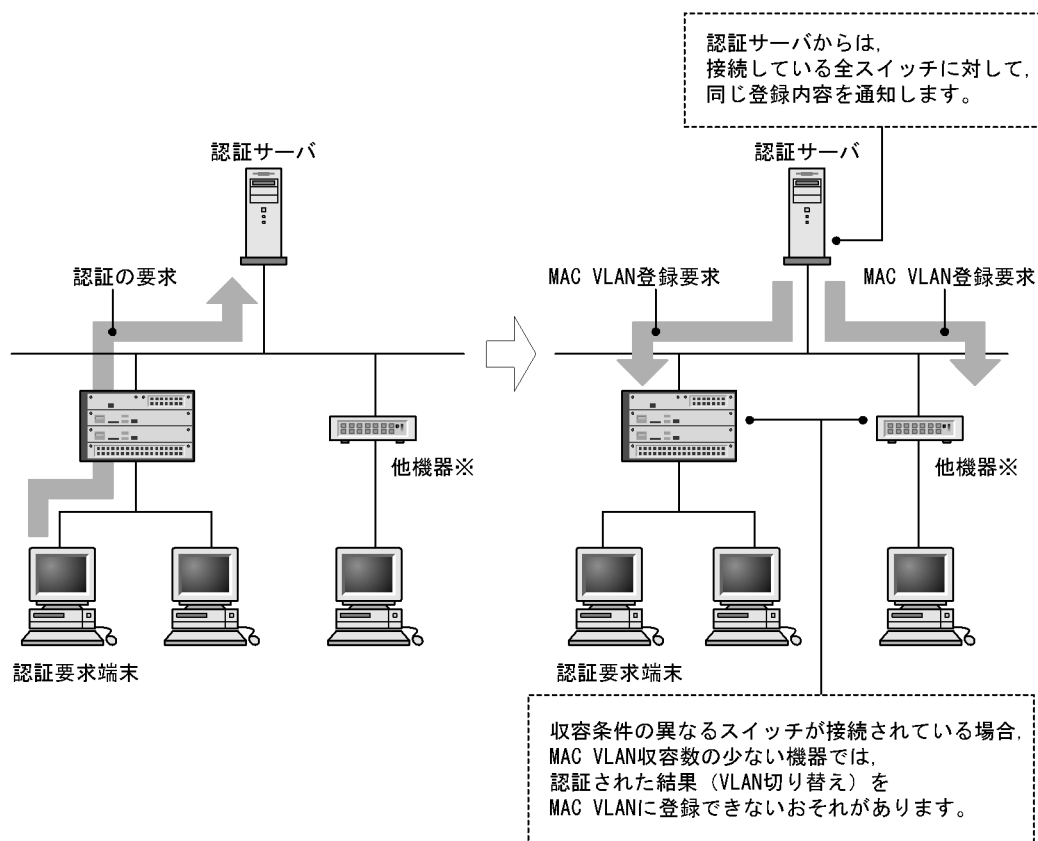
図 14-3 認証 VLAN 冗長構成



14.1.5 スイッチ間非同期モード

認証サーバで認証されたあと、認証サーバ配下の全認証スイッチに対して認証済み MAC アドレスの登録要求が出されますが、認証サーバ上の認証データがスイッチの収容条件を超えている場合、通常モードでは、認証された MAC アドレスが MAC VLAN に登録できない状態が発生することがあります。通常モードでの動作を次の図に示します。

図 14-4 通常モードでの動作



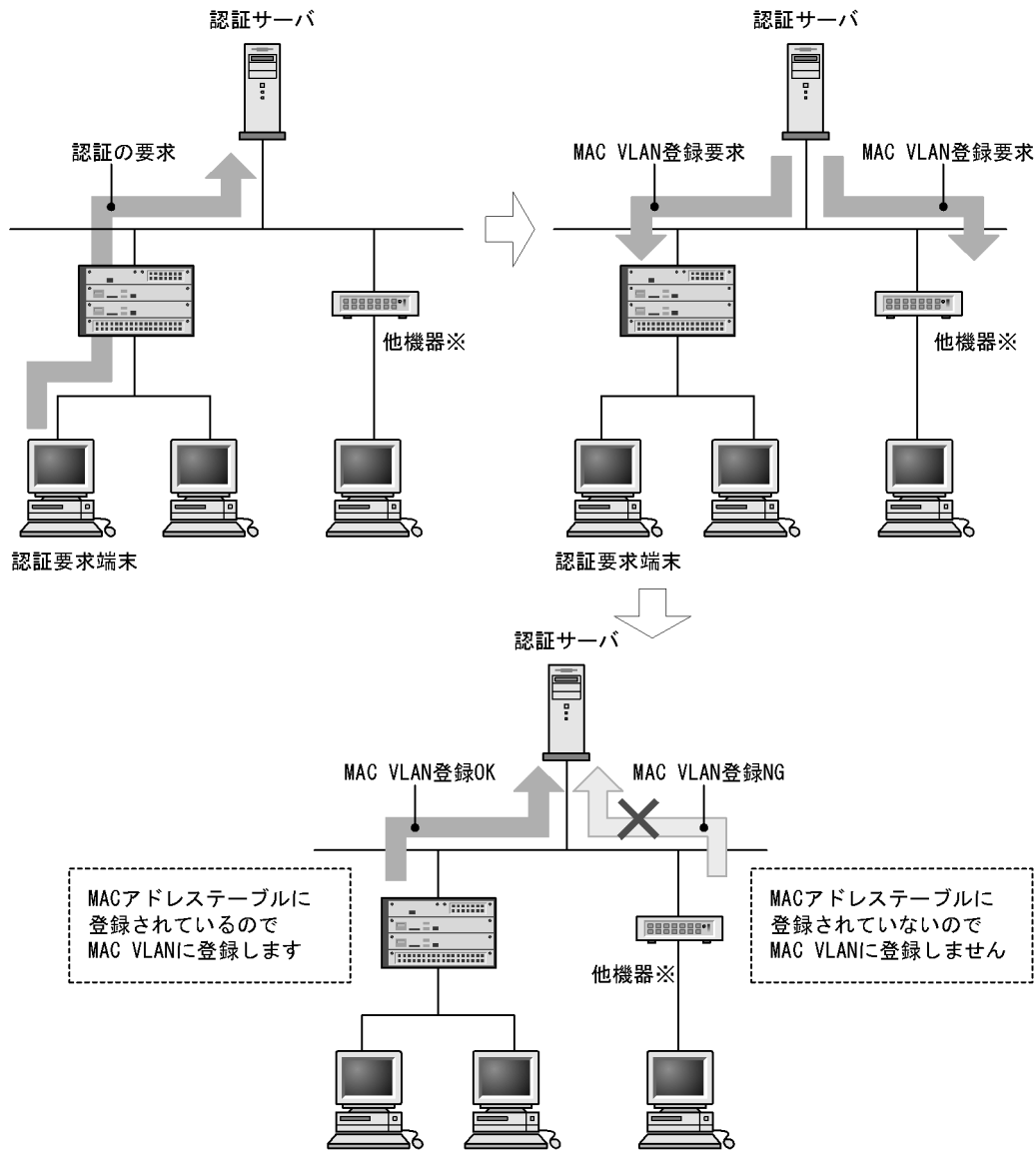
注※ 認証VLANが動作する他機器

この問題を解決するためには、コンフィグレーションコマンド `no fense vaa-sync` を設定して、スイッチ間非同期モードを有効にします。スイッチ間非同期モードでは、「図 14-5 認証対象端末だけの登録」に示すように、認証要求を行う端末を収容しているスイッチの MAC アドレステーブルに対象の MAC アドレスが登録されている場合だけ、MAC VLAN の MAC アドレスを登録します。認証要求端末を収容していないスイッチには MAC アドレスを登録しません。（認証サーバでは、MAC VLAN 登録完了通知が一つ受信できれば、その端末は認証したものとみなされます。）

スイッチ間非同期モードを有効とした場合、ほかのスイッチの MAC VLAN の収容条件によらずに、スイッチの収容能力まで認証できますが、「14.1.6 認証 VLAN 使用上の注意（11）スイッチ間非同期モード有効時の注意」に示す制限があります。

なお、コンフィグレーションコマンド `fense vaa-sync` が設定（デフォルト設定）されている場合は、通常モードの動作を行います。

図 14-5 認証対象端末だけの登録



注※ 認証VLANのスイッチ間非同期モードが動作する他機器

14.1.6 認証 VLAN 使用上の注意

(1) IEEE802.1X 認証との共存について

IEEE802.1X 認証が動作している場合 (コンフィグレーションコマンド `dot1x system-auth-control` を実行している場合), 認証 VLAN を同時に使用することはできません。

(2) 無線 LAN 使用について

本装置の配下に無線 LAN を使用する際は, アクセスポイントのルータの設定および DHCP サーバの設定を必ず OFF にしてください。

(3) 認証サーバで VLANaccess2.0 を使用する際の注意

認証サーバで VLANaccess2.0 を使用する場合は、Microsoft Windows 2000 Server に実装されている次のサービスを必ず停止してください。

- DHCP サーバ
- DHCP クライアント
- DNS サーバ

(4) エージングタイムの設定について

認証 VLAN を使用する場合は、MAC アドレステーブルエントリのエージングタイムに 0 (無限) を設定しないでください。0 を設定すると、認証後に VLAN が切り替わったとき、切り替わる前の VLAN の MAC アドレステーブルエントリがエージングされずに残ってしまうため、不要な MAC アドレステーブルエントリが蓄積することになります。

なお、切り替える前の VLAN に不要な MAC アドレステーブルエントリが蓄積した場合は、運用コマンド `clear mac-address-table` で消去してください。

(5) mac-address コマンドで静的 MAC アドレスを登録する際の注意

(`config-vlan`) モード時にコンフィグレーションコマンド `mac-address` で静的 MAC アドレスを登録する場合は、認証対象となる端末の MAC アドレスが指定されると認証済み VLAN に移動できなくなりますので、指定しないでください。

(6) no fense server コマンド実行時の動作について

コンフィグレーションコマンド `no fense server` を実行すると、対応する認証サーバとの接続を切断しますが、すでに認証済みとなっている MAC アドレスはそのままの状態ですので、認証済み端末からの通信を続けられます。さらに、コンフィグレーションコマンド `fense server` の実行によって認証サーバとの接続を再開しても、認証済み端末は再認証を行わずに通信を続けられます。認証サーバとの接続が切断された状態のまま放置してしまうと認証済み端末が不用意に使用されるおそれがありますので、このような場合は、本装置の認証 VLAN を運用コマンド `restart vaa` で再起動して、認証済み端末の MAC アドレスを削除してください。

(7) 認証サーバ設定時および認証 VLAN コンフィグレーション変更時の注意

認証サーバのネットワーク設定の変更、認証 VLAN のコンフィグレーションコマンド `fense vaa-name`、`fense server` および `fense vlan` で認証 VLAN システムのネットワーク構成を変更した場合、またはコンフィグレーションコマンド `no fense server` で認証 VLAN をいったん停止して、再度コンフィグレーションコマンド `fense server` で起動した場合は、必ず認証サーバの `VLANaccessController` を含む認証 VLAN 関連の各機能を再起動して、さらに、本装置の認証 VLAN を再起動してください。

なお、認証サーバの各機能の再起動については、認証サーバソフトに添付される説明書を参照してください。

(8) 認証サーバの HCInterval と fense alive-timer の推奨する設定値

認証 VLAN の安定動作のため、認証端末数に従って、コンフィグレーションおよび認証サーバの設定パラメータの値 (`fense.conf`) を設定してください。推奨する値を次の表に示します。

表 14-3 コンフィグレーション，認証サーバの設定パラメータの値

認証端末数	コンフィグレーション	認証サーバの設定パラメータ	
	fense alive-timer	HCInterval	RecvMsgTimeout
1 ~ 256	20 秒 (デフォルト)	15 秒 (デフォルト)	20 秒 (デフォルト)
257 ~ 4096	35 秒	30 秒	35 秒

(9) 認証サーバとの接続 / 切断が頻繁に発生する場合

認証 VLAN のコンフィグレーションコマンド設定変更によって認証サーバとの接続 / 切断を繰り返す場合があります。このような場合は，認証サーバ側の VLANAccessController を含む認証 VLAN の各機能を再起動してください。

(10) 動的 MAC アドレスの解放契機について

次の動作を行った場合，認証 VLAN が MAC VLAN に登録した動的 MAC アドレスを解放するため，端末から認証済み VLAN への通信ができなくなります。

- VLANAccessAgent を停止する。
- 認証 VLAN をログアウトする。

また，次の動作を行った場合，動的 MAC アドレスを一時的に解放しますが，認証サーバとのセッションが再接続されたあとに動的 MAC アドレスを再登録するので，端末から認証済み VLAN への通信を継続できます。

- 運用コマンド restart vaa で VLANAccessAgent を再起動する。
- 運用コマンド restart vlan mac-manager で L2MAC 管理機能を再起動する。

(11) スイッチ間非同期モード有効時の注意

スイッチ間非同期モードを有効とした場合，次に示す制限事項があります。

- 一度認証した端末がほかのスイッチに移動した場合は，再度認証操作が必要となります。
- VRRP，GSRP で装置冗長構成を組んだ場合に装置切り替えが発生すると，再度認証操作が必要となります。
- 認証端末が収容されているかの判断に MAC アドレステーブルを利用しているので，認証前 VLAN の MAC アドレステーブルがクリアされると，認証が失敗してしまいます。
- 本機能を実行しているスイッチと同一のサブネットに，通常モードの認証 VLAN が動作しているスイッチを混在させないでください。認証対象端末が接続されていなくても，通常モードの認証 VLAN が動作しているスイッチから認証サーバに登録完了の通知が届いてしまい，認証サーバ上の認証情報に不一致が発生する場合があります。
- 認証サーバに認証済みの MAC アドレスが保持されていても，スイッチが再起動すると MAC アドレステーブルをクリアしますので，スイッチ再起動後に認証が解除される場合があります。
- 二重化構成で系切替が発生した場合，MAC アドレステーブルの動的 MAC アドレスは新運用系システムに引き継がれませんので，接続されている端末は再度認証を行う必要があります。

14.2 コンフィグレーション

14.2.1 コンフィグレーションコマンド一覧

認証 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 14-4 コンフィグレーションコマンド一覧

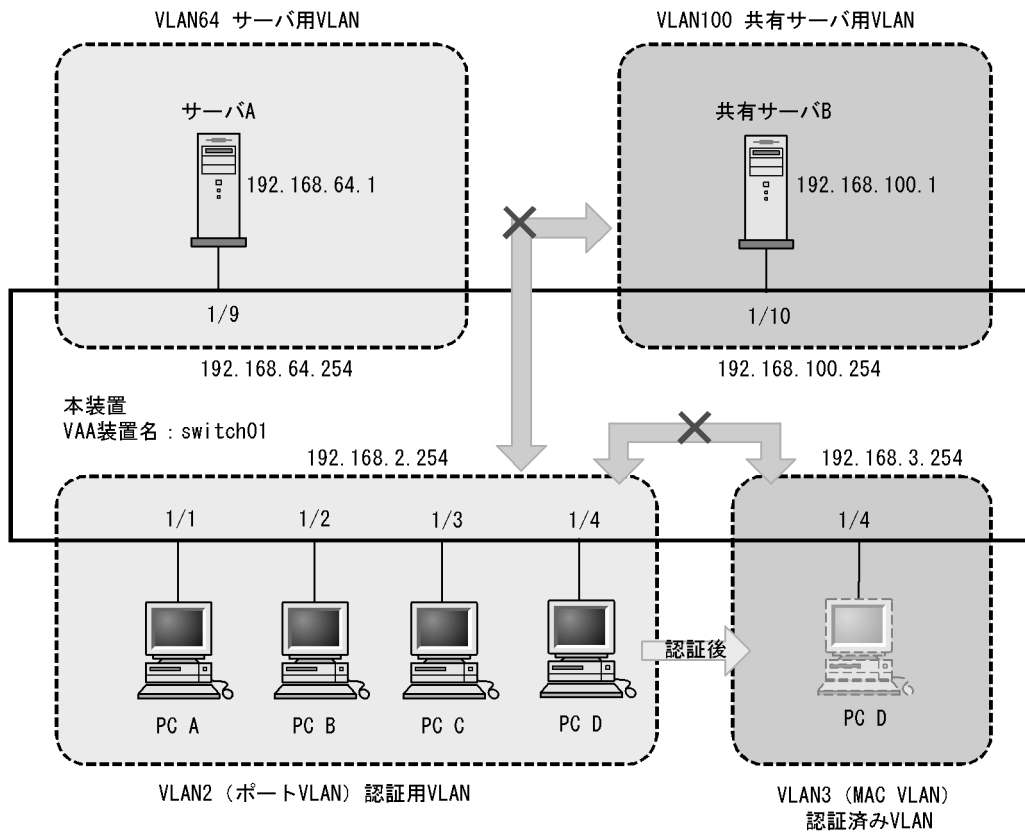
コマンド名	説明
fense alive-timer	VLANAccessController からの KeepAlive パケットの監視時間を設定します。
fense retry-count	登録済み動的 MAC アドレスを削除するまでの VLANAccessController との接続リトライ回数を設定します。
fense retry-timer	VLANAccessController との接続リトライ間隔を設定します。
fense server	VLANAccessController の IP アドレス, TCP ポート番号を指定します。
fense vaa-name	VLANAccessAgent の名称を設定します。
fense vaa-sync	通常モード / スイッチ間非同期モードを設定します。
fense vlan	認証済み VLAN の VLAN ID およびサブネットを指定します。

14.2.2 認証 VLAN の基本的な設定

認証 VLAN を使用する上での基本的な設定を説明します。

本装置と認証サーバ 1 台でシステムを構成した場合の構成図を次の図に示します。

図 14-6 認証 VLAN 基本構成



認証用 VLAN と認証済み VLAN を設定したあと、VLANaccessAgent の名称を設定し、VLANaccessController の IP アドレス、認証済み VLAN の VLAN ID、サブネットを設定します。

さらに、各 VLAN 間のフィルタ設定と、認証用 VLAN および認証済み VLAN からサーバ用 VLAN への DHCP リレーエージェントを設定します。

(1) DHCP リレーエージェントの設定

[設定のポイント]

認証用 VLAN および認証済み VLAN からサーバ用 VLAN への DHCP リレーエージェントを設定します。

[コマンドによる設定]

- ```
(config)# interface vlan 2
(config-if)# ip address 192.168.2.254 255.255.255.0
(config-if)# ip helper-address 192.168.64.1
```

VLAN2 に DHCP リレーエージェントを設定します。
- ```
(config)# interface vlan 3
(config-if)# ip address 192.168.3.254 255.255.255.0
(config-if)# ip helper-address 192.168.64.1
```

VLAN3 に DHCP リレーエージェントを設定します。

(2) 認証ポートの設定

[設定のポイント]

認証を行う端末が接続されているポート 1/1-4 に、認証用 VLAN と認証済み VLAN を指定します。

[コマンドによる設定]

1. (config)# interface gigabitethernet 1/1-4
 (config-if)# switchport mode mac-vlan
 (config-if)# switchport mac vlan 3
 (config-if)# switchport mac native vlan 2
 ポート 1/1-4 に MAC VLAN (VLAN3) と native vlan (VLAN2) を設定します。

(3) フィルタの設定

[設定のポイント]

認証用 VLAN からはサーバ用 VLAN に対して HTTP, DHCP, ICMP の通信だけ中継を許可するよう、フィルタ (アクセスリスト) を設定します。また、DHCP の動的 IP アドレスを取得要求のパケットを中継許可するよう、フィルタ (アクセスリスト) を設定します。

[コマンドによる設定]

1. (config)# ip access-list extended 100
 (config-ext-nacl)# permit tcp 192.168.2.0 0.0.0.255 host 192.168.64.1 eq http
 (config-ext-nacl)# permit udp 192.168.2.0 0.0.0.255 host 255.255.255.255 eq bootps
 (config-ext-nacl)# permit udp 192.168.2.0 0.0.0.255 host 192.168.64.1 eq bootps
 (config-ext-nacl)# permit icmp 192.168.2.0 0.0.0.255 host 192.168.64.1
 (config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 255.255.255.255
 (config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.64.1
 (config-ext-nacl)# deny ip any any
 アクセスリストを設定します。
2. (config)# interface vlan 2
 (config-if)# ip access-group 100 in layer3-forwarding
 VLAN2 にアクセスグループ 100 を設定します。

(4) 認証 VLAN の設定

[設定のポイント]

認証 VLAN のコンフィグレーションコマンドを設定して認証 VLAN を有効にします。

[コマンドによる設定]

1. (config)# fense vaa-name switch01
 本装置の VLANaccessAgent の名称を設定します。
2. (config)# fense 1 vlan 10 192.168.3.0 255.255.255.0
 認証済み VLAN のサブネットを設定します。

14. 認証 VLAN【OP-VAA】

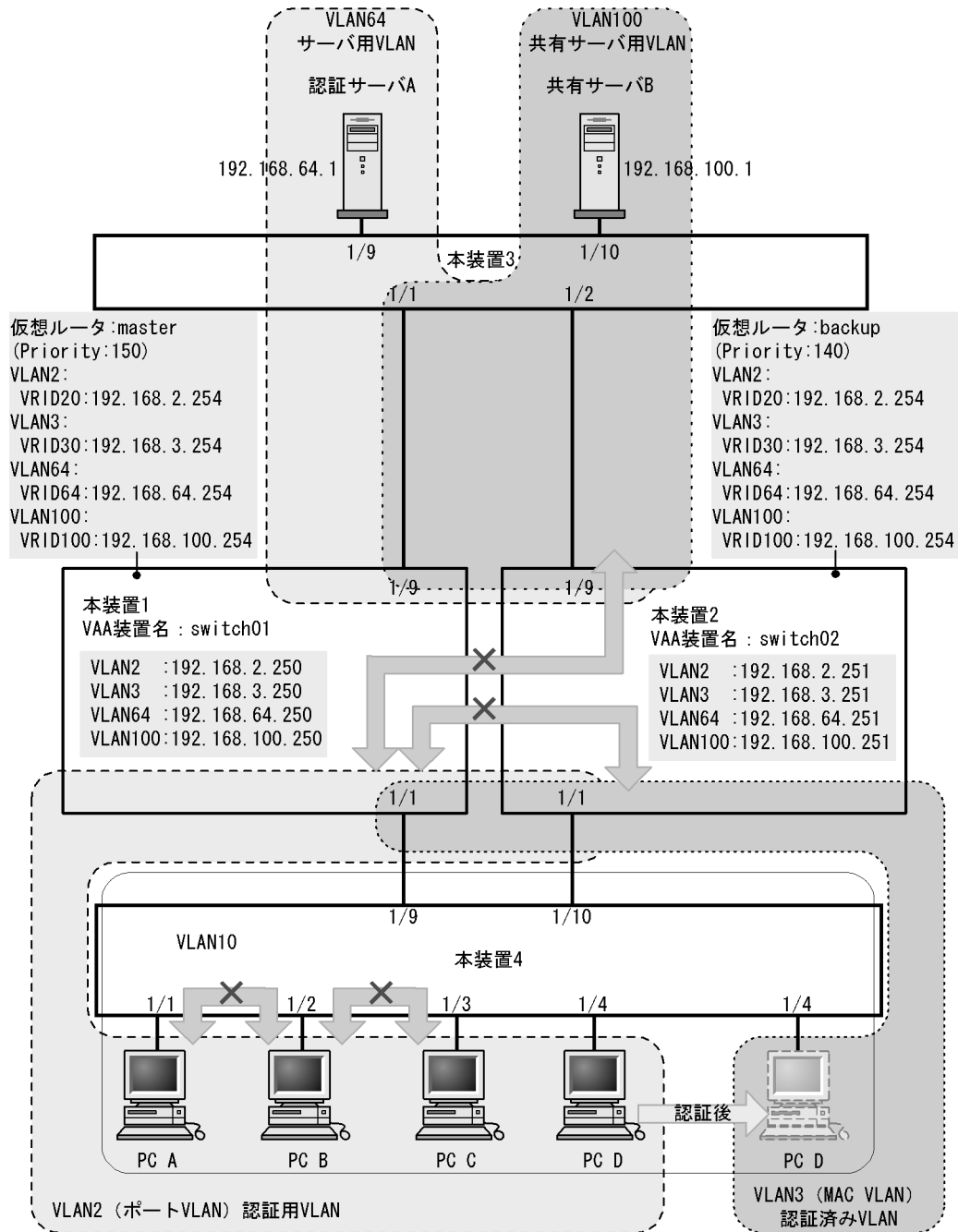
3. `(config)# fense 1 server 192.168.64.1`
VLANaccessController の IP アドレスを設定します。

14.2.3 冗長構成

VRRP と認証 VLAN を使用した冗長構成での本装置の設定を説明します。

本装置 2 台で VRRP 冗長構成とし、本装置 1 と本装置 2 で認証 VLAN を動作させる場合の構成図を次の図に示します。

図 14-7 認証 VLAN 冗長構成



認証用 VLAN と認証済み VLAN を、冗長化させる複数台の本装置にそれぞれ設定したあと、VRRP を設定します。fense vaa-name コマンドによる VLANAccessAgent の名称を設定する際は、装置ごとに別の名前を割り当ててください。さらに、各 VLAN 間のフィルタ設定と、認証用 VLAN および認証済み VLAN からサーバ用 VLAN へ DHCP リレーエージェントを設定します。

(1) 装置 1 の設定

(a) DHCP リレーエージェントの設定

[設定のポイント]

14. 認証 VLAN 【OP-VAA】

認証用 VLAN および認証済み VLAN からサーバ用 VLAN への DHCP リレーエージェントを設定します。

[コマンドによる設定]

```
1. (config)# interface vlan 2
   (config-if)# ip address 192.168.2.250 255.255.255.0
   (config-if)# ip helper-address 192.168.64.1
   VLAN2 に DHCP リレーエージェントを設定します。
```

```
2. (config)# interface vlan 3
   (config-if)# ip address 192.168.3.250 255.255.255.0
   (config-if)# ip helper-address 192.168.64.1
   VLAN3 に DHCP リレーエージェントを設定します。
```

(b) 認証ポートの設定

[設定のポイント]

装置 4 が接続されているポート 1/1 に、認証用 VLAN と認証済み VLAN を設定します。

[コマンドによる設定]

```
1. (config)# interface gigabitethernet 1/1
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac vlan 3
   (config-if)# switchport mac native vlan 2
   ポート 1/1 に MAC VLAN (VLAN 3) と native vlan (VLAN 2) を設定します。
```

(c) フィルタの設定

[設定のポイント]

認証用 VLAN からは認証サーバ用 VLAN に対して HTTP, DHCP, ICMP の通信だけ中継を許可するように、フィルタ (アクセスリスト) を設定します。また、DHCP の動的 IP アドレスを取得要求の packets を中継許可するように、フィルタ (アクセスリスト) を設定します。

[コマンドによる設定]

```
1. (config)# ip access-list extended 100
   (config-ext-nacl)# permit tcp 192.168.2.0 0.0.0.255 host 192.168.64.1 eq http
   (config-ext-nacl)# permit udp 192.168.2.0 0.0.0.255 host 255.255.255.255 eq
   bootps
   (config-ext-nacl)# permit udp 192.168.2.0 0.0.0.255 host 192.168.64.1 eq
   bootps
   (config-ext-nacl)# permit icmp 192.168.2.0 0.0.0.255 host 192.168.64.1
   (config-ext-nacl)# permit vrrp 192.168.2.0 0.0.0.255 host 192.168.64.1
   (config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 255.255.255.255
   (config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.64.1
   (config-ext-nacl)# deny ip any any
   アクセスリストを設定します。
```


2. (config)# interface vlan 2
 (config-if)# ip access-group 100 in layer3-forwarding
 VLAN2 にアクセスグループ 100 を設定します。

(d) 認証 VLAN の設定

[設定のポイント]

認証 VLAN のコンフィギュレーションコマンドを設定して認証 VLAN を有効にします。

[コマンドによる設定]

1. (config)# fense vaa-name switch01
 本装置 1 の VLANaccessAgent の名称を設定します。
2. (config)# fense 1 vlan 3 192.168.3.0 255.255.255.0
 認証済み VLAN のサブネットを設定します。
3. (config)# fense 1 server 192.168.64.1
 VLANaccessController の IP アドレスを設定します。

(2) 装置 2 の設定

(a) DHCP の設定

[設定のポイント]

認証前 VLAN および、認証済み VLAN からサーバ用 VLAN への DHCP リレーエージェントを設定します。

[コマンドによる設定]

1. (config)# interface vlan 2
 (config-if)# ip address 192.168.2.251 255.255.255.0
 (config-if)# ip helper-address 192.168.64.1
 (config-if)# exit
 VLAN 2 に DHCP リレーエージェントを設定します。
2. (config)# interface vlan 3
 (config-if)# ip address 192.168.3.251 255.255.255.0
 (config-if)# ip helper-address 192.168.64.1
 VLAN 3 に DHCP リレーエージェントの設定をします。

(b) 認証ポートの設定

[設定のポイント]

装置 4 が接続されているポートに、認証用 VLAN と認証済み VLAN を設定します。

[コマンドによる設定]

1. (config)# interface gigabitethernet 1/1
 (config-if)# switchport mode mac-vlan
 (config-if)# switchport mac vlan 3

14. 認証 VLAN 【OP-VAA】

```
(config-if)# switchport mac native vlan 2
```

ポート 1/1 に MAC VLAN (VLAN 3) と native vlan (VLAN 2) を設定します。

(c) フィルタの設定

[設定のポイント]

認証用 VLAN からはサーバ用 VLAN に対して HTTP, DHCP, ICMP の通信だけ中継を許可するよう、フィルタ (アクセスリスト) を設定します。また、DHCP の動的 IP アドレスを取得要求のパケットを中継許可するよう、フィルタ (アクセスリスト) を設定します。

[コマンドによる設定]

1. (config)# ip access-list extended 100
(config-ext-nacl)# permit tcp 192.168.2.0 0.0.0.255 host 192.168.64.1 eq http
(config-ext-nacl)# permit udp 192.168.2.0 0.0.0.255 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit udp 192.168.2.0 0.0.0.255 host 192.168.64.1 eq bootps
(config-ext-nacl)# permit icmp 192.168.2.0 0.0.0.255 host 192.168.64.1
(config-ext-nacl)# permit vrrp 192.168.2.0 0.0.0.255 host 192.168.64.1
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 255.255.255.255
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.64.1
(config-ext-nacl)# deny ip any any
アクセスリストを設定します。

2. (config)# interface vlan 2
(config-if)# ip access-group 100 in layer3-forwarding
VLAN 2 にアクセスグループ 100 を設定します。

(d) 認証 VLAN の設定

[設定のポイント]

認証 VLAN のコンフィグレーションコマンドを設定して認証 VLAN を有効にします。

[コマンドによる設定]

1. (config)# fense vaa-name switch02
本装置 2 の VLANAccessAgent の名称を設定します。
2. (config)# fense 1 vlan 3 192.168.3.0 255.255.255.0
認証済み VLAN のサブネットを設定します。
3. (config)# fense 1 server 192.168.64.1
VLANAccessController の IP アドレスを設定します。

14.2.4 認証 VLAN のパラメータ設定

認証 VLAN で可能なパラメータ設定を説明します。

(1) 認証サーバ接続リトライ間隔の設定

[設定のポイント]

認証サーバとの接続リトライ間隔を設定します。

[コマンドによる設定]

1. (config)# fense 1 retry-timer 30

VAA ID 1 の VLANAccessAgent に接続リトライ間隔を 30 秒に設定します。

(2) MAC アドレス削除接続リトライ回数の設定

[設定のポイント]

本装置に登録済みの MAC アドレスを削除するまでの認証サーバとの接続リトライ回数を設定します。

[コマンドによる設定]

1. (config)# fense 1 retry-count 10

VAA ID 1 の VLANAccessAgent に MAC アドレスを削除するまでの接続リトライ回数を 10 回に設定します。

(3) KeepAlive パケット監視時間間隔の設定

[設定のポイント]

VLANAccessController からの KeepAlive パケットがこのコマンドで設定した時間以内に到着しない場合、認証サーバへの再接続処理を実行します。

[コマンドによる設定]

1. (config)# fense 1 alive-timer 40

VAA ID 1 の VLANAccessAgent に認証サーバからの KeepAlive パケット受信を待つ時間を 40 秒に設定します。

(4) スイッチ間非同期モードの設定

[設定のポイント]

装置のスイッチ間非同期モードを有効にします。

[コマンドによる設定]

1. (config)# no fense vaa-sync

スイッチ間非同期モードを有効にします。

14.3 オペレーション

14.3.1 運用コマンド一覧

認証 VLAN の運用コマンド一覧を次の表に示します。

表 14-5 運用コマンド一覧

コマンド名	説明
show fense server	VLANAccessAgent の情報を表示します。
show fense statistics	VLANAccessAgent の統計情報を表示します。
show fense logging	VLANAccessAgent のログ情報を収集し表示します。
clear fense statistics	VLANAccessAgent の統計情報をクリアします。
clear fense logging	VLANAccessAgent のログ情報をクリアします。
restart vaa	VLANAccessAgent プログラムを再起動します。
dump protocols vaa	VLANAccessAgent のダンプ情報を収集します。

14.3.2 認証 VLAN 動作確認

認証 VLAN を使用した場合、show fense server detail コマンドを実行して動作の確認を行ってください。

図 14-8 認証 VLAN 詳細状態情報表示

```
> show fense server detail
Date 2006/03/01 10:50:49 UTC
VAA NAME: switch01
VAA Sync Mode: Sync
Current Registered MAC: 120 ... 1
Server Information:
ID:1      Status: enable      Agent Status: CONNECTED ... 2,3
  Server Address: 192.168.2.100      Port: 52153
    Retry Timer: 10  Retry Count: 25920  Current Count: 0
    Alive Timer: 20
  Target-VLAN Count: 4
  Target-VLAN Information:
    VLAN ID:2  1P Subnet Address: 192.168.2.0  mask 255.255.255.0
    VLAN ID:3  1P Subnet Address: 192.168.3.0  mask 255.255.255.0
    VLAN ID:4  1P Subnet Address: 192.168.4.0  mask 255.255.255.0
    VLAN ID:10 1P Subnet Address: 192.168.10.0  mask 255.255.255.0
```

[確認ポイント]

1. Current Registered MAC

MAC VLAN に登録済みの MAC アドレス数です。登録されている MAC アドレスの一覧を表示する場合は、show vlan mac-vlan <vlan id list> dynamic コマンドを使用してください。

2. Status

<vaa_id> ごとの起動 / 停止状態を表します。enable であることを確認してください。

3. Agent Status

認証サーバとの接続状態が CONNECTED であることを確認してください。

15 DHCP snooping

DHCP snooping は、本装置を通過する DHCP パケットを監視して信頼されていない端末からのアクセスを制限する機能で、IPv4 ネットワークに適用します。

この章では、DHCP snooping の解説と操作方法について説明します。

15.1 解説

15.2 コンフィグレーション

15.3 オペレーション

15.1 解説

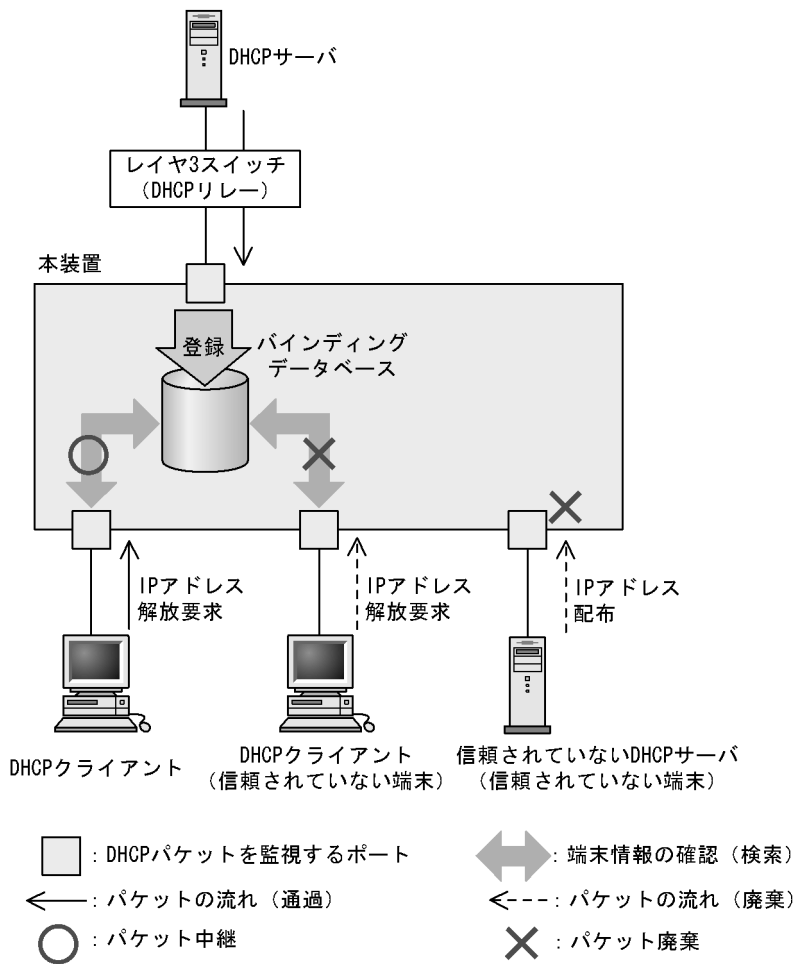
15.1.1 概要

DHCP snooping は、本装置を通過する DHCP パケットを監視して、信頼されていない端末からのアクセスを制限する機能です。

また、信頼されていない端末からの IPv4 パケットを制限する端末フィルタや、不正な ARP パケットを廃棄する動的 ARP 検査もサポートしています。

DHCP snooping は、次の図に示すように DHCP サーバと DHCP クライアントの間に本装置を接続して使用します。

図 15-1 DHCP snooping 概要



端末情報の登録先をバインディングデータベースと呼びます。

DHCP snooping でサポートする機能を次の表に示します。

表 15-1 DHCP snooping でサポートする機能

項目	機能の概要
DHCP パケットの監視	<ul style="list-style-type: none"> DHCP サーバから IP アドレスを配布された DHCP クライアントを監視し、端末情報をバインディングデータベースで管理
固定 IP アドレスを持つ端末の登録	<ul style="list-style-type: none"> バインディングデータベースへ端末情報をスタティックに登録
バインディングデータベースの保存	<ul style="list-style-type: none"> バインディングデータベースの保存および装置再起動時の復元
DHCP パケットの検査	<ul style="list-style-type: none"> 信頼されていない DHCP サーバからの IP アドレス配布を抑制 信頼されていない DHCP クライアントからの IP アドレス解放を抑制 MAC アドレスの詐称を抑制 Option82 の詐称を抑制
DHCP パケットの受信レート制限	<ul style="list-style-type: none"> 設定した受信レートを越えた DHCP パケットを廃棄
端末フィルタ	<ul style="list-style-type: none"> 信頼されていない端末からの IPv4 パケットの中継を抑制
ARP パケットの検査	<ul style="list-style-type: none"> 信頼されていない端末からの ARP パケットの中継を抑制 MAC アドレスおよび IP アドレスの詐称を抑制
ARP パケットの受信レート制限	<ul style="list-style-type: none"> 設定した受信レートを越えた ARP パケットを廃棄

15.1.2 DHCP パケットの監視

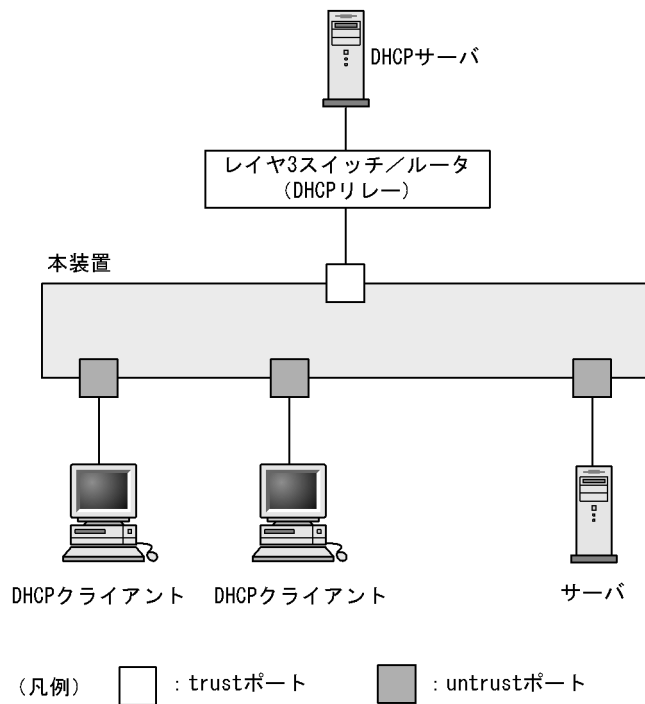
(1) ポートの種別

DHCP snooping では、ポートを次の種別に分類して、DHCP パケットを監視します。

- trust ポート
DHCP サーバや部門サーバなど、信頼済みの端末を接続するポートを trust ポートと呼びます。
- untrust ポート
DHCP クライアントなど、信頼されていない端末を接続するポートを untrust ポートと呼びます。
DHCP サーバは接続しません。

ポートの種別を次の図に示します。

図 15-2 ポートの種別



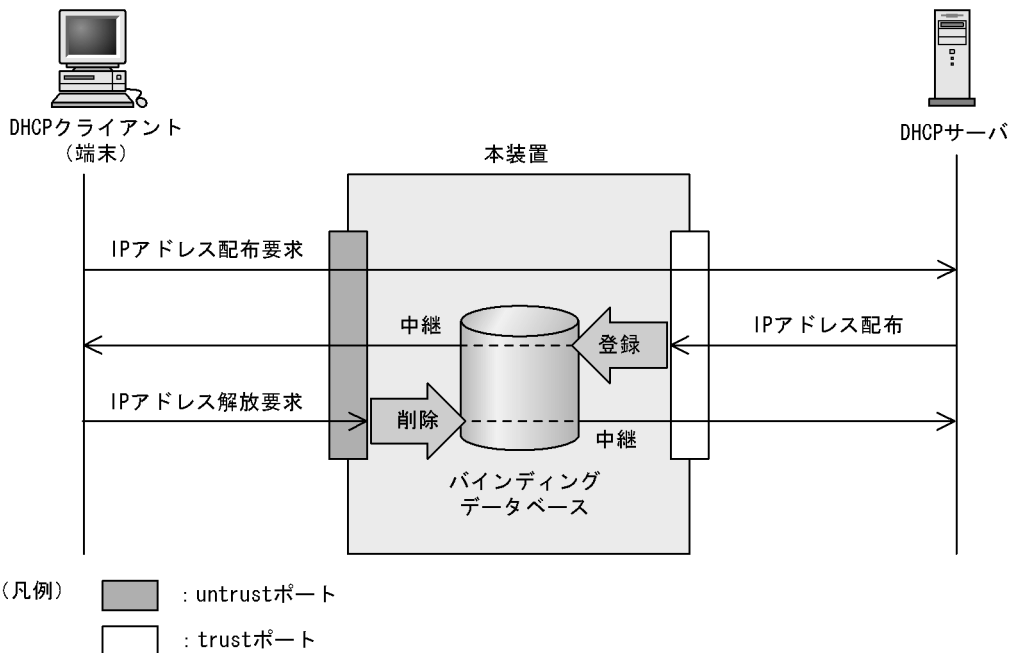
コンフィグレーションコマンド `ip dhcp snooping` で DHCP snooping を有効にすると、デフォルトですべてのポートが untrust ポートになります。DHCP サーバへ接続するポートを trust ポートとして設定してください。trust ポートはコンフィグレーションコマンド `ip dhcp snooping trust` で設定できます。

なお、DHCP snooping では、コンフィグレーションコマンド `ip dhcp snooping vlan` で指定した VLAN を監視対象にします。

(2) 端末情報の学習

端末情報の学習の動作概要を次の図に示します。

図 15-3 端末情報の学習の動作概要



trust ポートでは、受信した DHCP サーバからのパケットを監視し、IP アドレスが配布された場合にはバインディングデータベースに端末情報を登録します。

untrust ポートでは、受信した DHCP クライアントからのパケットを監視し、IP アドレスの解放要求の場合にはバインディングデータベースから端末情報を削除します。

バインディングデータベースの登録には、次の二つの種類があります。

- **ダイナミック登録**
 DHCP サーバから IP アドレスが配布されたときに登録します。
 通常は、ダイナミック登録によって端末情報を登録します。
- **スタティック登録**
 コンフィグレーションコマンド ip source binding で登録します。
 スタティック登録は、untrust ポートに固定 IP アドレスを持つ部門サーバなどを接続するときに利用します。バインディングデータベースに端末情報をスタティック登録することで通信を許可できます。

バインディングデータベースに登録する端末情報を次の表に示します。

表 15-2 バインディングデータベースに登録する端末情報

項目	ダイナミック登録	スタティック登録
端末の MAC アドレス	DHCP クライアントの MAC アドレス	固定 IP アドレスを持つ端末の MAC アドレス
端末の IP アドレス	DHCP サーバから配布された IP アドレス	固定 IP アドレスを持つ端末の IP アドレス
	次に示す範囲が有効	
	<ul style="list-style-type: none"> • 1.0.0.0 ~ 126.255.255.255 • 128.0.0.0 ~ 223.255.255.255 	
端末が所属する VLAN	端末を接続するポートまたはチャンネルグループの所属する VLAN ID	
端末を接続するポート番号	端末を接続するポート番号またはチャンネルグループ番号	

項目	ダイナミック登録	スタティック登録
エージング時間	エージングによってエントリを削除するまでの時間 なお、DHCP サーバから配布された IP アドレスのリース時間を適用します。	エージング対象外

(3) バインディングデータベースの保存

コンフィグレーションの設定によって、バインディングデータベースの保存および装置再起動時の復元ができます。

(a) バインディングデータベースの保存の動作条件

バインディングデータベースを保存するには、コンフィグレーションコマンド `ip dhcp snooping database url` を設定します。

実際に保存が開始されるのは、コンフィグレーションで設定された書き込み待ち時間満了時です。

(b) 書き込み待ち時間満了時の保存

書き込み待ち時間とは、バインディングデータベース保存時の、保存契機から書き込むまでの待ち時間です。次のどれかを保存契機としてタイマを開始し、タイマが満了した時点で指定した保存先へ保存します。

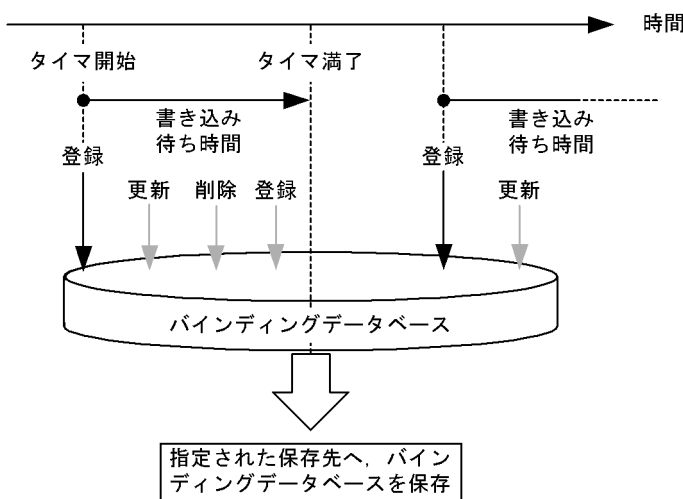
- ダイナミックのバインディングデータベースの登録，更新，または削除時
- コンフィグレーションコマンド `ip dhcp snooping database url` 設定時（保存先の変更を含む）
- 運用コマンド `clear ip dhcp snooping binding` 実行時

書き込み待ち時間は、コンフィグレーションコマンド `ip dhcp snooping database write-delay` で設定できます。

これらの保存契機で書き込み待ち時間のタイマを開始すると、タイマ満了までタイマは停止しません。この間にバインディングデータベースの登録，更新，または削除が発生してもタイマは再開しません。

保存契機と書き込み待ち時間との関係を次の図に示します。なお、この図ではバインディングデータベースへの登録を保存契機としています。

図 15-4 保存契機と書き込み待ち時間との関係



(c) バインディングデータベースの保存先

保存先には、内蔵フラッシュメモリとMCのどちらかを選択できます。保存先はコンフィグレーションコマンド ip dhcp snooping database url で設定します。

保存対象は、書き込み時点の全エントリです。また、次の書き込み時には上書きされます。

(d) 保存したバインディングデータベースの復元

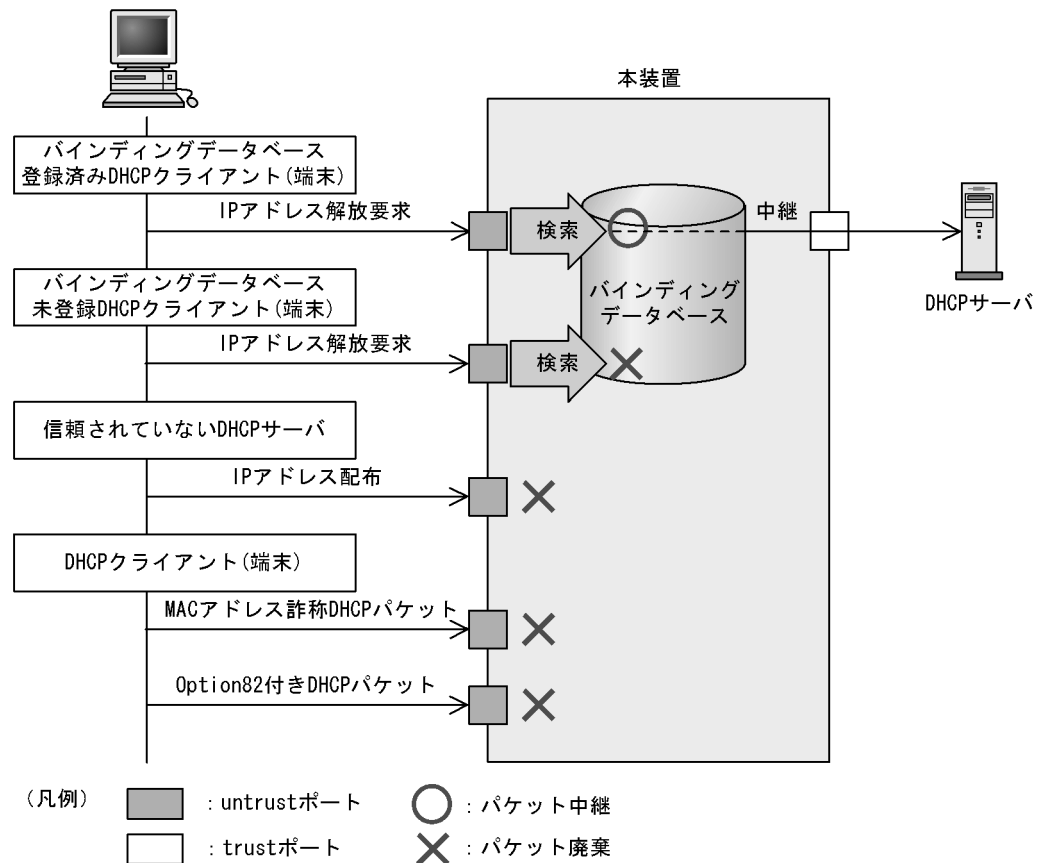
保存したバインディングデータベースは、装置起動時に復元します。復元には、装置起動時に次の条件をどちらも満たしている必要があります。

- コンフィグレーションコマンド ip dhcp snooping database url で保存先が設定されている
- 保存先がMCの場合、保存したファイルのMCが挿入されている

(4) DHCP パケットの検査

DHCP パケット検査の動作概要を次の図に示します。

図 15-5 DHCP パケット検査の動作概要



untrust ポートに接続された端末を対象に DHCP パケットを監視し、次に示すアクセスを除外します。

- 信頼されていない DHCP サーバからの IP アドレス配布を抑制
untrust ポートで、信頼されていない DHCP サーバからの DHCP パケットを受信した場合、該当する DHCP パケットを廃棄します。これによって、信頼されていない DHCP サーバからの IP アドレス配布を抑制します。

- 信頼されていない DHCP クライアントからの IP アドレス解放を抑制
untrust ポートで、バインディングデータベース未登録の端末から IP アドレス解放要求を受信した場合、該当する DHCP パケットを廃棄します。これによって、DHCP サーバから IP アドレスを配布されていない端末からの IP アドレス解放を抑制します。
また、同様に IP アドレス重複検出通知、リース時間更新、およびオプション情報取得要求を受信したときも DHCP パケットを廃棄します。これによって、信頼されていない DHCP クライアントからの不正な IP アドレスの解放、IP アドレスの取得、およびオプションの取得を抑制します。
- MAC アドレスの詐称を抑制
untrust ポートで、受信した DHCP パケットの送信元 MAC アドレス (Source MAC Address) と、DHCP パケット内のクライアントハードウェアアドレス (chaddr) が不一致の場合、該当する DHCP パケットを廃棄します。これによって、MAC アドレスの詐称を抑制します。
- Option82 の詐称を抑制
untrust ポートで、受信した DHCP パケットに Option82 が付与されている場合、該当する DHCP パケットを廃棄します。これによって、Option82 の詐称を抑制します。

15.1.3 DHCP パケットの受信レート制限

DHCP snooping 有効時に、受信する DHCP パケットを監視するとき、設定した受信レートを越えた DHCP パケットを廃棄する機能です。

受信レートはコンフィグレーションコマンド `ip dhcp snooping limit rate` で設定します。本コマンドを設定していない場合は、受信レートを制限しません。

DHCP パケットの受信レート制限は、本装置が受信するすべての DHCP パケットを対象にします。

受信レートを越えた DHCP パケットは廃棄し、運用ログ情報を採取します。ただし、Trap は発行しません。なお、運用ログ情報は運用コマンド `show ip dhcp snooping logging` で確認できます。

(1) CPU に転送するパケット数

CPU に転送するパケット数を次に示します。

(a) AX6700S の場合

CPU に転送するパケット数は、運用系 BSU の枚数によって異なります。運用系 BSU 枚数別の、CPU に転送するパケットの最大数を次の表に示します。

表 15-3 CPU に転送するパケットの最大数

運用系 BSU 枚数	CPU に転送するパケットの最大数
1 枚	設定値の約 2 倍
2 枚	設定値の約 4 倍
3 枚	設定値の約 6 倍

(b) AX6600S の場合

CPU に転送するパケット数は、運用系 PSP の数によって異なります。運用系 PSP 数別の、CPU に転送するパケットの最大数を次の表に示します。

表 15-4 CPU に転送するパケットの最大数

運用系 PSP 数	CPU に転送するパケットの最大数
1	設定値
2	設定値の約 2 倍

(c) AX6300S の場合

CPU に転送するパケットの最大数は、運用系 MSU が 1 枚だけなので、設定値と同じになります。

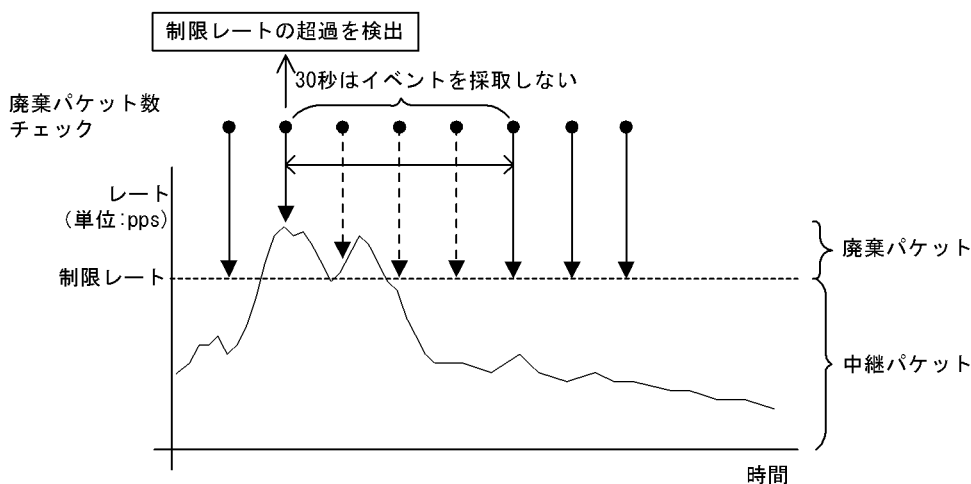
(2) 運用ログ情報の採取契機

運用ログ情報はコンフィグレーションで設定した受信レートを超過したときに、「超過検出」イベントを採取します。

「超過検出」イベントを採取後 30 秒間は、レート超過によってパケットを廃棄してもイベントを採取しません。

DHCP パケット受信レートの運用ログ情報の採取契機を次の図に示します。

図 15-6 DHCP パケット受信レートの運用ログ情報の採取契機



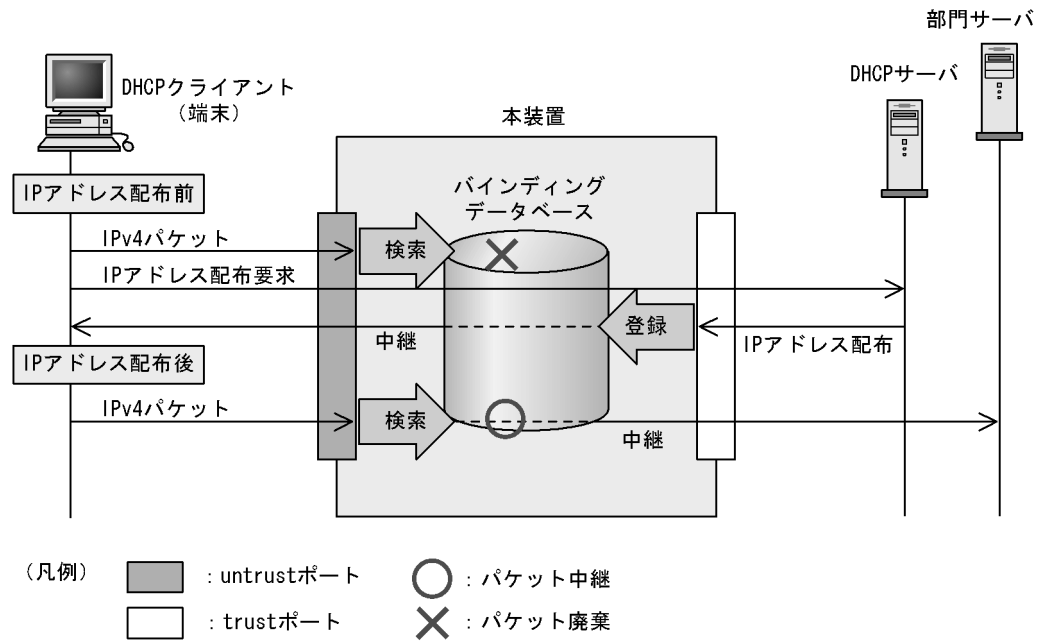
15.1.4 端末フィルタ

(1) 概要

端末フィルタは、本装置を通過する IPv4 パケットを監視して、信頼されていない端末からのアクセスを制限する機能です。

端末フィルタの動作概要を次の図に示します。

図 15-7 端末フィルタの動作概要



端末フィルタは、コンフィグレーションコマンド `ip verify source` でポート単位に設定できます。

なお、端末フィルタを使用する場合は、事前にフィルタ・QoS機能のフロー配分パターンの設定と、フロー検出拡張モード指定の有無に、端末フィルタに対応するものを設定する必要があります。

(2) IPv4 パケットの検査

untrustポートでIPv4パケットを受信した場合、バインディングデータベースとの整合性を検査し、未登録の端末であれば、該当するIPv4パケットを廃棄します。

端末フィルタの検査対象を次の表に示します。

表 15-5 端末フィルタの検査対象

端末フィルタ条件	IPv4 パケット			
	受信インタフェース		Ethernet ヘッダ	IP ヘッダ
	ポート	VLAN ID	送信元 MAC アドレス	送信元 IP アドレス
送信元 MAC アドレスだけ				-
送信元 IP アドレスだけ			-	
送信元 MAC アドレスと送信元 IP アドレス				

(凡例) : 検査対象 - : 検査対象外

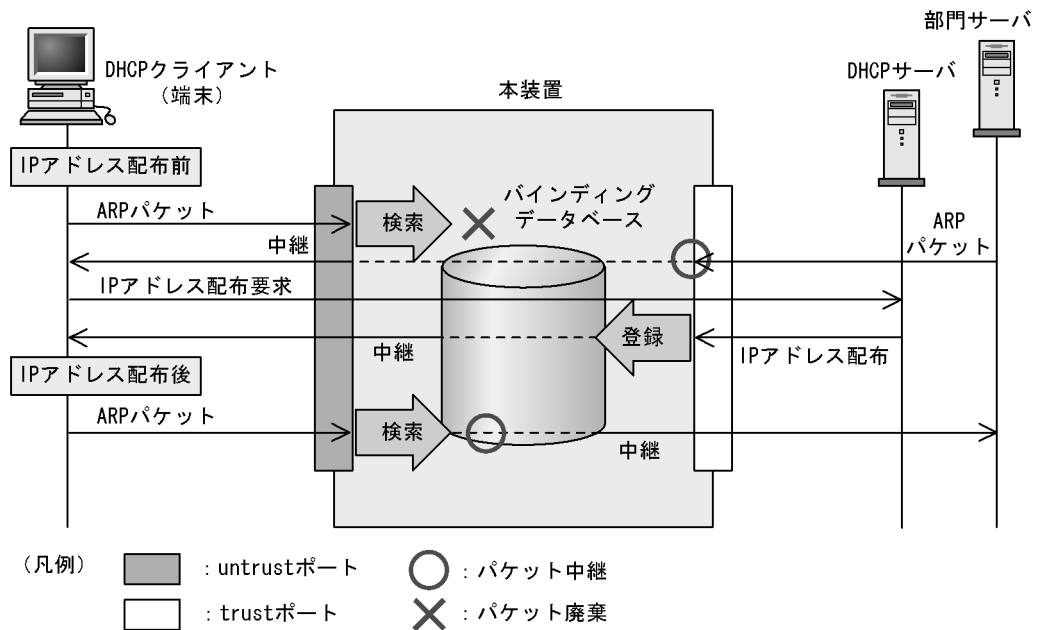
15.1.5 ダイナミック ARP 検査

(1) 概要

ダイナミック ARP 検査は、本装置を通過する ARP パケットを監視して、信頼されていない端末からの ARP パケットのアクセスを制限する機能です。

ダイナミック ARP 検査の動作概要を次の図に示します。

図 15-8 ダイナミック ARP 検査の動作概要



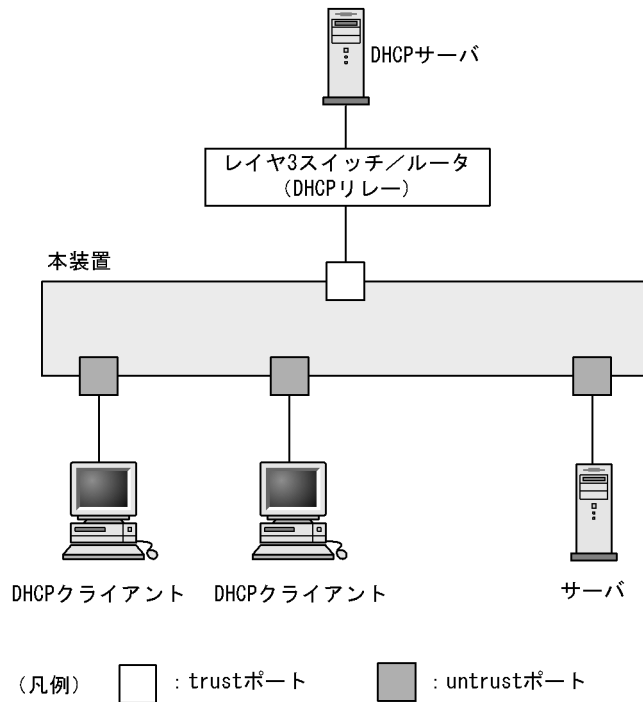
(2) ポートの種別

ダイナミック ARP 検査では DHCP snooping と同様に、ポートを次の種別に分類して、ARP パケットを監視します。

- trust ポート
DHCP サーバや部門サーバなど、信頼済みの端末を接続するポートを trust ポートと呼びます。
trust ポートで受信した ARP パケットは監視しません。
- untrust ポート
DHCP クライアントなど、信頼されていない端末を接続するポートを untrust ポートと呼びます。
DHCP サーバは接続しません。

ポートの種別を次の図に示します。

図 15-9 ポートの種別



コンフィグレーションコマンド `ip dhcp snooping` で DHCP snooping を有効にすると、デフォルトですべてのポートが untrust ポートになります。DHCP サーバへ接続するポートを trust ポートとして設定してください。trust ポートはコンフィグレーションコマンド `ip arp inspection trust` で設定できます。

なお、ダイナミック ARP 検査では、コンフィグレーションコマンド `ip arp inspection vlan` で指定した VLAN を監視対象にします。

通常の運用では、コンフィグレーションコマンド `ip dhcp snooping trust` および `ip arp inspection trust` で指定するポートを一致させることをお勧めします。

(3) ARP パケットの基本検査

untrust ポートで、ARP パケットを受信した場合、バインディングデータベースとの整合性を検査し、未登録の端末であれば、該当する ARP パケットを廃棄します。

基本検査の検査対象を次の表に示します。

表 15-6 基本検査の検査対象

ARP 種別	受信インタフェース		ARP パケット						
	ポート	VLAN ID	Ethernet ヘッダ		ARP ヘッダ				
			宛先 MAC アドレス	送信元 MAC アドレス	送信元 MAC アドレス	送信元 IP アドレス	宛先 MAC アドレス	宛先 IP アドレス	
Request			-	-				-	-
Reply			-	-				-	-

(凡例) □ : 検査対象 - : 検査対象外

(4) ARP パケットのオプション検査

untrust ポートで、受信した ARP パケット内のデータの整合性を検査します。

オプション検査は、コンフィグレーションコマンド `ip arp inspection validate` で設定します。

(a) 送信元 MAC アドレス検査 (src-mac 検査)

レイヤ 2 ヘッダに含まれる送信元 MAC アドレス (Source MAC) と、ARP ヘッダに含まれる送信元 MAC アドレス (Sender MAC Address) が同一であることを検査します。

ARP Request および ARP Reply の両方に対して検査します。

送信元 MAC アドレス検査の検査対象を次の表に示します。

表 15-7 送信元 MAC アドレス検査の検査対象

ARP 種別	受信インタフェース		ARP パケット					
	ポート	VLAN ID	Ethernet ヘッダ		ARP ヘッダ			
			宛先 MAC アドレス	送信元 MAC アドレス	送信元 MAC アドレス	送信元 IP アドレス	宛先 MAC アドレス	宛先 IP アドレス
Request	-	-	-	-	-	-	-	-
Reply	-	-	-	-	-	-	-	-

(凡例) : 検査対象 - : 検査対象外

(b) 宛先 MAC アドレス検査 (dst-mac 検査)

レイヤ 2 ヘッダに含まれる宛先 MAC アドレス (Destination MAC) と、ARP ヘッダに含まれる宛先 MAC アドレス (Target MAC Address) が同一であることを検査します。

ARP Reply に対してだけ検査します。

宛先 MAC アドレス検査の検査対象を次の表に示します。

表 15-8 宛先 MAC アドレス検査の検査対象

ARP 種別	受信インタフェース		ARP パケット					
	ポート	VLAN ID	Ethernet ヘッダ		ARP ヘッダ			
			宛先 MAC アドレス	送信元 MAC アドレス	送信元 MAC アドレス	送信元 IP アドレス	宛先 MAC アドレス	宛先 IP アドレス
Request	-	-	-	-	-	-	-	-
Reply	-	-	-	-	-	-	-	-

(凡例) : 検査対象 - : 検査対象外

(c) IP アドレス検査 (ip 検査)

ARP ヘッダに含まれる宛先 IP アドレス (Target IP Address) が次に示す範囲内であることを検査します。

- 1.0.0.0 ~ 126.255.255.255

- 128.0.0.0 ~ 223.255.255.255

ARP Reply に対してだけ検査します。

IP アドレス検査の検査対象を次の表に示します。

表 15-9 IP アドレス検査の検査対象

ARP 種別	受信インタフェース		ARP パケット						
	ポート	VLAN ID	Ethernet ヘッダ		ARP ヘッダ				
			宛先 MAC アドレス	送信元 MAC アドレス	送信元 MAC アドレス	送信元 IP アドレス	宛先 MAC アドレス	宛先 IP アドレス	
Request	-	-	-	-	-	-	-	-	-
Reply	-	-	-	-	-	-	-	-	-

(凡例) : 検査対象 - : 検査対象外

15.1.6 ARP パケットの受信レート制限

ダイナミック ARP 検査有効時に、受信する ARP パケットを監視するとき、設定した受信レートを越えた ARP パケットを廃棄する機能です。

受信レートはコンフィグレーションコマンド `ip arp inspection limit rate` で設定できます。本コマンドを設定していない場合は、受信レートを制限しません。

ARP パケットの受信レート制限は、本装置が受信するすべての ARP パケットを対象にします。

受信レートを越えた ARP パケットは廃棄し、運用ログ情報を採取します。ただし、Trap は発行しません。なお、運用ログ情報は運用コマンド `show ip dhcp snooping logging` で確認できます。

(1) CPU に転送するパケット数

CPU に転送するパケット数は、DHCP パケットの受信レート制限と同様です。

パケット数については、「15.1.3 DHCP パケットの受信レート制限 (1) CPU に転送するパケット数」を参照してください。

(2) 運用ログ情報の採取契機

運用ログ情報の採取契機は、DHCP パケットの受信レート制限と同様です。

採取契機については、「15.1.3 DHCP パケットの受信レート制限 (2) 運用ログ情報の採取契機」を参照してください。

15.1.7 DHCP snooping 使用時の注意事項

(1) レイヤ 2 スイッチ機能との共存

「コンフィグレーションガイド Vol.1 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) フロー配分パターン変更時の注意

オンラインでフロー配分パターンを変更した場合、DHCP snooping でバインディングデータベースにダイナミック登録されたエントリは削除されます。また、copy コマンドでフロー配分パターンの異なるバックアップコンフィギュレーションを反映した場合、ダイナミック登録されたエントリのうち収容条件に収まらない分は削除されます。

(3) フィルタ（ポリシーベーススイッチングおよびポリシーベースルーティングを含む）との共存

(a) DHCP snooping との共存

DHCP snooping とフィルタ（受信側）が共存する場合、フィルタ条件に関係なくアクセスリスト（受信側）の対象外となる、プロトコル名称 bootps および bootpc の両方のパケットを透過します。

(b) 端末フィルタとの共存

端末フィルタとフィルタ（受信側）は、同一ポート内で共存できません。

(4) レイヤ 2 認証との共存

(a) Web 認証との共存

「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。

(b) 認証専用 IPv4 アクセスリスト設定時の注意

DHCP snooping と認証専用 IPv4 アクセスリストが共存する場合、認証専用 IPv4 アクセスリストのフィルタ条件にプロトコル名称 bootps または bootpc のどちらか一方を設定しても、そのほかのフィルタ条件に関係なく、bootps および bootpc の両方のパケットを透過します。

(5) バインディングデータベースの保存と復元について

- コンフィギュレーションコマンド `ip dhcp snooping database url` が設定されていない（初期状態）場合、バインディングデータベースは保存されません。装置を停止または再起動すると登録済みのバインディングデータベースは消去されるため、DHCP クライアントからは通信できなくなります。通信できなくなった場合は、DHCP クライアント側で IP アドレスを解放および更新してください。例えば、Windows の場合、コマンドプロンプトから `ipconfig /release` を実行したあとに、`ipconfig /renew` を実行します。
これによって、バインディングデータベースに端末情報が再登録され、DHCP クライアントから通信できるようになります。
- 復元するエントリのうち、DHCP サーバのリース時間を満了したエントリは復元されません。バインディングデータベースが保存されたあと、装置の停止前または再起動前に時刻の設定を変更すると、装置の起動後にバインディングデータベースが正しく復元されないことがあります。
- コンフィギュレーションコマンド `ip source binding` でスタティック登録したエントリは、スタートアップコンフィギュレーションに従って復元されます。
- バインディングデータベースの保存先を MC にした場合は、装置の起動後の画面にプロンプトが表示されるまで MC を抜かないでください。

(6) DHCP パケットの受信レート制限について

- DHCP パケットの受信レート制限を使用した場合、マルチキャストのランデブーポイントで受信できる PIM-Register パケット数の上限値には、次の値が適用されます。
- IPv4 の場合、コンフィギュレーションコマンド `ip pim rate-limit register-receive` の指定値に関係なく、`ip pim rate-limit register-request` コマンドで設定した値

- IPv6 の場合、コンフィグレーションコマンド `ipv6 pim rate-limit register-receive` の指定値に関係なく、`ipv6 pim rate-limit register-request` コマンドで設定した値
- DHCP パケットの受信レート制限および ARP パケットの受信レート制限が共存する場合、DHCP パケットと ARP パケットの受信レートを合計した値で監視します。

(7) ダイナミック ARP 検査について

- ダイナミック ARP 検査は、次に示すコンフィグレーションを設定して、バインディングデータベースが生成されていることが必要です。
 - `ip dhcp snooping`
 - `ip dhcp snooping vlan`
- `ip source binding` でバインディングデータベースにスタティック登録されたエントリもダイナミック ARP 検査の対象となります。

(8) ARP パケットの受信レート制限について

- ARP パケットの受信レート制限を使用した場合、マルチキャストのランデブーポイントで受信できる PIM-Register パケット数の上限値には、次の値が適用されます。
 - IPv4 の場合、コンフィグレーションコマンド `ip pim rate-limit register-receive` の指定値に関係なく、`ip pim rate-limit register-request` コマンドで設定した値
 - IPv6 の場合、コンフィグレーションコマンド `ipv6 pim rate-limit register-receive` の指定値に関係なく、`ipv6 pim rate-limit register-request` コマンドで設定した値
- ARP パケットの受信レート制限および DHCP パケットの受信レート制限が共存する場合、ARP パケットと DHCP パケットの受信レートを合計した値で監視します。

15.2 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

DHCP 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 15-10 コンフィグレーションコマンド一覧

コマンド名	説明
ip arp inspection limit rate	本装置の ARP パケットの受信レートを設定します。
ip arp inspection trust	ダイナミック ARP 検査で信頼済みの端末を接続するポートを設定します。
ip arp inspection validate	ダイナミック ARP 検査のオプション検査を設定します。
ip arp inspection vlan	ダイナミック ARP 検査を使用する VLAN を設定します。
ip dhcp snooping	DHCP snooping を有効に設定します。
ip dhcp snooping database url	バインディングデータベースの保存先を設定します。
ip dhcp snooping database write-delay	バインディングデータベース保存時の書き込み待ち時間を設定します。
ip dhcp snooping information option allow-untrusted	DHCP パケットの Option82 の詐称検査を無効に設定します。
ip dhcp snooping limit rate	本装置の DHCP パケットの受信レート制限を設定します。
ip dhcp snooping logging enable	動作ログの syslog サーバへの出力を設定します。
ip dhcp snooping loglevel	動作ログメッセージで記録するメッセージレベルを指定します。
ip dhcp snooping trust	DHCP snooping で信頼済みの端末を接続するポートを設定します。
ip dhcp snooping verify mac-address	DHCP パケットの MAC アドレスの詐称検査を無効に設定します。
ip dhcp snooping vlan	DHCP snooping を使用する VLAN を設定します。
ip source binding	固定 IP アドレスを持つ端末をバインディングデータベースに登録します。
ip verify source	端末フィルタを使用するポートを設定します。

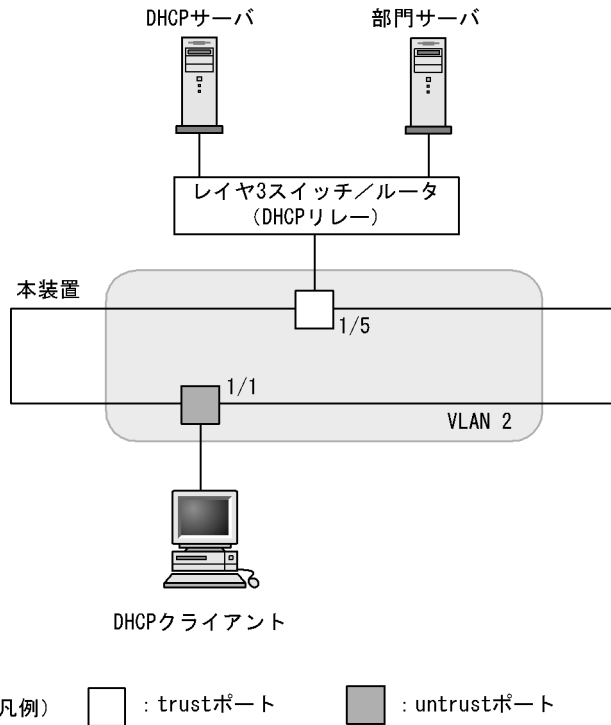
15.2.2 基本設定

DHCP snooping を使用するための基本的な設定について説明します。

なお、DHCP snooping を使用する場合は、事前にコンフィグレーションコマンド `fldm prefer` で、DHCP snooping に対応するフロー配分パターンおよびフロー検出拡張モードを設定しておく必要があります。

DHCP snooping の基本的な構成例を次の図に示します。

図 15-10 DHCP snooping の基本的な構成例



(1) DHCP snooping の有効設定

[設定のポイント]

装置としての DHCP snooping を有効にし、さらに DHCP snooping を有効にする VLAN を設定します。

[コマンドによる設定]

1. (config)# ip dhcp snooping

装置としての DHCP snooping を有効にします。

2. (config)# vlan 2

```
(config-vlan)# exit
```

```
(config)# ip dhcp snooping vlan 2
```

VLAN ID 2 で DHCP snooping を有効にします。本コマンドを指定しない VLAN では DHCP snooping は動作しません。

3. (config)# interface gigabitethernet 1/1

```
(config-if)# switchport mode access
```

```
(config-if)# switchport access vlan 2
```

```
(config-if)# exit
```

ポート 1/1 をアクセスポートとし、ポート 1/1 が所属する VLAN として VLAN ID 2 を設定します。

(2) DHCP snooping の trust ポートの設定

[設定のポイント]

DHCP サーバに接続するポート（「図 15-10 DHCP snooping の基本的な構成例」ではレイヤ 3 スイッチ/ルータと接続するポート）を trust ポートとして設定します。

[コマンドによる設定]

```
1. (config)# interface gigabitethernet 1/5
   (config-if)# ip dhcp snooping trust
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 2
   (config-if)# exit
```

ポート 1/5 を trust ポートとして設定します。そのほかのポートは untrust ポートとなります。また、ポート 1/5 をアクセスポートとし、ポート 1/5 が所属する VLAN として VLAN ID 2 を設定します。

(3) バインディングデータベースの保存先の設定

(a) 内蔵フラッシュメモリに保存する場合

[設定のポイント]

バインディングデータベースの保存先に内蔵フラッシュメモリを設定します。

[コマンドによる設定]

```
1. (config)# ip dhcp snooping database url flash
```

保存先として内蔵フラッシュメモリを設定します。

(b) MC に保存する場合

[設定のポイント]

バインディングデータベースの保存先に MC を設定します。MC の場合は保存するファイル名を設定できます。

[コマンドによる設定]

```
1. (config)# ip dhcp snooping database url mc dhcpsn-db
```

保存先として MC、および保存するファイル名として dhcpsn-db を設定します。

[注意事項]

保存先を MC にする場合は、本装置のメモリカードスロットに MC を挿入しておいてください。また、MC はアラクスラ製品をご使用ください。

(4) バインディングデータベースの保存先への書き込み待ち時間の設定

[設定のポイント]

バインディングデータベースの保存先への書き込み待ち時間を設定します。

[コマンドによる設定]

```
1. (config)# ip dhcp snooping database write-delay 3600
```

次のどれかを保存契機として、保存を開始するまでの時間を 3600 秒に設定します。

- ダイナミックのバインディングデータベースの登録、更新、および削除時
- コンフィグレーションコマンド ip dhcp snooping database url 設定時（保存先の変更を含む）
- 運用コマンド clear ip dhcp snooping binding 実行時

[注意事項]

次回の保存契機から本コマンドで設定した時間が運用に反映されます。

15.2.3 DHCP パケットの受信レート制限

DHCP パケットの受信レート制限を使用するための設定について説明します。

[設定のポイント]

本装置が端末から受信する DHCP パケットの受信レートを設定します。

[コマンドによる設定]

1. (config)# ip dhcp snooping limit rate 50
本装置の受信レートを 50 パケット / 秒に設定します。

15.2.4 端末フィルタ

端末フィルタを使用するための設定について説明します。

[設定のポイント]

DHCP クライアントを接続するポートに端末フィルタを設定します。

[コマンドによる設定]

1. (config)# interface gigabitethernet 1/1
(config-if)# ip verify source port-security
(config-if)# exit
ポート 1/1 に送信元 IP アドレスと送信元 MAC アドレスを端末フィルタ条件とする端末フィルタを設定します。

[注意事項]

trust ポートでコンフィグレーションコマンド ip verify source コマンドを設定しても、端末フィルタは無効です。また、DHCP snooping 有効時は、コンフィグレーションコマンド ip dhcp snooping vlan で設定されていない VLAN でも端末フィルタが有効となりますので注意してください。

15.2.5 ダイナミック ARP 検査

ダイナミック ARP 検査を使用するための設定について説明します。

(1) 基本設定

[設定のポイント]

ダイナミック ARP 検査の基本検査を有効にする VLAN を設定します。

[コマンドによる設定]

1. (config)# ip arp inspection vlan 2
VLAN ID 2 をダイナミック ARP 検査の対象に設定します。本コマンドを指定しない VLAN ではダイナミック ARP 検査は動作しません。

[注意事項]

- コンフィグレーションコマンド `ip dhcp snooping vlan` で設定している VLAN ID を指定してください。
- 本コマンドを設定した場合は、コンフィグレーションコマンド `ip source binding` で登録したバインディングデータベースのエントリも、ダイナミック ARP 検査の対象となります。
- 本コマンドを設定した VLAN に所属しているポートに対して、コンフィグレーションコマンド `ip arp inspection trust` を設定した場合は、そのポートはダイナミック ARP 検査の対象外となります。

(2) trust ポートの設定

[設定のポイント]

DHCP サーバに接続するポートを trust ポートとして設定します。

[コマンドによる設定]

1. `(config)# interface gigabitethernet 1/5`
`(config-if)# ip arp inspection trust`
`(config-if)# exit`

ポート 1/5 を trust ポートとして設定します。そのほかのポートは untrust ポートとなります。

[注意事項]

本コマンドを設定したポートでは、ダイナミック ARP 検査の検査対象 VLAN に所属していても、ダイナミック ARP 検査の対象外となります。

(3) オプション検査の設定

[設定のポイント]

本装置のダイナミック ARP 検査のオプション検査として送信元 MAC アドレス検査 (src-mac 検査) を有効に設定します。

[コマンドによる設定]

1. `(config)# ip arp inspection validate src-mac`

オプション検査として送信元 MAC アドレス検査 (src-mac 検査) を有効に設定します。

15.2.6 ARP パケットの受信レート制限

ARP パケットの受信レート制限を使用するための設定について説明します。

[設定のポイント]

本装置が受信する ARP パケットの受信レートを設定します。

[コマンドによる設定]

1. `(config)# ip arp inspection limit rate 100`

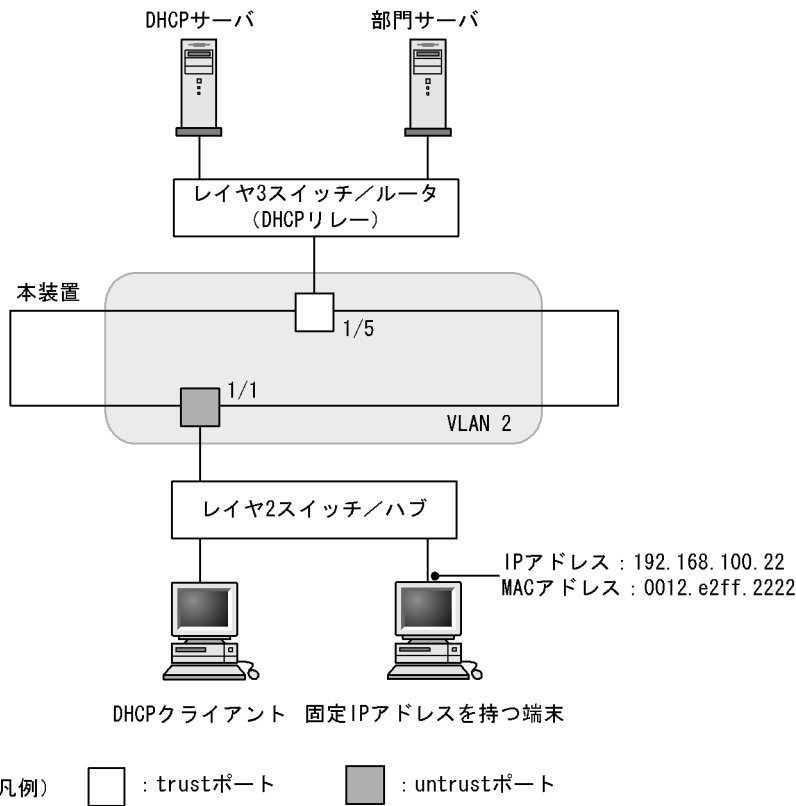
本装置の受信レートを 100 パケット / 秒に設定します。

15.2.7 固定 IP アドレスを持つ端末を接続した場合

固定 IP アドレスを持つ端末を接続する場合の設定について説明します。

固定 IP アドレスを持つ端末を接続した場合の構成例を次の図に示します。

図 15-11 固定 IP アドレスを持つ端末を接続した場合の構成例



DHCP snooping の設定は、「15.2.2 基本設定」と同様です。本例では、固定 IP アドレスを持つ端末を untrust ポートに接続するため、バインディングデータベースに固定 IP アドレスを持つ端末のスタティック登録が必要です。

[設定のポイント]

固定 IP アドレスを持つ端末の端末情報を、バインディングデータベースにスタティック登録します。

[コマンドによる設定]

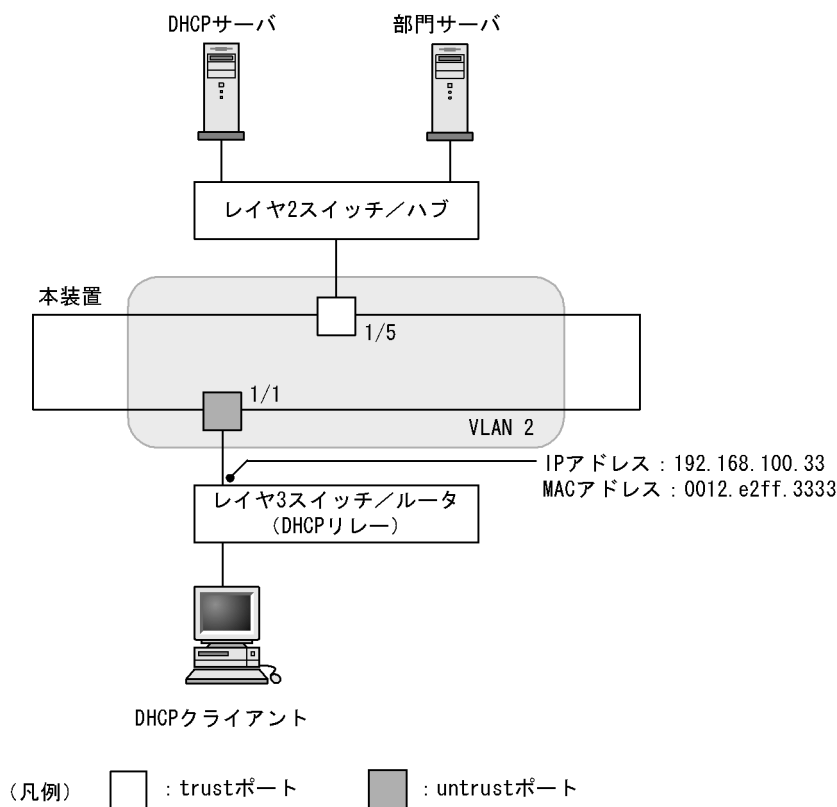
1. (config)# ip source binding 0012.e2ff.2222 vlan 2 192.168.100.22 interface gigabitethernet 1/1
 端末の MAC アドレス、端末が所属する VLAN (VLAN ID)、端末の IP アドレス、および端末が接続されているポート番号を、バインディングデータベースに設定します。

15.2.8 本装置の配下に DHCP リレーが接続された場合

本装置の配下に DHCP リレーを接続した場合、本装置でパケットを中継できるように設定します。

本装置の配下に DHCP リレーを接続した場合の構成例を次の図に示します。

図 15-12 本装置の配下に DHCP リレーを接続した場合の構成例



本装置の DHCP snooping 設定は、「15.2.2 基本設定」、「15.2.4 端末フィルタ」、および「15.2.5 ダイナミック ARP 検査」と同様です。

本例では、そのままでは DHCP クライアントからの DHCP パケットおよび IPv4 パケットが中継できません。また、レイヤ 3 スイッチ/ルータからの ARP パケットも中継できません。

パケットを中継するためには、本装置で DHCP パケットの中継を許可する設定、IPv4 パケットの中継を許可する設定、および ARP パケットの中継を許可する設定が必要です。

(1) DHCP パケットの中継を許可する設定

[設定のポイント]

DHCP クライアントからのパケットは、レイヤ 3 スイッチ/ルータ (DHCP リレー) によって送信元 MAC アドレスが書き換えられているため、DHCP パケットの MAC アドレス詐称検査を無効に設定します。

[コマンドによる設定]

1. (config)# no ip dhcp snooping verify mac-address
untrust ポートの MAC アドレス詐称検査を無効に設定します。

[注意事項]

本コマンドが設定されていない場合、MAC アドレス詐称検査をするため、untrust ポートに DHCP リレーを接続できません。

(2) IPv4 パケットの中継を許可する設定

[設定のポイント]

DHCP クライアントからのパケットは、レイヤ 3 スイッチ/ルータ (DHCP リレー) によって送信元 MAC アドレスが書き換えられているため、端末フィルタ条件に送信元 IP アドレスだけを設定します。

[コマンドによる設定]

```
1. (config)# interface gigabitethernet 1/1
   (config-if)# ip verify source
   (config-if)# exit
```

ポート 1/1 に、端末フィルタ条件として送信元 IP アドレスだけを設定します。

(3) ARP パケットの中継を許可する設定

ARP パケットの中継を許可する設定は固定 IP アドレスを持つ端末を接続した場合と同様です。

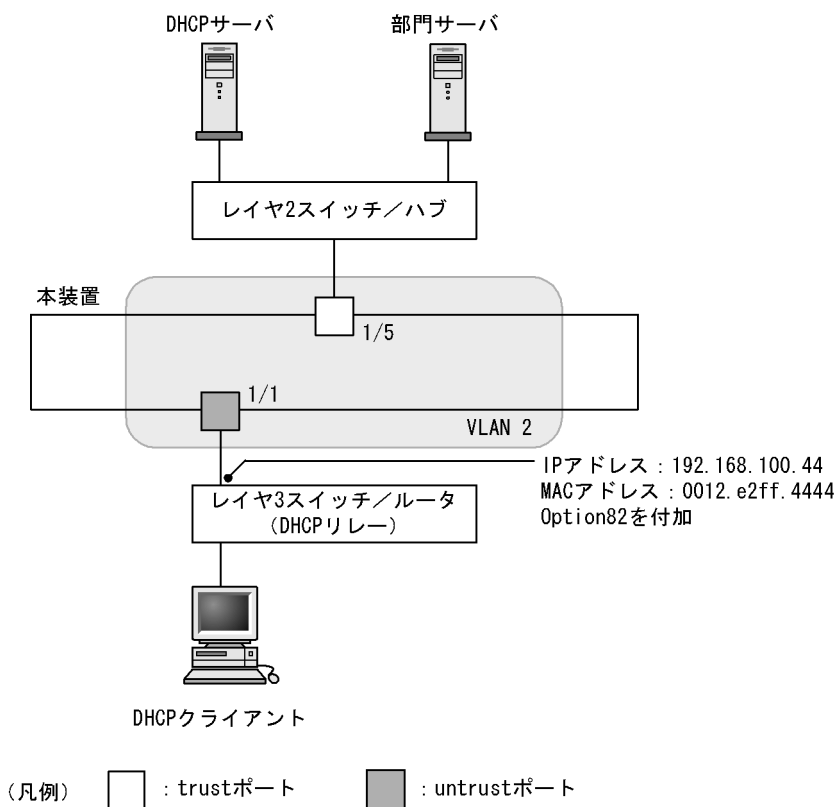
設定については、「15.2.7 固定 IP アドレスを持つ端末を接続した場合」を参照してください。

15.2.9 本装置の配下に Option82 を付与する DHCP リレーが接続された場合

本装置の配下に Option82 を付与する DHCP リレーを接続した場合、本装置でパケットを中継できるように設定します。

本装置の配下に Option82 を付与する DHCP リレーを接続した場合の構成例を次の図に示します。

図 15-13 本装置の配下に Option82 を付与する DHCP リレーを接続した場合の構成例



本装置の DHCP snooping 設定は「15.2.2 基本設定」、「15.2.4 端末フィルタ」、および「15.2.5 ダイナミック ARP 検査」と同様です。

本例では、そのままでは DHCP クライアントからの DHCP パケットおよび IPv4 パケットが中継できません。また、レイヤ 3 スイッチ/ルータからの ARP パケットも中継できません。

パケットを中継するためには、本装置で DHCP パケットの中継を許可する設定、IPv4 パケットの中継を許可する設定、および ARP パケットの中継を許可する設定が必要です。また、DHCP リレーが Option82 を付与する場合、Option82 付き DHCP パケットの中継を許可する設定も必要です。

(1) DHCP パケットの中継を許可する設定

DHCP パケットの中継を許可する設定は本装置の配下に DHCP リレーが接続された場合と同様です。

設定については、「15.2.8 本装置の配下に DHCP リレーが接続された場合 (1) DHCP パケットの中継を許可する設定」を参照してください。

(2) IPv4 パケットの中継を許可する設定

DHCP パケットの中継を許可する設定は本装置の配下に DHCP リレーが接続された場合と同様です。

設定については、「15.2.8 本装置の配下に DHCP リレーが接続された場合 (2) IPv4 パケットの中継を許可する設定」を参照してください。

(3) ARP パケットの中継を許可する設定

ARP パケットの中継を許可する設定は固定 IP アドレスを持つ端末を接続した場合と同様です。

設定については、「15.2.7 固定 IP アドレスを持つ端末を接続した場合」を参照してください。

(4) Option82 付き DHCP パケットの中継を許可する設定

[設定のポイント]

DHCP パケットの Option82 の詐称検査を無効に設定します。

[コマンドによる設定]

1. (config)# ip dhcp snooping information option allow-untrusted
untrust ポートの Option82 の詐称検査を無効に設定します。

15.2.10 syslog サーバへの出力

[設定のポイント]

動作ログを syslog サーバに出力する設定をします。

[コマンドによる設定]

1. (config)# ip dhcp snooping logging enable
動作ログを syslog サーバに出力する設定をします。
2. (config)# logging event-kind dsn
syslog サーバに送信対象とするログ情報の、イベント種別に DHCP snooping を設定します。

15.3 オペレーション

15.3.1 運用コマンド一覧

DHCP snooping の運用コマンド一覧を次の表に示します。

表 15-11 運用コマンド一覧

コマンド名	説明
show ip dhcp snooping binding	バインディングデータベース情報を表示します。
clear ip dhcp snooping binding	バインディングデータベース情報をクリアします。
show ip dhcp snooping statistics	統計情報を表示します。
clear ip dhcp snooping statistics	統計情報をクリアします。
show ip arp inspection statistics	ダイナミック ARP 検査の統計情報を表示します。
clear ip arp inspection statistics	ダイナミック ARP 検査の統計情報をクリアします。
show ip dhcp snooping logging	プログラムで採取しているログメッセージを表示します。
clear ip dhcp snooping logging	プログラムで採取しているログメッセージをクリアします。
restart dhcp snooping	プログラムを再起動します。
dump protocols dhcp snooping	プログラムで採取しているログや内部情報をファイルへ出力します。

15.3.2 DHCP snooping バインディングデータベースの確認

バインディングデータベース情報を show ip dhcp snooping binding コマンドで表示します。端末の MAC アドレス, IP アドレス, バインディングデータベースのエージング時間などを表示します。

show ip dhcp snooping binding コマンドの実行結果を次の図に示します。

図 15-14 show ip dhcp snooping binding の実行結果

```
> show ip dhcp snooping binding
Date 2010/04/20 12:00:00 UTC
Agent URL: flash
Last succeeded time: 2010/04/20 11:50:00 UTC
Total Bindings Used/Max      :      5/   500
Total Source guard Used/Max:      2/   500

Bindings: 5
MAC Address      IP Address      Expire (min)   Type           VLAN   Port
0012.e287.0001  192.168.0.201   -              static*        1      1/1
0012.e287.0002  192.168.0.204   1439           dynamic        2      1/4
0012.e287.0003  192.168.0.203   -              static         3      1/3
0012.e287.0004  192.168.0.202   3666           dynamic        4      ChGr:2
0012.e2be.b0fb  192.168.100.11  59             dynamic*       12     1/11
>
```

15.3.3 DHCP snooping 統計情報の確認

DHCP snooping 統計情報を show ip dhcp snooping statistics コマンドで表示します。untrust ポートで受信した DHCP 総パケット数, インタフェースごとの受信した DHCP パケット数, およびフィルタした DHCP パケット数を表示します。

show ip dhcp snooping statistics コマンドの実行結果を次の図に示します。

図 15-15 show ip dhcp snooping statistics の実行結果

```
> show ip dhcp snooping statistics
Date 2010/04/20 12:00:00 UTC
Database Exceeded: 0
Total DHCP Packets: 8995
Port          Recv          Filter
1/1           170           170
1/3           1789          10
:
1/25          0             0
ChGr:1        3646          2457
>
```

15.3.4 ダイナミック ARP 検査の確認

(1) ダイナミック ARP 検査統計情報の確認

ダイナミック ARP 検査の統計情報を show ip arp inspection statistics コマンドで表示します。中継した ARP パケット数、廃棄した ARP パケット数、および廃棄 ARP パケット数の内訳を表示します。

show ip arp inspection statistics コマンドの実行結果を次の図に示します。

図 15-16 show ip arp inspection statistics の実行結果

```
> show ip arp inspection statistics
Date 2010/04/20 12:00:00 UTC
Port          Forwarded      Dropped ( DB mismatch      Invalid )
1/1           0              15 (          15           0 )
1/2           584           883 (          883           0 )
1/3           0              0 (           0           0 )
:
ChGr:2        170           53 (           53           0 )
>
```

15.3.5 DHCP snooping ログメッセージの確認

DHCP snooping ログメッセージを show ip dhcp snooping logging コマンドで表示します。バインディングデータベースの更新、端末フィルタの更新、不正な DHCP サーバの検出、不正な DHCP パケットの廃棄、または ARP パケットの廃棄などのログメッセージを表示します。

show ip dhcp snooping logging コマンドの実行結果を次の図に示します。

図 15-17 show ip dhcp snooping logging の実行結果

```
> show ip dhcp snooping logging
Date 2010/04/20 12:00:00 UTC
Apr 20 11:00:00 ID=2201 NOTICE DHCP server packets were received at an untrust
port (1/2/1/0012.e2ff.fe01/192.168.100.254) .
>
```


16 電源機構 (P S) の冗長化

この章では本装置の電源について説明します。

16.1 解説

16.2 PS の状態確認，および PS に関するコンフィグレーション

16.1 解説

本装置は装置モデルごとに必要な電源個数が異なります。装置と電源数の対応について次の表に示します。

表 16-1 PS（AC 電源）必要実装数

装置モデル	PS 基本構成時	PS 冗長時
AX6708S	4	8
AX6604S	2	4
AX6608S	2	4
AX6304S	2	4
AX6308S	2	4

表 16-2 PS（DC 電源）必要実装数

装置モデル	PS 基本構成時	PS 冗長時
AX6708S	2	4
AX6604S	1	2
AX6608S	1	2
AX6304S	1	2
AX6308S	1	2

PS 基本構成時を下回る電源数では、装置を起動できません。また、運用中に電源障害が発生した場合など、動作可能な電源数が下回ると、装置を正常に運用できなくなります。

AC 電源と DC 電源は同一筐体に混載することはできません。

PS 冗長構成時の電源を実装して運用している場合には、電源に障害が発生し電力供給が停止したとしても、自動的に残りの電源で負荷バランスを行い、安定供給できます。また、障害となった電源は装置を運用したままで交換できます。

PS の実装数が基本構成時の実装数を超え、PS 冗長時の実装数に満たない場合は、冗長電源部の異常として取り扱います。

16.2 PS の状態確認 , および PS に関するコンフィグレーション

16.2.1 コンフィグレーション・運用コマンド一覧

PS 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 16-3 コンフィグレーションコマンド一覧

コマンド名	説明
power redundancy-mode	PS 冗長構成でなくなった契機を警告します。

表 16-4 運用コマンド一覧

コマンド名	説明
show system	装置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。

16.2.2 PS 冗長構成で運用する場合のコンフィグレーション

本装置は , PS 冗長構成時の必要電源数を下回る実装であった場合 , ログを出力し警告する機能があり , 冗長構成でなくなった状態の管理ができます。この機能を使用する場合は , power redundancy-mode edundancy-check コマンドを使用してください。立ち上げ時に冗長電源が未実装であった場合 , または運用中に電源を抜去した場合に ' E8 PS 00000102 2200:000000000000 Power unit isn't redundantly mounted. (電源が冗長実装ではありません) ' のログを出力します。

[コマンドによる設定]

1. (config)# power redundancy-mode redundancy-check

コンフィグレーションモードで , PS 冗長構成でなくなった場合に警告を出力するように設定します。

16.2.3 PS の状態確認

show system コマンドによって PS の状態を確認できます。また , power redundancy-mode コンフィグレーションで PS の冗長構成をチェックするように設定されているかどうか , show system コマンドによって確認できます。

PS の入れ替え , 増設 , および移設作業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 , 注意事項を遵守してください。

図 16-1 PS の状態確認

```
> show system
Date 2006/03/13 06:35:27 UTC
System: AX6304S, OS-SE Ver. 10.3
Node : Name=System Name
      :
      :
      Power redundancy-mode : check is executed
      PS1 = active
      PS2 = active
      PS3 = active
      PS4 = active
      :
      :
```

17 BCU/CSU/MSU の冗長化

この章では、基本制御機構（BCU）、制御スイッチング機構（CSU）および管理スイッチング機構（MSU）の冗長構成について説明します。

17.1 解説

17.2 オペレーション

17.1 解説

17.1.1 冗長化時の装置構成

基本制御機構 (BCU), 制御スイッチング機構 (CSU) または管理スイッチング機構 (MSU) を冗長化 (二重化) する場合, AX6700S シリーズでは BCU を, AX6600S シリーズでは CSU を, AX6300S シリーズでは MSU をそれぞれ 2 枚実装します。2 枚のボードそれぞれが運用系システム, 待機系システムとして動作します。二重化構成では装置の管理機能を持つシステム部位の二重化と, 装置を構成するボード間の通信インタフェースを冗長化することができ, 障害に対する信頼性を高めることができます。運用系システムに障害が発生した場合, 運用系と待機系の切り替えを行い, 待機系システムが新運用系システムとなって運用を始めます。

シリーズごとの冗長構成でのインタフェースを次の図に示します。

図 17-1 BCU-BSU 間の冗長構成でのインタフェース

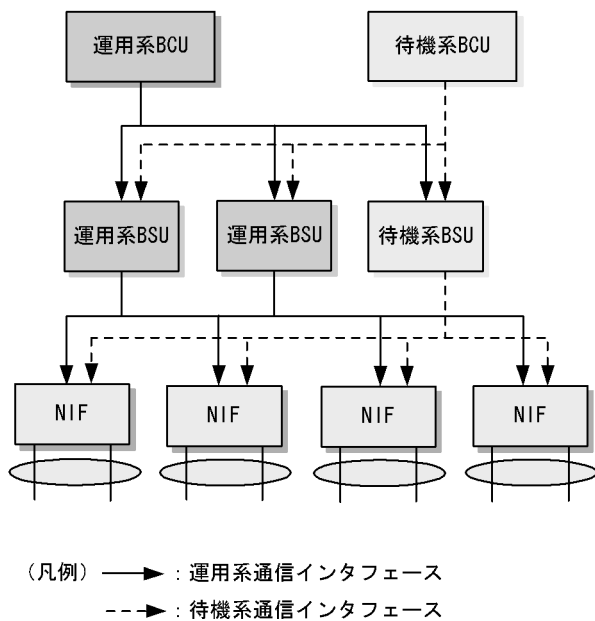


図 17-2 CSU-NIF 間の冗長構成でのインタフェース

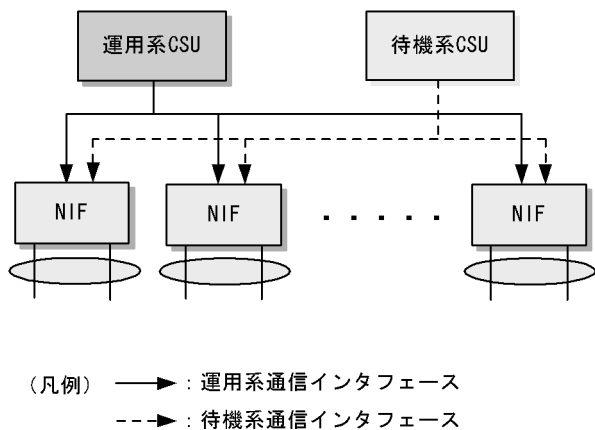
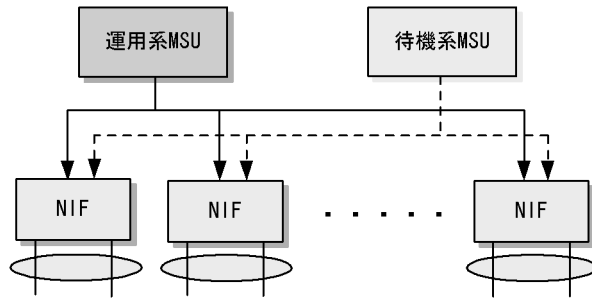


図 17-3 MSU-NIF 間の冗長構成でのインターフェース



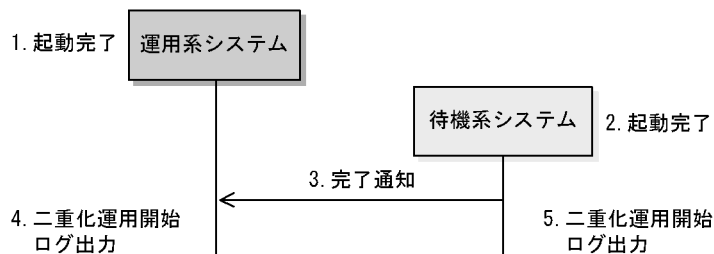
(凡例) —▶ : 運用系通信インターフェース
 - -▶ : 待機系通信インターフェース

17.1.2 冗長構成での動作

本装置では、AX6700S では BCU ボード、AX6600S では CSU ボード、AX6300S では MSU ボードの実装枚数が 1 枚であれば一重化で動作します。実装枚数が 2 枚であれば待機系システムの起動が完了し、系切替が可能な状態になったとき、' System mode changed from simplex to duplex. ' のログを表示して、二重化での運用を開始します。実装枚数が 2 枚でも待機系システムが起動完了していない場合、一重化で動作します。一重化から二重化へ、または二重化から一重化へ構成が変化しても通信への影響はありません。

一重化から二重化で運用開始するまでの流れを次の図に示します。

図 17-4 二重化運用開始時の動作



(図の説明)

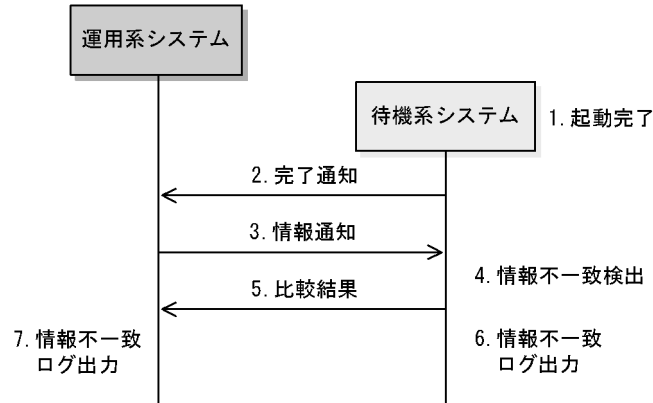
1. 運用系システムだけで一重化運用
2. 待機系システムの起動が完了
3. 待機系システムの起動が完了した契機を運用系システムへ通知
4. 3. の通知を受け取り、運用系システムは二重化で運用が開始された事象をログ表示
5. 3. の通知を送出し、待機系システムは二重化で運用が開始された事象をログ表示

電源を入れた後、冗長構成で運用を開始すると、AX6700S シリーズでは BCU1 が運用系として動作し、BCU2 は待機系として運用を開始します。AX6600S シリーズでは CSU1 が運用系として動作し、CSU2 は待機系として運用を開始します。AX6300S シリーズでは MSU1 が運用系として動作し、MSU2 は待機系として運用を開始します。これらの実装位置については、マニュアル「コンフィグレーションガイド Vol.1 2.1 本装置のモデル」を参照してください。

17.1.3 装置起動時の待機系および運用系との整合性確認

系切替前後で差分がないようにするためには、幾つかの情報を両系間で合わせておく必要があります。そのため、本装置では、装置起動時に待機系は運用系から「表 17-2 運用中に同期する管理情報」に示す情報を取得して比較します。比較した情報に差異がある場合は、ログ出力によって警告します。情報の比較が行われ不一致を検出するまでの流れを次の図に示します。

図 17-5 装置起動時の情報比較



(図の説明)

1. 待機系システムの起動が完了
2. 待機系システムの起動が完了した契機を運用系システムへ通知
3. 運用系システムの各種情報を待機系システムへ通知
4. 待機系システムは 3. の情報と自系の情報を比較し、情報不一致を検出
5. 待機系システムは比較結果を運用系システムへ通知
6. 待機系システムは 4. で情報不一致を検出したため、情報不一致ログを出力
7. 運用系システムは 5. の比較結果に従い、情報不一致ログを出力

立ち上げ時に行う両系間の比較情報を次の表に示します。

表 17-1 立ち上げ時に行う両系間の比較情報の一覧

項番	立ち上げ時に両系間で整合性確認を行う情報
1	ソフトウェアのバージョン情報
2	ライセンスキー情報
3	コンフィグレーション

17.1.4 運用系システムの管理情報の同期および同期契機

運用系と待機系の間で同期するシステムの管理情報を次の表に示します。

同期を行った情報は、待機系側の動作にも適用され、系切替後も動作矛盾が発生することなく、運用が可能となります。

表 17-2 運用中に同期する管理情報

管理情報	同期が行われる契機
コンフィグレーション	<ul style="list-style-type: none"> • コンフィグレーションの保存操作 (save , copy , erase) • synchronize コマンド実行時 • 冗長化運用開始時 ¹ • コンフィグレーション変更時 ²
ユーザアカウント情報	<ul style="list-style-type: none"> • ユーザアカウント情報の変更 (adduser , rmuser , password , clear password) • synchronize コマンド実行時
ライセンスキー情報	<ul style="list-style-type: none"> • synchronize コマンド実行時 ³
ホームディレクトリ情報	<ul style="list-style-type: none"> • synchronize コマンド実行時

注 1

ランニングコンフィグレーションファイル (running-config) を同期します。スタートアップコンフィグレーションファイル (startup-config) は同期しません。

注 2

変更を行ったコンフィグレーションだけを同期します。

注 3

同期したライセンスキーを有効にするには待機系を再起動してください。

17.1.5 系切替時の通信無停止対応機能一覧

次の表に通信無停止機能をサポートする機能を示します。無停止機能をサポートしている機能については、系切替時においても各機能が無停止で動作するため、系切替後も通信を維持することができます。通信無停止機能を未サポートの機能については系切替後再学習を行うため、ネットワーク情報が再構築されるまでの間通信が中断します。

表 17-3 系切替時の無停止機能サポート状況

分類	機能	サポート
ネットワークインタフェース	全 NIF 共通	
リンクアグリゲーション	スタティック	
	LACP	×
	スタンバイリンク リンクダウンモード	×
	スタンバイリンク 非リンクダウンモード	
	異速度混在モード	×
レイヤ 2 中継	MAC アドレス学習	
	ポート VLAN	
	プロトコル VLAN	
	MAC VLAN	
	VLAN Tag 変換	
	VLAN トンネリング	
	BPDU フォワーディング	
	EAPOL フォワーディング	
	ポリシーベーススイッチング	1

17. BCU/CSU/MSU の冗長化

分類	機能	サポート
スパンニングツリー	PVST+	×
	シングルスパンニングツリー	×
	マルチプルスパンニングツリー	×
リングプロトコル	Ring Protocol	×
IGMP/MLD snooping	IGMP snooping	
	MLD snooping	
フィルタ・QoS	フィルタ・QoS	
レイヤ 2 認証	IEEE802.1X	
	Web 認証	
	MAC 認証	
	認証 VLAN	
セキュリティ	DHCP snooping	
高信頼化機能	GSRP	×
	VRRP	×
	IEEE802.3ah/UDLD	
	L2 ループ検知	
IPv4 パケット中継	IPv4, ARP	
	ポリシーベースルーティング	2
	IPv4 DHCP リレー	
	IPv4 DHCP サーバ	
IPv4 ユニキャストルーティングプロトコル	スタティックルーティング	
	RIP, RIP2	×
	OSPF	3
	BGP4	3
IPv4 マルチキャストルーティングプロトコル	PIM-SM	4
	PIM-SSM	×
	PIM-DM	×
IPv6 パケット中継	IPv6, NDP	
	ポリシーベースルーティング	×
	IPv6 DHCP リレー	
	IPv6 DHCP サーバ	
IPv6 ユニキャストルーティングプロトコル	スタティックルーティング	
	RIPng	×
	OSPFv3	3
	BGP4+	3
IPv6 マルチキャストルーティングプロトコル	PIM-SM	×
	PIM-SSM	5

(凡例) : サポート × : 未サポート

- 注 1
 コンフィグレーションコマンド `policy-switch-list default-aging-interval` で指定した時間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。
- 注 2
 ポリシーベースルーティンググループでは、コンフィグレーションコマンド `policy-list default-aging-interval` で指定した時間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。
- 注 3
 Graceful Restart 機能を使用した場合です。
- 注 4
 コンフィグレーションコマンド `ip pim nonstop-forwarding` を設定した場合です。ただし、VRF のインタフェースで IPv4 マルチキャストを動作させた場合、本機能は無効になります。
- 注 5
 コンフィグレーションコマンド `ipv6 pim nonstop-forwarding` を設定した場合です。ただし、VRF のインタフェースで IPv6 マルチキャストを動作させた場合、本機能は無効になります。

17.1.6 コンフィグレーション不一致時の動作

基本制御機構 (BCU)、制御スイッチング機構 (CSU) または管理スイッチング機構 (MSU) の増設や交換時など、運用系と待機系でコンフィグレーションの差分が両系間で生じる場合があります。この状態で系が切り替わった場合、運用中のハードウェア設定と新運用系のコンフィグレーションが異なる場合があります。このため、本装置では運用系システムと待機系システム間のコンフィグレーションに不一致を検出するとログを出力します。また、立ち上げ時のコンフィグレーションに差分がある場合も同様に、不一致を検出するとログを出力します。コンフィグレーションの同期によって不一致が解消した場合には、一致検出のログを出力します。コンフィグレーションの同期処理中は、一時的にコンフィグレーションの編集が抑止されます。

17.1.7 運用コマンドおよび ACH スイッチによる系切替

本装置は AX6700S では BCU ボード、AX6600S では CSU ボード、AX6300S では MSU ボードを冗長構成で運用している場合、運用コマンド `redundancy force-switchover` の実行、または、それぞれのボードに搭載されている ACH スイッチを押すことによって運用系システムを切り替えられます。

運用コマンド `redundancy force-switchover` による系切替では、コマンドを実行した系は系切替後に待機系として動作します。待機系システムの起動が完了していない、系切替の準備ができていないなどの場合には系切替は抑止されます。

ACH スイッチによる系切替では、ACH スイッチを押した系は系切替後に再起動します。待機系システムの起動が完了していない場合には系切替は抑止されますが、系切替の準備ができていないなどの場合でも強制的に系切替を実行します。この場合、系切替後の新運用系は再起動します。

冗長構成の状態は運用コマンド `show system` で確認できます。起動が完了しない要因または系切替の準備ができていない要因の特定は、運用コマンド `show logging` を使用しログの対処方法、およびトラブルシューティングガイドに従って処置してください。

- 待機系システムの起動失敗
 待機系システムの起動が完了しない要因としてハードウェア故障、未サポートボードの挿入、標準版、拡張版ボードの混載などの禁止する構成となっている、コンフィグレーションと実装しているボードが一致していない、ソフトウェア障害があります。運用状態の確認、待機系システムの運用ログ情報、STATUS LED を確認し、回復処置を行ってください。
- 系切替の準備ができていない

待機系システムの系切替の準備ができていない要因は、運用コマンド `synchronize`、およびコンフィグレーションコマンド `save`、`copy` または `erase` によるコンフィグレーションの保存処理中の場合です。この保存処理中は一時的に系切替を抑止します。

- コンフィグレーションを操作している
コンフィグレーションを操作している状態の時は系切替が抑止されます。コンフィグレーションコマンド `end`、`quit`、`exit` によってコンフィグレーションの操作を終了してください。また、コンフィグレーションコマンド `status` で確認して、コンフィグレーション操作中のすべてのユーザについて、コンフィグレーションコマンドモードを終了してください。
- 運用系と待機系でライセンスキーが一致しない
ライセンスキーが一致しない状態では、運用コマンド `redundancy force-switchover` の実行は抑止されます。また、運用コマンド `reload active` または ACH スイッチによる系切替を実行すると、新運用系が再起動します。
- 電力制御モードを変更中
電力制御モードの変更中は、運用コマンド `redundancy force-switchover` の実行は抑止されます。変更開始時には "The change of power control mode was started." のログメッセージが表示され、変更が完了すると "The change of power control mode was completed." のログメッセージが表示されます。

17.1.8 冗長構成時の注意事項

(1) 運用系システムのボード交換

運用系 BCU、運用系 CSU または運用系 MSU を交換する場合は、運用コマンド `redundancy force-switchover` で運用系システムと待機系システムを系切替させ、交換部位を待機系にしてから交換してください。

(2) 冗長構成による運用開始時の注意事項

ソフトウェアの注意事項

運用系システムと待機系システムのソフトウェアバージョンが異なった冗長構成による運用中は、コンフィグレーションの編集ができません。ソフトウェアのバージョンを一致させてください。

(3) 冗長構成運用時のログインに関する注意事項

シリアル接続ポート

運用系システムおよび待機系システムのそれぞれにコンソールを接続してログインが可能です。

マネージメントポート

冗長構成時は運用系システムのマネージメントポートを使用して装置にログインできます。待機系システムのマネージメントポートからはログインできません。

通信用ポート

リモート運用端末から通信用ポートを経てログインする場合は運用系システムにログインします。待機系システムへログインすることはできません。

シリアル接続ポート (AUX) にダイアルアップ IP 接続

リモート運用端末からダイアルアップ IP 接続してログインする場合は、運用系システムおよび待機系システムへログインが可能です。

(4) 運用系システムの管理情報の同期に関する注意事項

AX6700S および AX6300S で、容量が異なる内蔵フラッシュメモリを搭載した BCU または MSU で冗長構成を構築している場合、運用コマンド `synchronize` 実行時にエラーになることがあります。詳細は、「運用コマンドレファレンス Vol.2 synchronize」の注意事項を参照してください。

17.2 オペレーション

17.2.1 運用コマンド一覧

運用系システム、待機系システムを管理する上で必要な運用コマンド一覧を次の表に示します。また、BCU、CSU または MSU を冗長構成で運用するために必要なコンフィグレーションはありません。

表 17-4 運用コマンド一覧

コマンド名	説明
inactivate standby	待機系システムを停止します。
activate standby	待機系システムを起動します。
redundancy force-switchover	運用系システムと待機系システムを切り替えます。
synchronize	待機系システムの情報を運用系システムの情報に合わせます。
show system ¹	装置の運用状態を表示します。
reload ¹	standby パラメータで待機系システムを再起動します。
show logging ²	運用系システムまたは待機系システムの運用ログを表示します。

注 1

「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。

注 2

「運用コマンドレファレンス Vol.1 13. ログ」を参照してください。

17.2.2 待機系の状態確認

show system コマンドによって、運用系システムを介して待機系システムの状態を参照できます。また、運用系システムで show logging コマンドの standby パラメータを指定することで待機系システムのログを参照できます。ただし、障害などによって待機系システムが起動できない場合は状態およびログを参照できません。

17.2.3 系切替の実施

二重化運用時、運用系システムを交換する必要がある場合や運用系システムに障害がある場合は、次に示す「1.redundancy force-switchover コマンドによる系切替」を行ってください。ただし、運用系システムの障害が原因でコマンドによる系切替が実行できない場合は、「2.ACH スイッチによる系切替」を行ってください。

1. redundancy force-switchover コマンドによる系切替

運用系システムから redundancy force-switchover コマンドを実行すると、運用系システムが切り替わります。

2. ACH スイッチによる系切替

冗長構成で運用している状態で、運用系のボードにある ACH スイッチを押すと、運用系システムが切り替わります。運用系システムが切り替わったあと、新待機系システムは自動的に再起動します。

17.2.4 情報同期の実施

運用中に「表 17-2 運用中に同期する管理情報」で示す情報が両系間で不一致になった場合、

17. BCU/CSU/MSU の冗長化

synchronize コマンドを実行して情報不一致の状態を解消してください。

18 BSU の冗長化【AX6700S】

この章では基本スイッチング機構（BSU）の冗長構成について説明します。

18.1 解説

18.2 コンフィグレーション

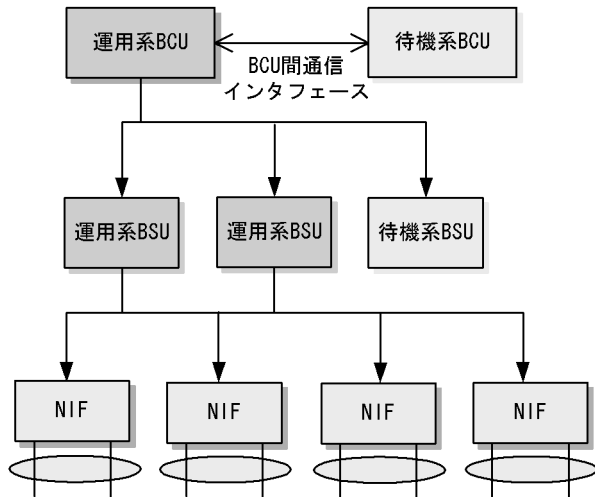
18.3 オペレーション

18.1 解説

18.1.1 冗長化時の装置構成

基本スイッチング機構（BSU）を冗長化する場合、BSU を 2 枚以上実装して冗長構成にできます。BSU を冗長化することによって、NIF との通信インターフェースも冗長化されます。冗長構成にすることで障害に対する信頼性を高めることができます。

図 18-1 BCU-BSU-NIF 間の冗長構成でのインターフェース



（凡例） —▶ : 通信インターフェース

運用系および待機系の BSU はそれぞれ独立したインターフェースで NIF と接続し、パケット転送を行います。

18.1.2 冗長構成の運用方法

（1）運用形態

BSU の運用形態を次に示します。

すべての BSU を運用系にする。

すべての BSU を運用系にすることによって、パケット転送性能を最大にします。

1 ~ 2 枚の BSU を運用系、1 枚を待機系にする。

1 枚の BSU を待機系とし、1 ~ 2 枚の BSU を運用系とします。障害発生時に待機系 BSU を使用してパケット転送性能を維持します。

（2）待機系の運用

ホットスタンバイ

待機系の電力を ON にして、BSU を起動した状態で待機させ、運用系 BSU の障害発生時に系切替を瞬時に行います。

コールドスタンバイ

待機系の電力を部分的に OFF にして、BSU を停止させた状態で待機させ、運用系 BSU の障害発生時

に待機系 BSU を起動し、系切替を行います。電力を OFF にすることによって、待機系 BSU の消費電力を抑えられます。なお、系切替時に待機系 BSU を起動するため、系切替に時間が必要です。

コールドスタンバイ 2

待機系 BSU の電力供給を完全に OFF にすることによって、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 の障害発生時には自動的に起動し、系切替を行います。なお、系切替時に待機系 BSU を起動するため、系切替に時間が必要です。

18.1.3 障害発生時の BSU 動作

(1) フェイルセーフモード

冗長構成で BSU に障害が発生した場合、ほかの正常な BSU を使用して通信を継続します。本装置のデフォルトのモードです。

すべての BSU を運用系として使用している場合に障害が発生すると、ほかの正常な BSU を使用して通信を継続します。待機系を使用している場合に障害が発生すると、通信を待機系に切り替えることでパケット転送性能を維持したまま回復します。

障害発生時の動作例を次に示します。

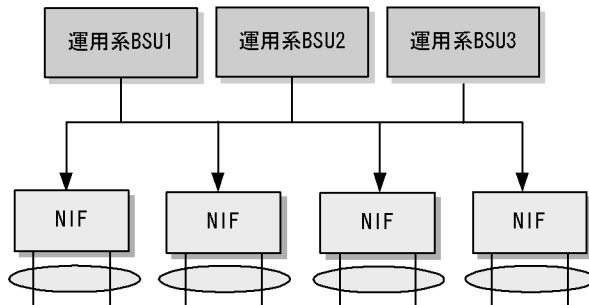
すべての BSU が運用系の場合

すべての BSU が運用系として動作している場合に、障害が発生した例を次に示します。

- 障害前

BSU 動作状態が稼働中のものが 3 枚で動作しています。障害発生前の動作を次の図に示します。

図 18-2 障害発生前の動作

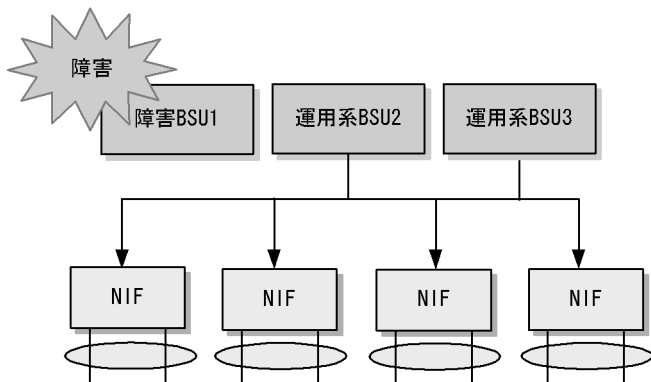


(凡例) —▶ : 通信インターフェース

- 障害発生後

BSU 番号 1 のボードに障害が発生した場合、障害が発生していない BSU で動作し続けます。障害発生後の動作を次の図に示します。

図 18-3 障害発生後の動作



(凡例) → : 通信インターフェース

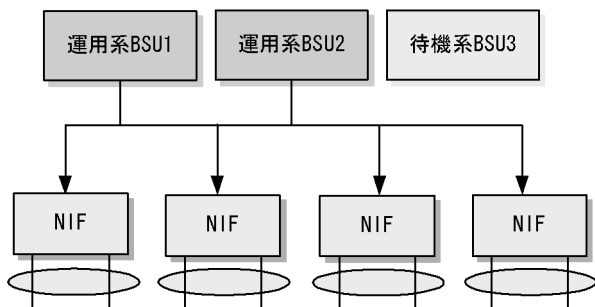
待機系 BSU がある場合

運用系と待機系に分けて動作している場合に、障害が発生した例を次に示します。

• 障害前

BSU 動作状態が稼働中のものが 2 枚、コンフィグレーションの運用系の枚数に 2 を設定した状態で動作しています。障害発生前の動作を次の図に示します。

図 18-4 障害発生前の動作

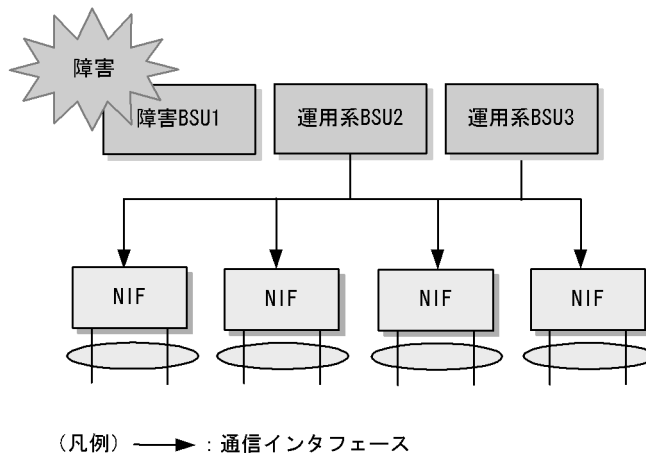


(凡例) → : 通信インターフェース

• 障害発生後

BSU 番号 1 のボードに障害が発生した場合、待機系 BSU3 が運用系に切り替わり、動作し続けます。障害発生後の動作を次の図に示します。

図 18-5 障害発生後の動作



(2) 固定モード

冗長構成で BSU に障害が発生しても、該当 BSU を経由していた通信を通信障害とすることで、ほかの正常な BSU のパケット転送性能に影響を与えないモードです。本モードは、通信障害を検出して通信経路を切り替えられる他装置と組み合わせての使用が想定されます。

また、本モードは使用する BSU 数をあらかじめコンフィグレーションコマンド `redundancy max-bsu` で指定し、指定した数に対応したスロット番号に BSU を実装する必要があります。コンフィグレーションで指定する BSU 数とスロット番号の関係を次の表に示します。

表 18-1 コンフィグレーションで指定する BSU 数とスロット番号の関係

コンフィグレーションで指定する BSU 数	動作する BSU スロット番号
1	1
2	1, 2
3	1, 2, 3

18.1.4 パケット転送時の負荷分散

BSU を冗長化し、2 枚以上の BSU を運用系として使用している場合、パケット転送を行う BSU を分散させることで運用系 BSU を効率的に利用します。負荷分散方法として、受信したポートごとに振り分ける方法と、受信パケットの送信元 MAC アドレスごとに振り分ける方法があります。

(1) ポートごとの振り分け

パケットを受信したポートごとに振り分け先 BSU を選択します。本装置のデフォルトのモードです。サーバやルータなどの通信のようにトラフィックが集中するポートについて、接続ポートを選択することでパケット転送を行う BSU を分散させることができます。

BSU と NIF の間のパケット転送バスは BSU1 枚当たり 2 本あり、それぞれの中継バスでパケット転送性能を共有します。そのため、パケット転送性能を共有する組み合わせは最大 BSU3 枚で 6 組あります。

パケット転送性能を共有するポートの組み合わせを次の表に示します。

表 18-2 パケット転送性能を共有するポートの組み合わせ

NIF の種類	ポート数	運用系 BSU 枚数ごとの パケット転送性能を共有するポートの組み合わせ		
		1 枚	2 枚	3 枚
NK1G-24T	24	(1,3,5,7,9,11,13,15,17,19,21,23) (2,4,6,8,10,12,14,16,18,20,22,24)	(1,5,9,13,17,21) (2,6,10,14,18,22) (3,7,11,15,19,23) (4,8,12,16,20,24)	(1,7,13,19) (2,8,14,20) (3,9,15,21) (4,10,16,22) (5,11,17,23) (6,12,18,24)
NK1G-24S				
NK1GS-8M	8	(1,2,3,4,5,6,7,8) (なし)	(1,2,3,4,5,6,7,8) (なし) (なし) (なし)	(1,2,3,4,5,6,7,8) (なし) (なし) (なし) (なし) (なし)
NK10G-4RX	4	(1,3) (2,4)	(1) (2) (3) (4)	(1) (2) (3) (4)
NK10G-8RX	8	(1,3,5,7) (2,4,6,8)	(1,5) (2,6) (3,7) (4,8)	(1,7) (2,8) (3) (4) (5) (6)

(凡例) (): BSU を共有するポートの組み合わせ

NK1GS-8M では、すべての入力ポートが同一のパケット転送バスに割り当てられます。

(2) 送信元 MAC アドレスごとの振り分け

受信パケットの送信元 MAC アドレスごとに振り分け先 BSU を選択します。本装置の中継するパケットの送信元 MAC アドレスが多数ある構成、または送信元 MAC アドレスごとのトラフィックの偏りが少ない構成で有効な方式です。

サーバ宛てやルータ経由の通信が集中する環境では、同じ送信元 MAC アドレスのトラフィックが偏るおそれがあります。その場合、パケットの振り分けが特定の BSU に集中するおそれがあるため注意してください。

18.1.5 運用時の同期情報および同期契機

運用系と待機系の間で同期される情報を次の表に示します。同期を行った情報は待機系側の動作にも適用され、系切替後も動作矛盾が発生すること無く運用できます。

表 18-3 運用中の同期情報

同期情報	同期が行われる契機
MAC アドレスエントリ	MAC アドレスエントリが変更された際、即時に同期します。
ルーティングエントリ情報	ルーティングエントリ情報が変更された際、即時に同期します。

18.1.6 冗長構成時の注意事項

(1) BSU の固定モードと送信元 MAC アドレスごとの振り分けに関する注意事項

BSU の固定モードと、送信元 MAC アドレスごとの振り分け機能を設定するときは、次に示す項目に注意してください。

表 18-4 BSU の固定モードと送信元 MAC アドレスごとの振り分けに関する注意事項

項目	注意事項
同時使用時だけのサポート	BSU の固定モードと送信元 MAC アドレスごとの振り分けは、これらの機能を同時に使用する場合だけサポートされます。
コンフィグレーションの変更	コンフィグレーションを変更する場合、変更を保存したあとに、装置を再起動してください。
障害部位の復旧	BSU の固定モードと送信元 MAC アドレスごとの振り分けを使用する場合、装置の障害が発生した際に障害部位を復旧しないで、停止したままにする動作だけがサポートされます。 コンフィグレーションコマンド <code>no system recovery</code> を設定してください。
同時使用未サポートの機能	次に示す機能は、BSU の固定モード、送信元 MAC アドレスごとの振り分けと同時に使用することはできません。 <ul style="list-style-type: none"> 待機系の BSU 省電力機能（電力制御） 帯域監視機能 ストームコントロール NIF のポートを使用した本装置宛通信を伴うすべての機能（NIF のポートを経由した本装置への telnet やルーティングプロトコルなどが使用不可となります）

(2) 運用系 BSU 数の設定とポートごとの振り分けに関する注意事項

パケット転送時の負荷分散モードにポートごとの振り分け機能を設定するときは、運用系として使用する BSU 数をコンフィグレーションコマンド `redundancy max-bsu` で指定してください。運用系として使用する BSU 数とコンフィグレーションコマンド `redundancy max-bsu` で指定した数を一致させることで、パケット転送を行う BSU を分散させて運用系 BSU を効率良く利用できます。

18.2 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

BSU の冗長構成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を次の表に示します。

表 18-5 コンフィグレーションコマンド一覧

コマンド名	説明
redundancy bsu-load-balancing	パケット転送の負荷分散を設定します。
redundancy bsu-mode	BSU の運転モードを設定します。
redundancy max-bsu	稼働する BSU 数を設定します。
redundancy standby-bsu	待機系の BSU モードを設定します。
power enable	no power enable コマンドで、ボードの電力 OFF を設定します。本コマンドにより系切替が可能です。

注

「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。

18.2.2 BSU の冗長構成の設定

[設定のポイント]

BSU を待機系にして冗長構成を設定する場合、運用系の枚数を設定します。設定した運用系の枚数より多く BSU を実装している場合に、残りの BSU が待機系として動作します。設定後は、最小の BSU 番号から順に運用系になります。設定した運用系の枚数以下の BSU を実装している場合には、すべての BSU が運用系として動作します。

次に示す例では、フェイルセーフモードで、運用系 BSU を 2 枚として運用します。BSU を 3 枚実装した場合に、1 枚が待機系として動作します。

[コマンドによる設定]

1. (config)# redundancy max-bsu 2
BSU を運用系として 2 枚使用します。

18.2.3 待機系の電力消費量を下げる設定

[設定のポイント]

待機系をコールドスタンバイ 2 に設定し、電力消費量を下げます。

[コマンドによる設定]

1. (config)# redundancy standby-bsu cold2
待機系をコールドスタンバイ 2 に指定します。

18.2.4 BSU の固定モードおよび送信元 MAC アドレスごとの振り分けの設定

[設定のポイント]

BSU の固定モード，送信元 MAC アドレスごとの振り分けは両機能を併せて設定する必要があります。

[コマンドによる設定]

1. `(config)# no system recovery`
障害が発生した場合に，障害部位を復旧しないで停止したままとする動作を設定します。
2. `(config)# redundancy max-bsu 2`
BSU を固定モードで稼働させる数を設定します。本設定では BSU2 枚とし，BSU スロット 1，2 で動作します。
3. `(config)# redundancy bsu-mode fixed`
BSU の固定モードを設定します。
4. `(config)# redundancy bsu-load-balancing smac`
送信元 MAC アドレスごとの振り分けを設定します。
5. `(config)# save`
`(config)# exit`
`# reload`
コンフィギュレーションを保存し，本装置を再起動します。再起動後に本機能が有効になります。

[注意事項]

- 本機能を設定または削除したあとは，ほかのコンフィギュレーションを変更したり，運用コマンドによる操作をしたりする前に，コンフィギュレーションを保存し，装置を再起動してください。

18.2.5 BSU の固定モードおよび送信元 MAC アドレスごとの振り分け設定時に BSU を増設する設定

[設定のポイント]

BSU を増設するときは，一時的に固定モードおよび送信元 MAC アドレスごとの振り分け設定を削除してから BSU 数を変更し，再度固定モードおよび送信元 MAC アドレスごとの振り分けを設定する必要があります。

[コマンドによる設定]

1. `(config)# no redundancy bsu-mode`
`(config)# no redundancy bsu-load-balancing`
固定モードおよび送信元 MAC アドレスごとの振り分けが設定されていることを前提とし，BSU を 2 枚から 3 枚に増設します。次に BSU の固定モードおよび送信元 MAC アドレスごとの振り分け設定をいったん削除します。
2. `(config)# redundancy max-bsu 3`
BSU の固定モードで稼働させる BSU 数を 3 枚に変更します。

18. BSU の冗長化【AX6700S】

3. (config)# redundancy bsu-mode fixed

(config)# redundancy bsu-load-balancing smac

BSU の固定モードおよび送信元 MAC アドレスごとの振り分けを設定します。

4. (config)# save

(config)# exit

reload

コンフィグレーションを保存し、本装置を再起動します。再起動後に本設定が有効になります。

18.3 オペレーション

18.3.1 運用コマンド一覧

BSU の冗長構成を管理する上で必要な運用コマンド一覧を次の表に示します。

表 18-6 運用コマンド一覧

コマンド名	説明
show system ¹	BSU の冗長構成の状態を表示します。
inactivate bsu ²	ボードの電力 OFF を設定します。本コマンドにより系切替が可能です。
show logging ³	BSU の障害情報を表示します。

注 1

「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。

注 2

「運用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 3

「運用コマンドレファレンス Vol.1 13. ログ」を参照してください。

18.3.2 運用系および待機系の状態確認

show system コマンドで運用系および待機系 BSU の動作状態が参照できます。show logging コマンドで運用系および待機系の障害情報が参照できます。

図 18-6 BSU の冗長構成の状態確認

```
> show system
Date 2006/10/13 06:35:27 UTC
System: AX-6700-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]
:
:
```

図 18-7 BSU の障害情報の確認

```
> show logging
Date 2006/03/25 14:14:18 UTC
System Information
:
:
EVT 12/24 12:35:25 R6 BSU BSU:1 25070002 1681:000000000000 BSU initialized.
:
:
```

18.3.3 系切替の実施

BSU の冗長構成による運用時，系切替が必要な場合は，`inactivate` コマンドまたはコンフィグレーションコマンド `no power enable` で系切替を行ってください。

上記の方法で系切替ができない場合，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。

19 PSP の冗長化【AX6600S】

この章では、PSP の冗長構成について説明します。

19.1 解説

19.2 コンフィグレーション

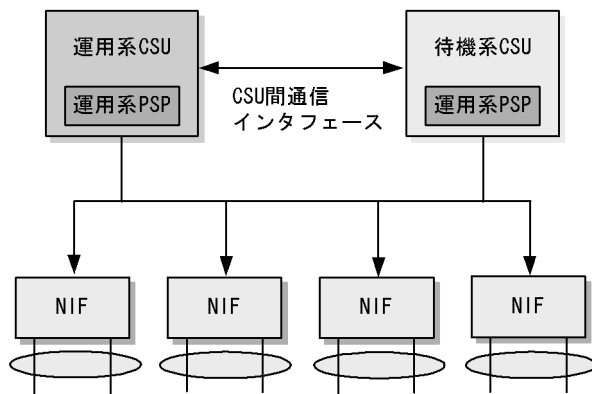
19.3 オペレーション

19.1 解説

19.1.1 冗長化時の装置構成

CSU を 2 枚実装し、すべての PSP を運用系として稼働させることで、パケット転送性能を最大にできます。また、CSU を 2 枚実装し、それぞれの PSP を運用系、待機系として稼働させると PSP は冗長構成になり、PSP-NIF 間の通信インターフェースも冗長化されます。この冗長化によって、障害に対する信頼性を向上できます。

図 19-1 すべての PSP を運用系として稼働した場合の CSU-NIF 間インターフェース



(凡例) → : 通信インターフェース

運用系および待機系の PSP はそれぞれ独立したインターフェースで NIF と接続し、パケット転送を行います。

19.1.2 冗長構成の運用方法

(1) 運用形態

PSP の運用形態を次に示します。

すべての PSP を運用系にする。

すべての PSP を運用系にするによって、パケット転送性能を最大にします。

PSP を運用系と待機系にする。

片方の PSP を待機系とし、もう一方の PSP を運用系とします。障害発生時に待機系 PSP を使用してパケット転送性能を維持します。

(2) 待機系の運用

ホットスタンバイ

待機系の電力を ON にして、PSP を起動した状態で待機させ、運用系 PSP の障害発生時に系切替を瞬時に行います。

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 の障害発生時に自動的に起動し、系切替を行います。なお、系切替時に待機系 PSP を起動するため、系切替に時間が掛かります。

19.1.3 障害発生時の PSP 動作

冗長構成で PSP に障害が発生した場合、ほかの正常な PSP を使用して通信を継続します。すべての PSP を運用系として使用している場合に障害が発生すると、ほかの正常な PSP を使用して通信を継続します。待機系 PSP がある場合に障害が発生すると、運用系から待機系に切り替えることでパケット転送性能を維持したまま通信を継続します。

障害発生時の動作例を次に示します。

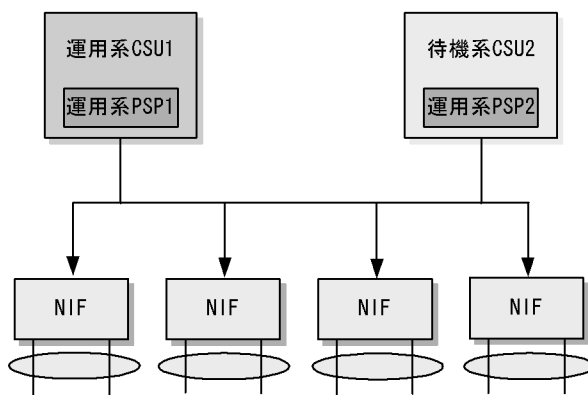
すべての PSP が運用系の場合

すべての PSP が運用系として動作している場合に、障害が発生した例を次に示します。

- 障害前

両系の PSP が運用系として動作しています。障害発生前の動作を次の図に示します。

図 19-2 障害発生前の動作

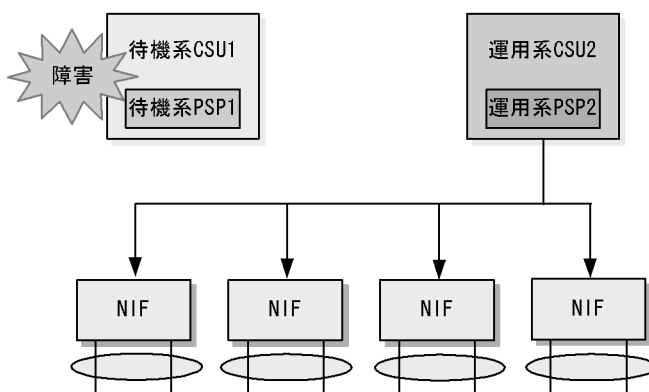


(凡例) —▶ : 通信インターフェース

- 障害発生後

CSU1 系のボードに障害が発生した場合、障害が発生していない PSP で動作し続けます。障害発生後の動作を次の図に示します。

図 19-3 障害発生後の動作



(凡例) —▶ : 通信インターフェース

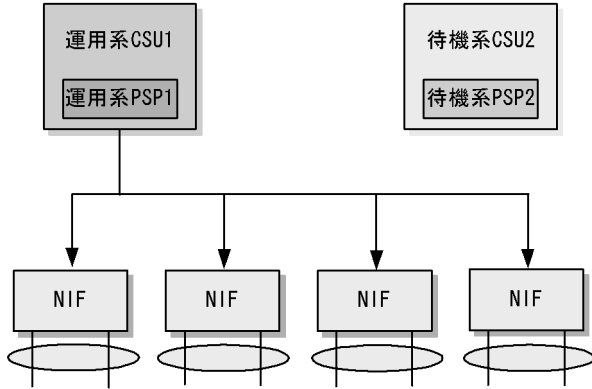
待機系 PSP がある場合

運用系と待機系に分けて動作している場合に、障害が発生した例を次に示します。

• 障害前

運用系 CSU の PSP が運用系として動作しています。また、コンフィグレーションの運用系 PSP 数に 1 を設定した状態で動作しています。障害発生前の動作を次の図に示します。

図 19-4 障害発生前の動作

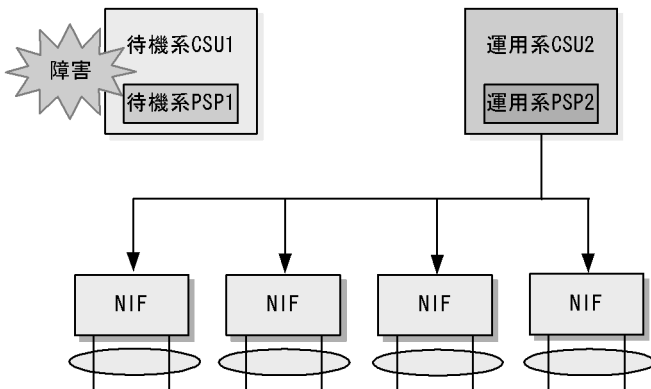


(凡例) → : 通信インターフェース

• 障害発生後

CSU1 系のボードに障害が発生した場合、CSU2 系が待機系から運用系に切り替わり、動作し続けます。障害発生後の動作を次の図に示します。

図 19-5 障害発生後の動作



(凡例) → : 通信インターフェース

19.1.4 パケット転送時の負荷分散

CSU を冗長化し、両系の PSP を運用系として使用している場合、パケット転送を行う PSP を分散させることで運用系 PSP を効率的に利用します。

パケットを受信するポートごとに振り分け先 PSP が決まります。したがって、サーバやルータなどの通信のようにトラフィックが集中するポートは、できるだけ振り分け先 PSP が分散するように接続ポートを選択します。これによって、パケット転送を行う PSP の負荷を分散できます。

PSP と NIF の間のパケット転送パスは 1PSP 当たり 1 本あり、それぞれの中継パスでパケット転送性能を共有します。

パケット転送性能を共有するポートの組み合わせを次の表に示します。

表 19-1 パケット転送性能を共有するポートの組み合わせ

NIF の種類	ポート数	運用系 PSP 数ごとの パケット転送性能を共有するポートの組み合わせ	
		1	2
NK1G-24T NK1G-24S	24	(1,2,3,4,5,6,7,8,9,10,11,12, 13,14,15,16,17,18,19,20,21, 22,23,24)	(1,3,5,7,9,11,13,15,17,19,21,23) (2,4,6,8,10,12,14,16,18,20,22,24)
NK1GS-8M	8	(1,2,3,4,5,6,7,8)	(1,2,3,4,5,6,7,8) (なし)
NK10G-4RX	4	(1,2,3,4)	(1,3) (2,4)
NK10G-8RX	8	(1,2,3,4,5,6,7,8)	(1,3,5,7) (2,4,6,8)

(凡例)(): PSP を共有するポートの組み合わせ

19.1.5 運用時の同期情報および同期契機

運用系と待機系の間で同期される情報を次の表に示します。同期を行った情報は待機系側の動作にも適用され、系切替後も動作矛盾が発生することなく運用できます。

表 19-2 運用中の同期情報

同期情報	同期が行われる契機
MAC アドレスエントリ	MAC アドレスエントリが変更された際、即時に同期します。
ルーティングエントリ情報	ルーティングエントリ情報が変更された際、即時に同期します。

19.2 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

PSP の冗長構成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を次の表に示します。

表 19-3 コンフィグレーションコマンド一覧

コマンド名	説明
redundancy max- <i>psp</i>	稼働する PSP 数を設定します。
redundancy standby- <i>psp</i>	待機系の PSP モードを設定します。

19.2.2 すべての PSP を運用系とする設定

[設定のポイント]

すべての PSP を運用系とするときは、運用系 PSP 数を 2 に設定します。本装置のデフォルトのモードです。

次に示す例では、両系の PSP を運用系として運用します。CSU を 2 枚実装した場合に、両系の PSP が運用系として動作します。

[コマンドによる設定]

1. (config)# redundancy max-*psp* 2
両系の PSP を運用系として使用します。

19.2.3 PSP の冗長構成の設定

[設定のポイント]

PSP の一つを待機系にして冗長構成を設定する場合、運用系 PSP 数を 1 に設定します。設定後は、運用系 CSU の PSP が運用系になり、待機系 CSU の PSP が待機系になります。

次に示す例では、片系の PSP を運用系として使用します。CSU を 2 枚実装した場合に、待機系 CSU の PSP が待機系として動作します。

[コマンドによる設定]

1. (config)# redundancy max-*psp* 1
片系の PSP を運用系として使用します。

19.2.4 待機系 PSP の電力消費量を下げる設定

[設定のポイント]

待機系 PSP をコールドスタンバイ 2 に設定し、電力消費量を下げます。

[コマンドによる設定]

1. (config)# redundancy standby-*psp* cold2
待機系 PSP をコールドスタンバイ 2 に指定します。

19.3 オペレーション

19.3.1 運用コマンド一覧

PSP の冗長構成を管理する上で必要な運用コマンド一覧を次の表に示します。

表 19-4 運用コマンド一覧

コマンド名	説明
show system ¹	PSP の冗長構成の状態を表示します。
show logging ²	PSP の障害情報を表示します。

注 1

「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。

注 2

「運用コマンドレファレンス Vol.1 13. ログ」を参照してください。

19.3.2 運用系および待機系 PSP の状態確認

show system コマンドで運用系および待機系 PSP の動作状態が参照できます。show logging コマンドで運用系および待機系の障害情報が参照できます。

図 19-6 PSP の冗長構成の状態確認

```
> show system
Date 2009/04/01 06:35:27 UTC
System: AX6608S, OS-SE Ver. 11.1
      :
      :
      CSU1 : active
      :
      PSP : active
      :
      :
      CSU2 : standby
      :
      PSP : standby cold2
      :
      :
>
```

図 19-7 PSP の障害情報の確認

```
> show logging
Date 2009/04/01 14:14:18 UTC
System Information
      :
      :
EVT 04/01 12:35:25 R8 CSU 25070002 2301:000000000000 PSP initialized.
      :
      :
```


20 NIF の冗長化【AX6700S】 【AX6600S】

この章では、NIF の冗長構成について説明します。

20.1 解説

20.2 コンフィグレーション

20.3 オペレーション

20.1 解説

20.1.1 冗長化時の装置構成

本装置では、搭載した 2 枚の NIF をグループ化（NIF 冗長グループと呼びます）して、それぞれの NIF を運用系または待機系に分けられます。また、グループ化した NIF のポートにリンクアグリゲーションを設定して、冗長化ができます。このため、障害に対する信頼性を向上できるだけでなく、待機系 NIF の電力供給を完全に OFF（コールドスタンバイ）にして、消費電力をほぼ 0（ゼロ）に抑えられます。

NIF 冗長グループ内での運用系および待機系の NIF 数と、どの NIF が運用系になるかは、コンフィグレーションで設定する最大待機系 NIF 数と NIF 優先度によって決まります。

NIF 冗長グループ

一つの NIF 冗長グループに NIF は 2 枚まで所属できます。各 NIF が所属できる NIF 冗長グループは一つだけです。なお、NIF 種別が異なる場合でも、同じ NIF 冗長グループに所属できます。

最大待機系 NIF 数

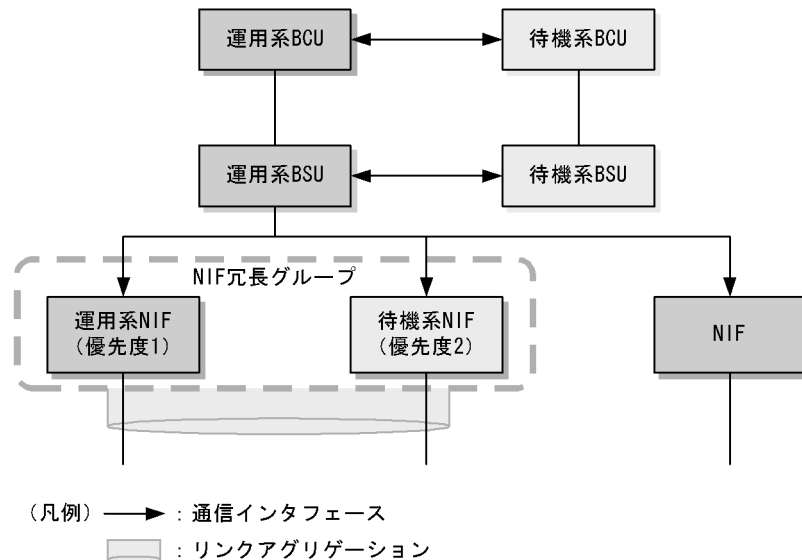
NIF 冗長グループに所属する NIF のうち、待機状態となる NIF の最大枚数です。

NIF 優先度

NIF 冗長グループに所属する各 NIF の優先度です。値が小さいほど優先度が高くなり、優先度の高い NIF が運用系になります。

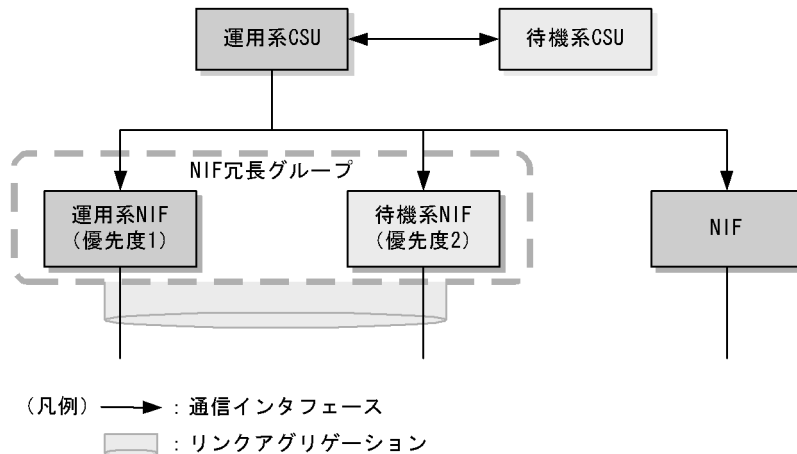
シリーズごとの冗長構成でのインタフェースを次の図に示します。

図 20-1 BCU-BSU-NIF 間の冗長構成でのインタフェース



運用系および待機系の NIF はそれぞれ独立したインタフェースで BSU と接続し、パケット転送を行います。

図 20-2 CSU-NIF 間の冗長構成でのインタフェース



運用系および待機系の NIF はそれぞれ独立したインタフェースで CSU と接続し、パケット転送を行います。

20.1.2 冗長構成での動作

(1) 待機系 NIF を起動する条件

NIF 冗長グループ内で運用系 NIF と待機系 NIF が 1 枚ずつ稼働している場合、次の表に示す条件が発生すると待機系 NIF を起動します。なお、待機系 NIF を起動しても、運用系 NIF は待機系にはなりません。

表 20-1 待機系 NIF の起動条件

対象部位	対象条件
運用系 NIF	<ul style="list-style-type: none"> ハードウェア障害 HDC の更新による再起動 コンフィグレーションによる再起動 運用コマンドの実行による再起動 NIF が inactive 状態、または disable 状態になる
運用系 NIF 配下のポート	<ul style="list-style-type: none"> ハードウェア障害 回線障害 トランシーバ障害 コンフィグレーションによる再起動 ポートが inactive 状態、または test 状態になる

注

通信に使用しないポートは、コンフィグレーションで disable 状態にすることが必要です。disable 状態にしない場合、待機系 NIF を起動します。

(2) 運用系 NIF を待機系にする条件

NIF 冗長グループ内のすべての NIF が運用系の場合、NIF 優先度の高い運用系 NIF 配下のポートが次のどちらかの状態になると、NIF 優先度が低い運用系 NIF を待機系 NIF へ変更します。

- active up 状態
- コンフィグレーションによる disable 状態

20.1.3 冗長構成の運用方法

NIF の運用形態を次に示します。

すべての NIF を運用系にする。

NIF 冗長グループ内の最大待機系 NIF 数を 0 にすることで、2 枚の NIF を運用系とします。

1 枚の NIF を運用系、1 枚を待機系にする。

NIF 冗長グループ内の最大待機系 NIF 数を 1 にすることで、1 枚の NIF を待機系とし、もう 1 枚の NIF を運用系とします。障害発生時に待機系 NIF を使用してパケット転送性能を維持します。

20.1.4 NIF 冗長機能に関する注意事項

- NIF 冗長機能でコールドスタンバイとなっている待機系 NIF に対して、コンフィグレーションまたは運用コマンドで NIF を inactive または disable 状態にした場合、運用系 NIF に障害が発生しても該当 NIF を起動しません。
- 通信に使用しないポートは、コンフィグレーションで disable 状態にしてください。
- リンクアグリゲーションを設定する場合には、スタティックモードを設定してください。

20.2 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

NIF の冗長構成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
redundancy nif-group max-standby-nif	NIF 冗長グループを指定して、グループ内で待機状態となる NIF の最大枚数を設定します。
redundancy nif-group nif priority	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	ポートをシャットダウン状態にします。

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 NIF の冗長構成の設定

[設定のポイント]

NIF を待機系にして冗長構成を設定する場合、NIF を 2 枚搭載して、グループ化した NIF のポートにスタティックリンクアグリゲーションを設定します。

NIF 冗長グループを指定して、グループ内で待機状態となる NIF の最大数を設定します。また、NIF 冗長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。優先度を設定するときは、運用系および待機系 NIF の優先度と、スタティックリンクアグリゲーションの運用系および待機系ポートの優先度が合うようにする必要があります。設定後は、NIF 冗長グループ内で優先度の低い NIF が待機系になります。

次に示す例では、運用系 NIF を 1 枚として運用します。NIF を 2 枚実装した場合に、1 枚が待機系として動作します。

[コマンドによる設定]

1. (config)# interface port-channel 10

(config-if)# channel-group max-active-port 1

(config-if)# exit

チャンネルグループ 10 を設定します。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 1 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。

2. (config)# interface tengigabitethernet 1/1

(config-if)# channel-group 10 mode on

(config-if)# lacp port-priority 200

(config-if)# exit

チャンネルグループ 10 にポート 1/1 をスタティックリンクアグリゲーションとして登録して、ポート優先度を 200 に設定します。

3. (config)# interface tengigabitethernet 2/1

(config-if)# channel-group 10 mode on

```
(config-if)# lacp port-priority 300
```

```
(config-if)# exit
```

チャンネルグループ 10 にポート 2/1 をスタティックリンクアグリゲーションとして登録して、ポート優先度を 300 に設定します。

4. (config)# interface range tengigabitethernet 1/2-8, tengigabitethernet 2/2-8

```
(config-if-range)# shutdown
```

```
(config-if-range)# exit
```

使用しないポートをシャットダウンします。

5. (config)# redundancy nif-group 1 max-standby-nif 1

NIF 冗長グループの最大待機系 NIF 数を設定します。

6. (config)# redundancy nif-group 1 nif 1 priority 1

```
(config)# redundancy nif-group 1 nif 2 priority 2
```

NIF 冗長グループに所属する NIF およびグループ内での NIF の優先度を設定します。

20.3 オペレーション

20.3.1 運用コマンド一覧

NIF の冗長構成を管理する上で必要な運用コマンド一覧を次の表に示します。

表 20-3 運用コマンド一覧

コマンド名	説明
show nif ¹	NIF 情報およびポートの summary 情報を表示します。
show redundancy nif-group ¹	NIF 冗長グループの情報を表示します。
show logging ²	NIF の障害情報を表示します。

注 1

「運用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

「運用コマンドレファレンス Vol.1 13. ログ」を参照してください。

20.3.2 冗長化 NIF の状態確認

show redundancy nif-group コマンドで NIF 冗長グループの動作状態が参照できます。show nif コマンドで NIF およびポートの動作状態が参照できます。また、show logging コマンドで運用系および待機系の障害情報が参照できます。

図 20-3 NIF 冗長グループの動作確認

```
> show redundancy nif-group
Date 2010/03/01 12:00:00 UTC
NIF Group Counts:1
NIF Group No:1
  NIF Counts:2 Max-Standby-NIF:1 Active NIF:1 Standby NIF:1
NIF:1   Priority:1   Status:active
NIF:2   Priority:2   Status:standby cold
>
```

図 20-4 NIF の動作状態の確認

```
>show nif 1
Date 2010/03/01 12:00:00 UTC
NIF1: active 8-port 10GBASE-R(XFP)   retry:0
      Average:0Mbps/108Gbps   Peak:0Mbps at 00:00:00
Port1: active up 10GBASE-LR   0012.e220.3bc3
      XFP connect
      Bandwidth:10000000kbps   Average out:0Mbps   Average in:0Mbps
Port2: disable 10GBASE-LR   0012.e220.3bc4
      XFP connect
      Bandwidth:10000000kbps   Average out:0Mbps   Average in:0Mbps
:
:
>

>show nif 2
Date 2010/03/01 12:00:00 UTC
NIF2: standby cold 8-port 10GBASE-R(XFP)   retry:0
      Average:0Mbps/108Gbps   Peak:0Mbps at 00:00:00
>
```

図 20-5 NIFの障害情報の確認

```
> show logging
Date 2010/03/01 12:00:00 UTC
System Information
:
:
EVT 03/01 12:35:25 R6 NIF NIF:1 25000002 1240:000000000000 NIF initialized.
:
:
>
```

21 GSRP の解説

GSRP は、レイヤ 2 およびレイヤ 3 で装置の冗長化を行う機能です。この章では、GSRP の概要について説明します。

21.1 GSRP の概要

21.2 GSRP の基本原理

21.3 GSRP の動作概要

21.4 レイヤ 3 冗長切替機能

21.5 GSRP のネットワーク設計

21.6 GSRP 使用時の注意事項

21.1 GSRP の概要

21.1.1 概要

GSRP (Gigabit Switch Redundancy Protocol) は、スイッチに障害が発生した場合でも、同一ネットワーク上の別スイッチを経由して通信経路を確保することを目的とした装置の冗長化を実現する機能です。

レイヤ 2 ではネットワークの冗長化を行うスパニングツリー、レイヤ 3 ではデフォルトゲートウェイの冗長化を行う VRRP を冗長化機能として利用できますが、GSRP を使うと、レイヤ 2 とレイヤ 3 の冗長化を一つの機能で同時に実現できます。

- レイヤ 2
2 台のスイッチ間で制御するため、スパニングツリーよりも装置間の切り替えが高速です。また、ネットワークのコアスイッチを多段にするような大規模な構成にも適しています。
- レイヤ 3
2 台のスイッチで同一の IP アドレスと MAC アドレスを持つことでデフォルトゲートウェイを冗長化します。PC などに対するデフォルトゲートウェイに GSRP を適用することで、PC などから上流のネットワークへの通信経路を冗長化できます。デフォルトゲートウェイの装置に障害が発生した場合でも同一の IP アドレス、MAC アドレスを引き継いで切り替えることで、PC などからのデフォルトゲートウェイを経由した通信を継続できます。

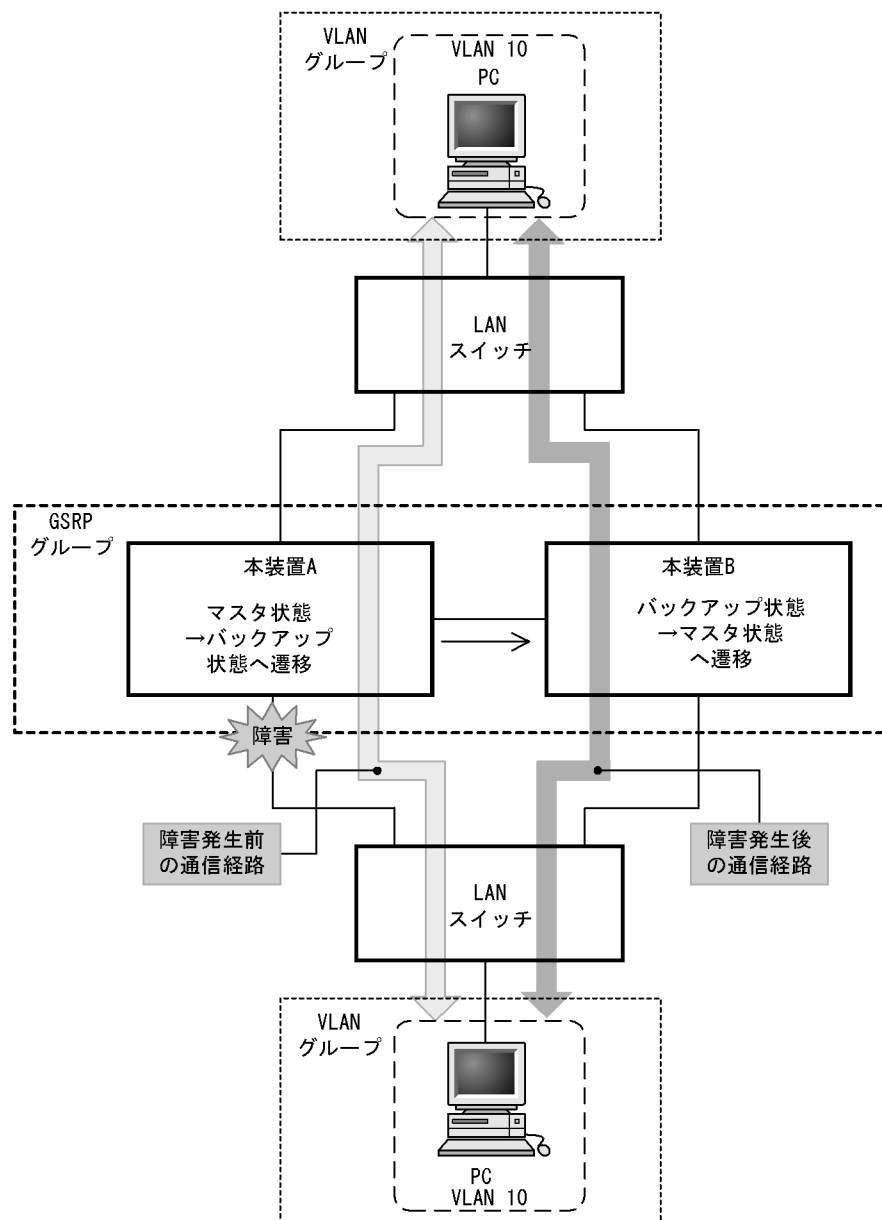
レイヤ 2 およびレイヤ 3 を同時に冗長化する機能の比較を次の表に示します。

表 21-1 レイヤ 2 およびレイヤ 3 を同時に冗長化する機能の比較

冗長化機能	説明
GSRP	<ul style="list-style-type: none"> • レイヤ 2 とレイヤ 3 の冗長化を一つの機能で実現しているため、管理が容易になる。 • 本装置独自仕様の機能のため、他社装置との接続はできない。
スパニングツリー + VRRP	<ul style="list-style-type: none"> • レイヤ 2 およびレイヤ 3 の両方で同時に冗長化を確保したい場合は、スパニングツリー、VRRP の両方の機能が必要になる。 • 標準プロトコルのため、マルチベンダーによるネットワークを構築できる。

GSRP によるレイヤ 2 の冗長化の概要を次の図に示します。

図 21-1 GSRP の概要



GSRP 機能を動作させる本装置 2 台をペアにしてグループを構成し、通常運用では片側をマスタ状態、もう一方をバックアップ状態として稼働させます。マスタ状態の本装置 A はフレームをフォワーディングし、バックアップ状態の本装置 B はブロッキングします。リンクの障害や装置障害などが発生した場合、本装置 A、B 間でマスタ状態とバックアップ状態の切り替えを行います。これによって、通信を継続できます。

21.1.2 特長

(1) 同時マスタ状態の回避

GSRP では本装置間を直接接続するリンク上で状態確認用の制御フレームの送受信を行い、対向装置の状態を確認します。制御フレームの送受信が正常にできている間にリンクの障害などを検出した場合は、自動的に切り替えを行います。その際、本装置は、対向の本装置が確実にバックアップ状態として稼働中

あることを確認した上でマスタ状態へ切り替わります。これによって 2 台の本装置が同時にマスタ状態になることを回避します。

また、装置障害などによって、制御フレームの送受信が正常にできなくなり、対向の本装置の状態が確認できない状態となった場合の切り替えは手動で行うことを基本とします。その理由は、対向の本装置がマスタ状態として稼働し続けている可能性があり、自動的にマスタ状態へ遷移したことによって、同時マスタ状態となることを回避するためです。運用者が障害の対応などを行い確実にマスタ状態へ切り替えても安全であると判断した上で、手動でマスタ状態へ切り替えることを想定しています。なお、手動による切り替えとは別に、本装置間を直接接続するリンクのダウンを検出した場合は、対向装置障害とみなして自動的に切り替える機能もサポートしています。

(2) 制御フレームの送信範囲の限定

GSRP では、制御フレームの送信範囲を限定し、不要な個所へ送信されることを防止するため、制御フレームの送受信は指定した VLAN だけで行います。

21.1.3 サポート仕様

GSRP でサポートする項目と仕様を次の表に示します。

表 21-2 GSRP 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 (IPv4, IPv6)
装置当たりの GSRP グループ最大数	1
GSRP グループを構成する本装置の最大数	2
GSRP グループ当たりの VLAN グループ最大数	128
VLAN グループ当たりの VLAN 最大数	4095
GSRP Advertise フレーム送信間隔	0.5 ~ 60 秒の範囲で 0.5 秒単位
GSRP Advertise フレーム保有時間	1 ~ 120 秒の範囲で 1 秒単位
ロードバランス機能	
バックアップ固定機能	
ポトリセット機能	
リンク不安定時の連続切り替え防止機能	
GSRP VLAN グループ限定制御機能	
GSRP 制御対象外ポート	

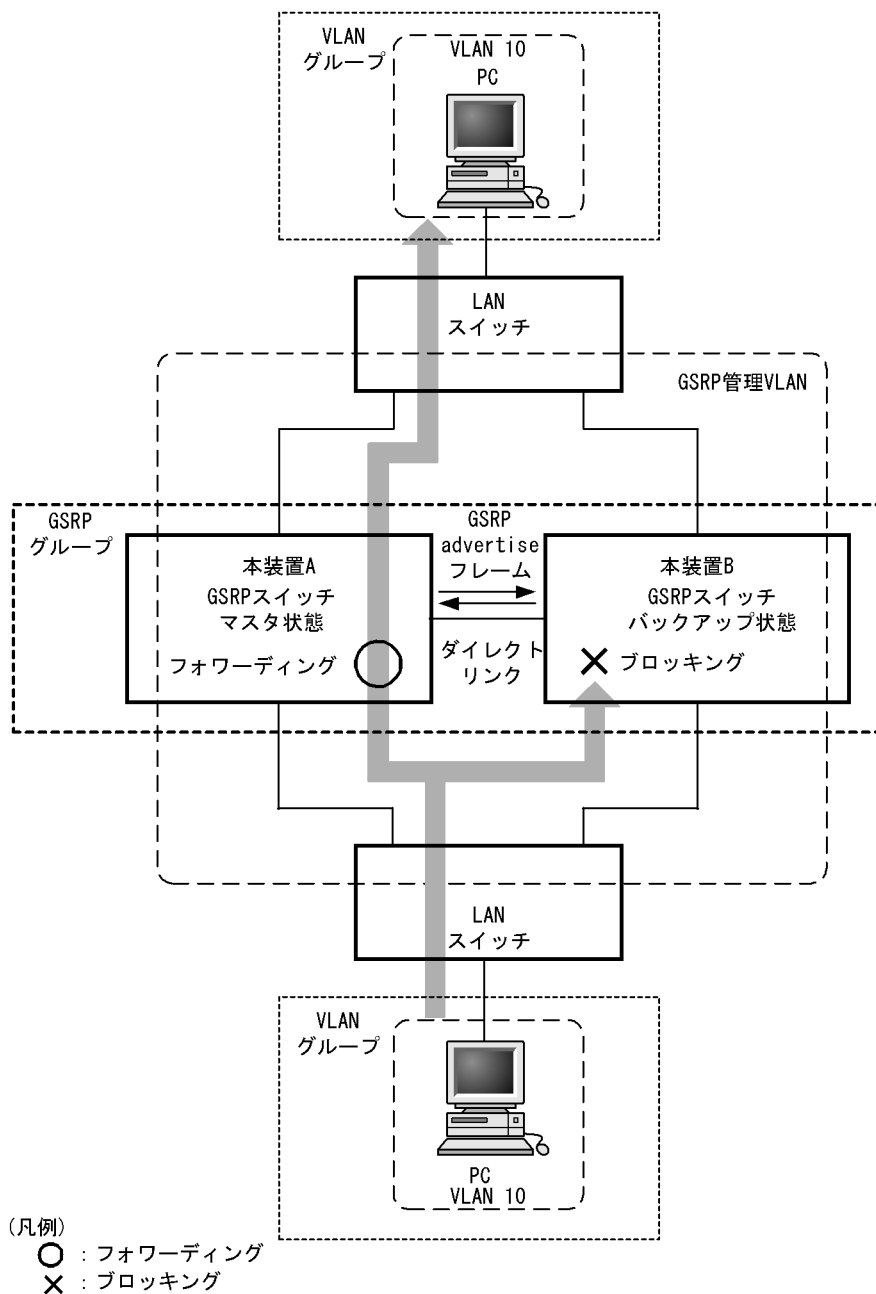
(凡例) : サポート

21.2 GSRP の基本原理

21.2.1 ネットワーク構成

GSRP を使用する場合の基本的なネットワーク構成を次の図に示します。

図 21-2 GSRP のネットワーク構成



GSRP の機能を動作させるスイッチを GSRP スイッチと呼びます。GSRP スイッチは 2 台のペアで GSRP グループを構成し、通常運用では片側がマスタ状態、もう一方がバックアップ状態として稼働します。GSRP ではこの 2 台の GSRP スイッチと周囲のスイッチとで三角形の構成を組むことを基本とします。

GSRP スイッチ同士の間は必ず直接接続する必要があります。この GSRP スイッチ間のリンクをダイレクトリンクと呼びます。

ダイレクトリンク上では GSRP Advertise フレームと呼ぶ状態確認用の制御フレームを送受信します。デフォルトの状態ではそのほかのデータフレームはブロッキングします。そのほかのデータフレームも送受信したい場合は、GSRP VLAN グループ限定制御機能を設定して、VLAN グループに所属しない VLAN を使用するか、ダイレクトリンクを GSRP 制御対象外ポートに設定します。レイヤ 3 冗長切替機能を使用する場合、GSRP スイッチ間の通常データ中継のためにダイレクトリンクを使用する場合があります。その際に GSRP VLAN グループ限定制御機能を使用するか、ダイレクトリンクを GSRP 制御対象外ポートに設定します。詳細は「21.4 レイヤ 3 冗長切替機能」および「21.5.3 レイヤ 3 冗長切替機能での上流ネットワーク障害による切り替え」を参照してください。

GSRP スイッチは GSRP Advertise フレームの送受信によって、GSRP スイッチは互いの状態を確認し、マスタ状態、バックアップ状態の切り替え制御を行います。マスタ状態とバックアップ状態の切り替えは、VLAN グループと呼ぶ複数の VLAN をまとめた一つの論理的なグループ単位で行います。

マスタ状態の GSRP スイッチは指定された VLAN グループのフレームをフォワーディングしますが、バックアップ状態の GSRP スイッチではブロッキングします。

21.2.2 GSRP 管理 VLAN

GSRP を利用するネットワークでは、GSRP の制御フレームの送信範囲を限定するため、専用の VLAN の設定が必要です。この VLAN を GSRP 管理 VLAN と呼びます。GSRP ではこの GSRP 管理 VLAN 上だけで制御フレームを送受信します。

GSRP スイッチはマスタ状態へ遷移する際、周囲のスイッチに向けて MAC アドレステーブルエントリのクリアを要求するため、GSRP Flush request フレームと呼ぶ制御フレームを送信します。このため、GSRP 管理 VLAN には、ダイレクトリンクのポートだけでなく VLAN グループに参加させるすべての VLAN のポートを設定する必要があります。また、周囲のスイッチでも GSRP の制御フレームを受信できるように、GSRP 管理 VLAN と同一の VLAN の設定をしておく必要があります。ただし、VLAN グループに参加させる VLAN のポートのうち、GSRP Flush request フレームの受信による MAC アドレステーブルのクリアをサポートしていないスイッチとの接続ポート、およびその対向のポートには、GSRP 管理 VLAN の設定をする必要はありません。

21.2.3 GSRP の切り替え制御

GSRP スイッチで切り替えを行う際、フレームに対するフォワーディングおよびブロッキングの切り替え制御を行うだけでは、エンド - エンド間の通信を即時に再開できません。これは、周囲のスイッチの MAC アドレステーブルにおいて、MAC アドレスエントリが切り替え前にマスタ状態であった GSRP スイッチ向けに登録されたままであるためです。通信を即時に再開するためには、GSRP スイッチの切り替えと同時に、周囲のスイッチの MAC アドレステーブルエントリをクリアする必要があります。

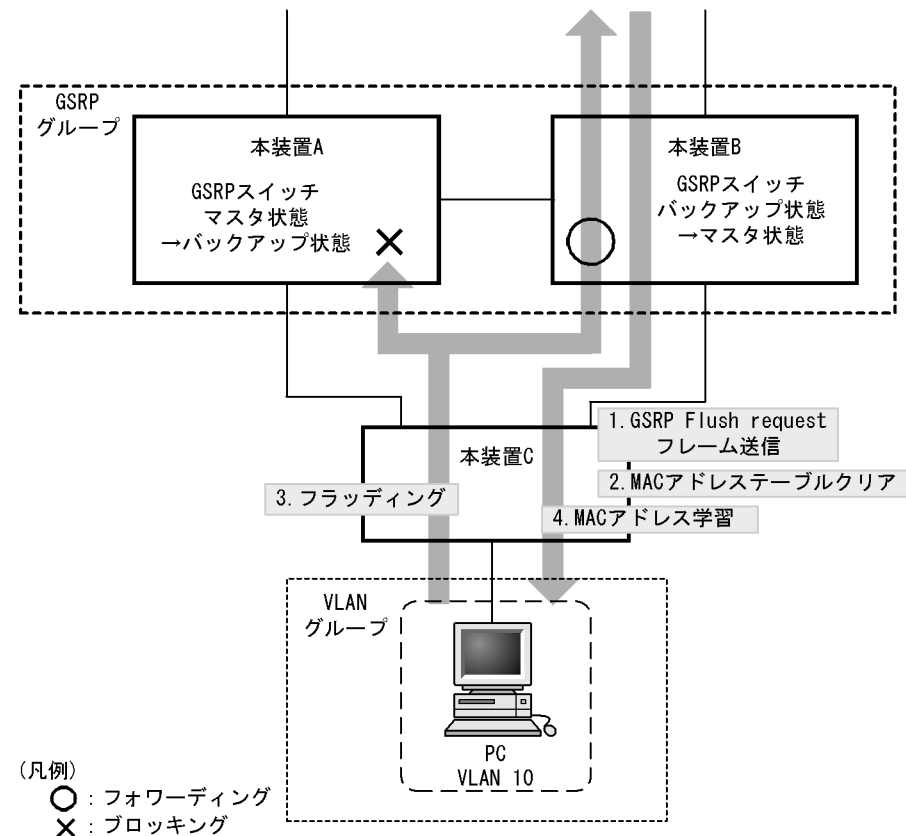
GSRP では、周囲のスイッチの MAC アドレステーブルエントリをクリアする方法として下記をサポートしています。

(1) GSRP Flush request フレームの送信

GSRP では切り替えを行うとき、周囲のスイッチに対して MAC アドレステーブルエントリのクリアを要求するため GSRP Flush request フレームと呼ぶ制御フレームを送信します。この GSRP Flush request フレームを受信して、自装置内の MAC アドレステーブルをクリアできるスイッチを GSRP aware と呼び

ます。本装置は特にコンフィグレーションの設定がないと、常に GSRP aware として動作します。GSRP aware は GSRP Flush request フレームをフラッディングします。一方、GSRP Flush Request フレームに対する機能をサポートしていないスイッチを GSRP unaware と呼びます。周囲のスイッチが GSRP unaware である場合は、「(2) ポートリセット機能」を使用する必要があります。GSRP Flush request フレームによる切り替え制御の概要を次の図に示します。

図 21-3 GSRP Flush request フレームによる切り替え制御の概要



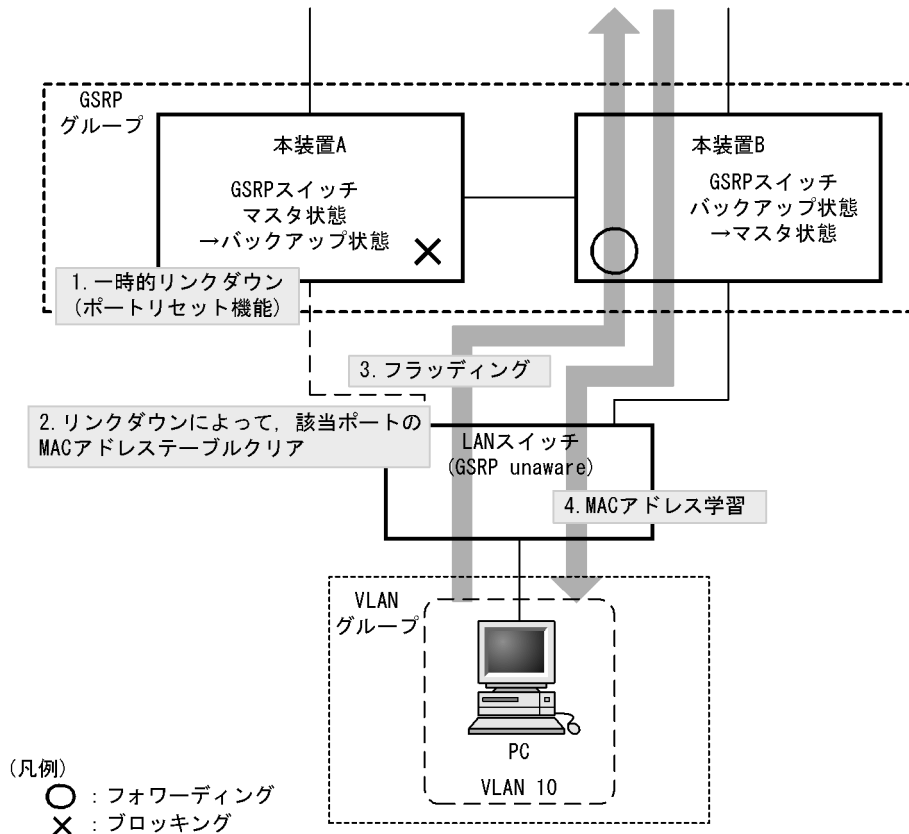
1. 本装置 A と本装置 B との間で切り替えが行われ、本装置 B は GSRP Flush request フレームを本装置 C へ向けて送信します。
2. 本装置 C は GSRP Flush request フレームを受けて、自装置内の MAC アドレステーブルをクリアします。
3. この結果、本装置 C 上は PC の送信するフレームに対して、MAC アドレス学習が行われるまでフラッディングを行います。
当該フレームは、マスタ状態である本装置 B を経由して宛先へフォワーディングされます。
4. 応答として PC 宛のフレームが戻ってくると、本装置 C は MAC アドレス学習を行います。
以後、本装置 C は PC からのフレームを本装置 B へ向けてだけフォワーディングするようになります。

(2) ポートリセット機能

ポートリセット機能は、GSRP スイッチにおいて周囲のスイッチと接続するリンクを一時的に切断する機能です。周囲のスイッチが GSRP unaware である場合に利用します。リンクの切断を検出したスイッチが、該当ポート上で学習した MAC アドレスエントリを MAC アドレステーブルからクリアする仕組みを利用します。

ポートリセット機能による切り替え制御の概要を次の図に示します。

図 21-4 ポートリセット機能による切り替え制御の概要



1. 本装置 A と本装置 B との間で切り替えが行われ、本装置 A はポートリセット機能によってリンクを切断します。
2. GSRP unaware である LAN スイッチ（以下、本説明内では単に GSRP unaware と表記します）はリンクダウンにより該当ポートの MAC アドレステーブルをクリアします。
3. この結果、GSRP unaware は PC の送信するフレームに対して、MAC アドレス学習が行われるまでフラッディングを行います。
当該フレームは、マスタ状態である本装置 B を経由して宛先へフォワーディングされます。
4. 応答として PC 宛のフレームが戻ってくると、GSRP unaware は MAC アドレス学習を行います。
以後、GSRP unaware は PC からのフレームを本装置 B へ向けてだけフォワーディングするようになります。

21.2.4 マスタ、バックアップの選択方法

(1) 選択基準

GSRP スイッチは GSRP Advertise フレームを周期的に送受信し、当該フレームに含む VLAN グループ単位の選択基準の情報によって、VLAN グループ単位でマスタ、バックアップを決定します。GSRP でサポートするマスタ、バックアップの選択基準を次の表に示します。

表 21-3 GSRP でサポートするマスタ，バックアップの選択基準

項目	内容
アクティブポート数	装置内の VLAN グループに参加している全 VLAN (コンフィグレーションコマンド state suspend を設定した VLAN を除く) の物理ポートのうち、リンクアップしている物理ポートの数です。アクティブポート数の多い方がマスタになります。リンクアグリゲーションを設定している場合は、チャンネルグループを 1 ポートとして換算します。
優先度	コンフィグレーションで指定する VLAN グループごとの優先度です。優先度の値の大きい方がマスタになります。
装置 MAC アドレス	装置の MAC アドレスです。MAC アドレス値の大きい方がマスタになります。

(2) 選択優先順

「(1) 選択基準」に示す選択基準の優先順をコンフィグレーションによって指定できます。指定できる順位を次に示します。

- アクティブポート数 優先度 装置 MAC アドレス (デフォルト)
- 優先度 アクティブポート数 装置 MAC アドレス

21.3 GSRP の動作概要

21.3.1 GSRP の状態

GSRP は五つの状態を持ち動作します。状態の一覧を次の表に示します。

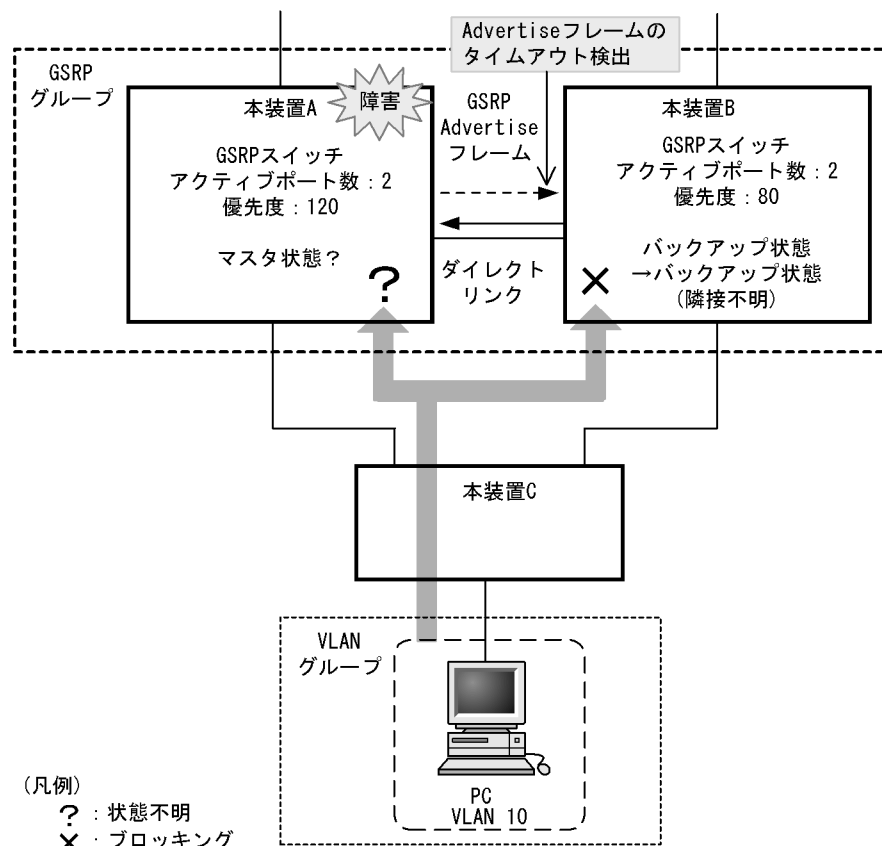
表 21-4 GSRP の状態一覧

状態	内容
バックアップ	バックアップ状態として稼働する状態です。バックアップ状態の GSRP スイッチは、VLAN グループ内の VLAN に対してポートごとにブロッキングします。GSRP 制御フレーム以外のフレームの中継は行わないため、MAC アドレス学習は行いません。初期稼働時は必ずバックアップ状態から開始します。
バックアップ (マスタ待ち)	バックアップ状態からマスタ状態へ切り替わる際、対向の GSRP スイッチが確実にバックアップ状態、またはバックアップ (固定) 状態であることを確認するための過渡的な状態です。バックアップ (マスタ待ち) 状態では、バックアップ状態と同様、GSRP 制御フレーム以外のフレームの中継は行いません。
バックアップ (隣接不明)	バックアップ状態、およびバックアップ (マスタ待ち) 状態で、対向の GSRP スイッチからの GSRP Advertise フレームの受信タイムアウトを検出した際に遷移する状態です。対向の GSRP スイッチはマスタ状態として稼働中の可能性があるため、GSRP Advertise フレームを再受信する、または運用コマンド <code>set gsrp master</code> によってマスタ状態へ遷移させる以外は、本状態のままです。バックアップ (隣接不明) 状態では、バックアップ状態と同様、GSRP 制御フレーム以外のフレームの中継は行いません。
バックアップ (固定)	コンフィグレーションによって強制的にバックアップ固定にされた状態です。コンフィグレーションが削除されるまで、本状態のままです。バックアップ (固定) 状態では、バックアップ状態と同様、GSRP 制御フレーム以外のフレームの中継は行いません。
マスタ	マスタ状態として稼働する状態です。マスタ状態の GSRP スイッチは、VLAN グループ内の VLAN に対してポートごとにフォワーディングします。GSRP 制御フレームを含むすべてのフレームの中継を行い、MAC アドレス学習を行います。

21.3.2 装置障害時の動作

装置障害時の動作例を次の図に示します。

図 21-5 装置障害時の動作



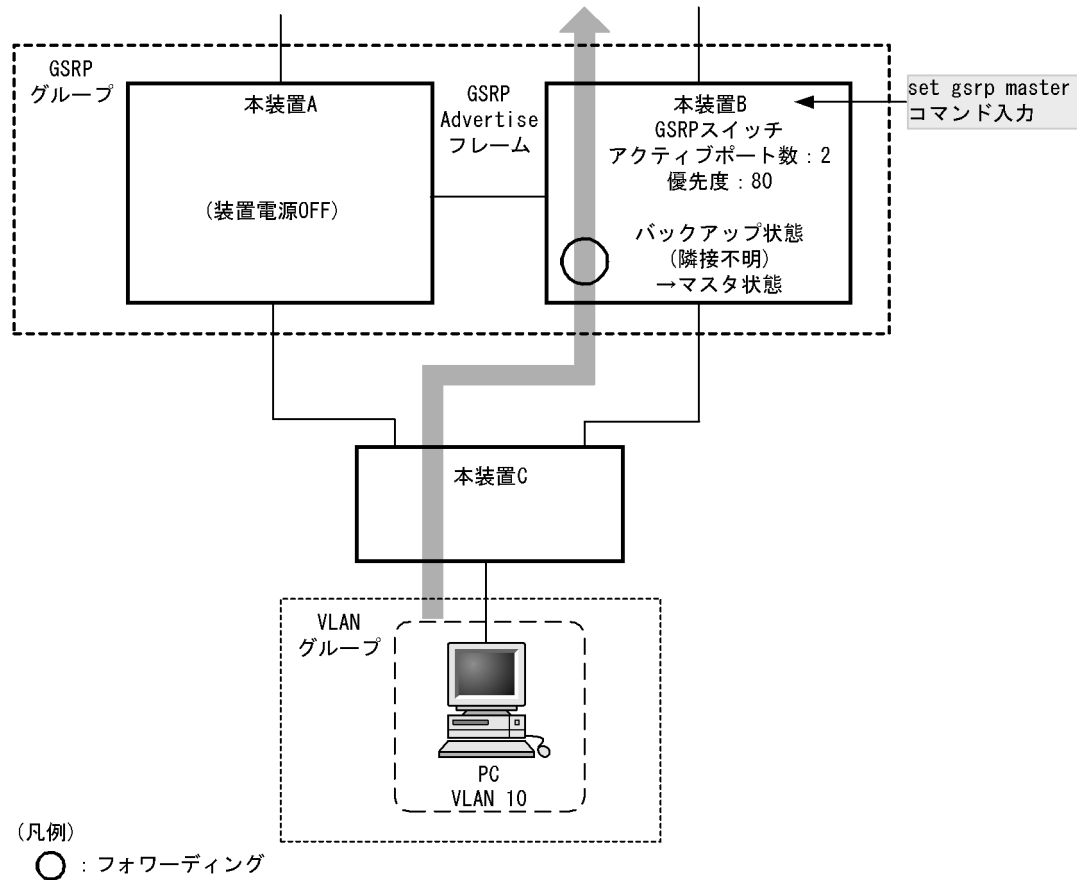
装置障害などが発生したことによって、マスタ状態の本装置 A が GSRP Advertise フレームを正常に送信できなくなった場合、本装置 B は本装置 A から GSRP Advertise フレームの受信タイムアウトを検出します。このとき、本装置 B はバックアップ（隣接不明）状態に移ります。バックアップ（隣接不明）状態では、バックアップ状態と同様に、フレームの中継は行いません。バックアップ（隣接不明）状態になった場合、メッセージを出力し、運用者に対して装置の状態の確認を促します。

GSRP では、バックアップ（隣接不明）状態となった本装置 B をマスタ状態へ切り替える手段として、手動で切り替える方法と自動的に切り替える方法の二つをサポートしています。

(1) 手動による切り替え（運用コマンドによる切り替え）

GSRP では手動でマスタ状態へ切り替えるための運用コマンド `set gsrp master` をサポートしています。運用者は本装置 A のポートがブロッキングされていること、または装置が起動していないことを確認したうえで、本コマンドを使用することによって本装置 B をマスタ状態に移させることができます。運用コマンド `set gsrp master` 入力後の動作を次の図に示します。

図 21-6 運用コマンド set gsrp master 入力後の動作



(2) 自動での切り替え (ダイレクトリンク障害検出による切り替え)

自動での切り替えを行う機能として、ダイレクトリンク障害検出機能をサポートしています。また、ダイレクトリンク障害検出機能では対象外となる、装置起動時も自動で切り替えを行う GSRP スイッチ単独起動時のマスタ遷移機能もサポートしています。

- ダイレクトリンク障害検出機能**
 ダイレクトリンク障害検出機能を動作させるには、コンフィグレーションコマンド `no-neighbor-to-master` でパラメータ `direct-down` を指定します。
 本機能は、装置起動後、対向装置からの GSRP Advertise フレームを受信したあとで有効になります。VLAN グループがバックアップ (隣接不明) 状態に遷移した際、ダイレクトリンクのポートがダウン状態であれば、対向装置が装置障害状態であるとみなして、自動的にマスタ状態へ遷移します。
 装置起動時¹ から対向装置からの GSRP Advertise フレームを受信するまでは、対向装置の状態が不明のため、ダイレクトリンク障害検出機能による自動での切り替えは行いません。マスタとして動作させたい場合は、手動で切り替えてください。装置起動時など、対向装置からの GSRP Advertise フレームを受信していないときにも自動で切り替えたい場合は、GSRP スイッチ単独起動時のマスタ遷移機能を使用することによって、マスタへ遷移させることもできます。
- GSRP スイッチ単独起動時のマスタ遷移機能**
 GSRP スイッチ単独起動時のマスタ遷移機能を動作させるには、コンフィグレーションコマンド `no-neighbor-to-master` でパラメータ `direct-down forced-shift-time` を指定します。
 本機能は、対向となる GSRP スイッチが障害などによって起動せず、装置起動時² からダイレクトリンクがアップしていない時にだけ動作します。

GSRP スイッチ単独起動時のマスタ遷移機能を開始する条件³をすべて満たすと自動マスタ遷移待ち状態になり、パラメータ `forced-shift-time` で設定する自動マスタ遷移待ち時間経過後に自動的にマスタ状態へ遷移します。

自動マスタ遷移待ち状態では、運用コマンド `clear gsrp forced-shift` によって、自動マスタ遷移待ち状態を解除して VLAN グループが自動的にマスタ遷移する動作を抑止できます。

本機能は、対向装置の状態が不明なままマスタに遷移させることとなります。自動的にマスタとして動作するまでの時間は、対向装置のポートがブロッキングされていること、または装置が起動していないことを十分に保障できる時間を設定してください。

注 1

次の動作が行われたときも、装置起動時と同じ動作になります。

- 系切替
- 運用コマンド `restart vlan` の実行
- 運用コマンド `restart gsrp` の実行
- コンフィグレーションコマンド `gsrp` の `no-neighbor-to-master` で `direct-down` を指定
- コンフィグレーションコマンド `gsrp` の `direct-link` によるダイレクトリンクポートの設定
- 運用コマンド `copy` によるランニングコンフィグレーションへの反映
- 運用コマンド `inactivate bsu` の実行によって、すべての BSU が `inactivate` 状態【AX6700S】

注 2

次の動作が行われたときも、装置起動時と同様に GSRP スイッチ単独起動時のマスタ遷移機能が動作します。

- 系切替
- 運用コマンド `restart vlan` の実行
- 運用コマンド `restart gsrp` の実行
- 運用コマンド `copy` によるランニングコンフィグレーションへの反映
- 運用コマンド `activate bsu` の実行によって、最初の BSU が `activate` 状態【AX6700S】

注 3

GSRP スイッチ単独起動時のマスタ遷移機能を開始する条件を次に示します。

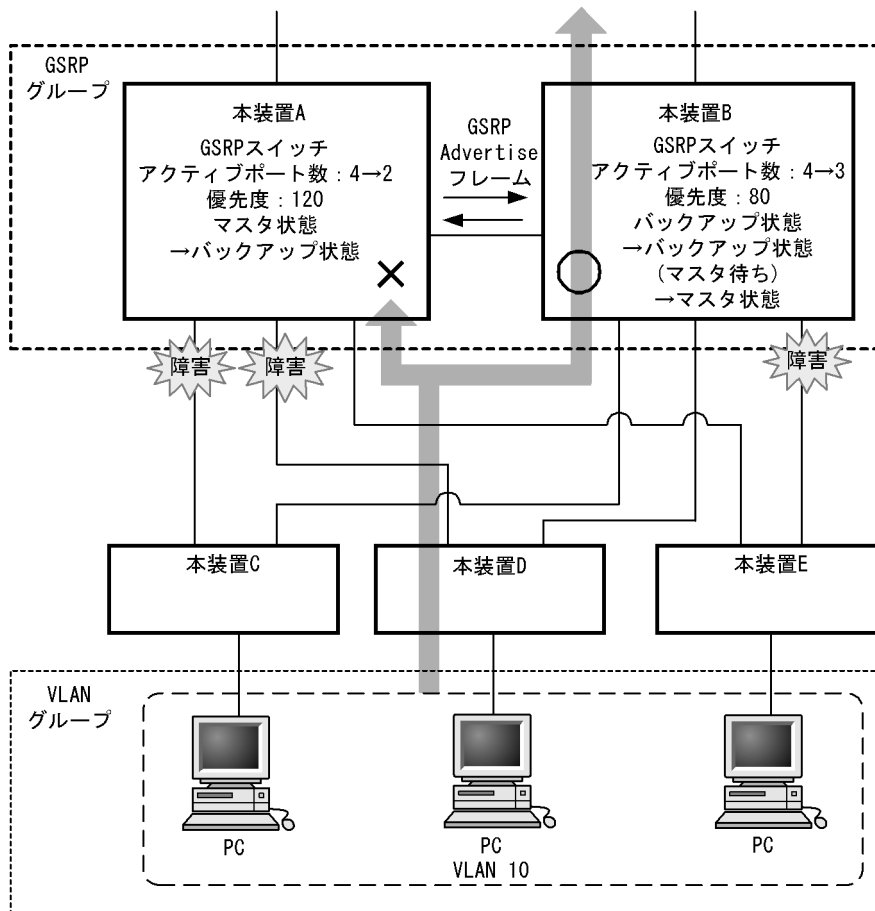
- GSRP Advertise フレームの受信タイムアウトが発生
- 本装置に設定されている VLAN グループのどれかのメンバポートがアップ

21.3.3 リンク障害時の動作

(1) リンク障害時の動作例

リンク障害時の動作例を次の図に示します。

図 21-7 リンク障害時の動作例



(凡例)

- : フォワーディング
- × : ブロッキング

この図では、本装置 A がマスタ状態、本装置 B がバックアップ状態として稼働している状況で、本装置 A と本装置 C、および本装置 D の間のリンクと、本装置 B と本装置 E の間のリンクで障害が発生した場合を示しています。本装置 A、および本装置 B で、マスタ、バックアップの選択優先順としてアクティブポート数を最優先とした設定をしている場合、本装置 B は、アクティブポート数が本装置 A よりも多くなるため、マスタになることを選択します。本装置 B は、マスタ状態へ遷移する前に、いったんバックアップ（マスタ待ち）状態へ遷移します。バックアップ（マスタ待ち）状態へ遷移した本装置 B は、本装置 A からの GSRP Advertise フレームを待ちます。GSRP Advertise フレームを受信したら、本装置 A がバックアップ状態であることを確認したうえで、マスタ状態へ遷移します。なお、この図に示す例では、本装置 E はマスタ状態である本装置 B との間のリンクが障害となっているため、通信ができなくなります。

(2) リンク不安定時の連続切り替え防止機能

GSRP では、マスタ状態とバックアップ状態の選択基準としてアクティブポート数を用います。そのため、リンクのアップ、ダウンが頻発するなどリンクが不安定な状態となった場合にアクティブポート数の増減が多発し、その結果、マスタ状態とバックアップ状態の切り替えが連続して発生するおそれがあります。

そのため、GSRP ではリンクが安定化したことを運用者が確認できるまでの間、アップしたリンクのポートをアクティブポート数としてカウントしないようにするための遅延時間をコンフィグレーションコマンド `port-up-delay` で設定できます。これによって、リンク不安定時の不用意な切り替えを抑制できます。

port-up-delay コマンドでは 1 から 43200 秒（12 時間）内で 1 秒単位に指定できます。また、infinity と設定することで、遅延時間を無限とすることもできます。リンクが安定したことを確認できた場合、port-up-delay コマンドで指定した遅延時間を待たないですぐにアクティブポート数としてカウントするための運用コマンド clear gsrp port-up-delay もサポートしています。

21.3.4 バックアップ固定機能

バックアップ固定機能によって、GSRP スイッチを強制的にバックアップ状態にすることができます。コンフィグレーションコマンド backup-lock によって、バックアップ（固定）状態になり、コンフィグレーションが削除されるまで本状態のままです。バックアップ（固定）状態では、バックアップ状態と同様、GSRP 制御フレーム以外のフレームの中継は行いません。

21.3.5 GSRP VLAN グループ限定制御機能

コンフィグレーションコマンド gsrp limit-control によって、GSRP の制御対象を VLAN グループに所属する VLAN に限定して運用できます。VLAN グループに所属しない VLAN は、GSRP の制御対象外になり、常時通信可能な VLAN となります。

21.3.6 GSRP 制御対象外ポート

コンフィグレーションコマンド gsrp exception-port によって、指定したポートを GSRP 制御対象外ポートとして運用できます。GSRP 制御対象外ポートにすることで、マスタ/バックアップ状態に関係なく、常時通信可能なポートとなります。

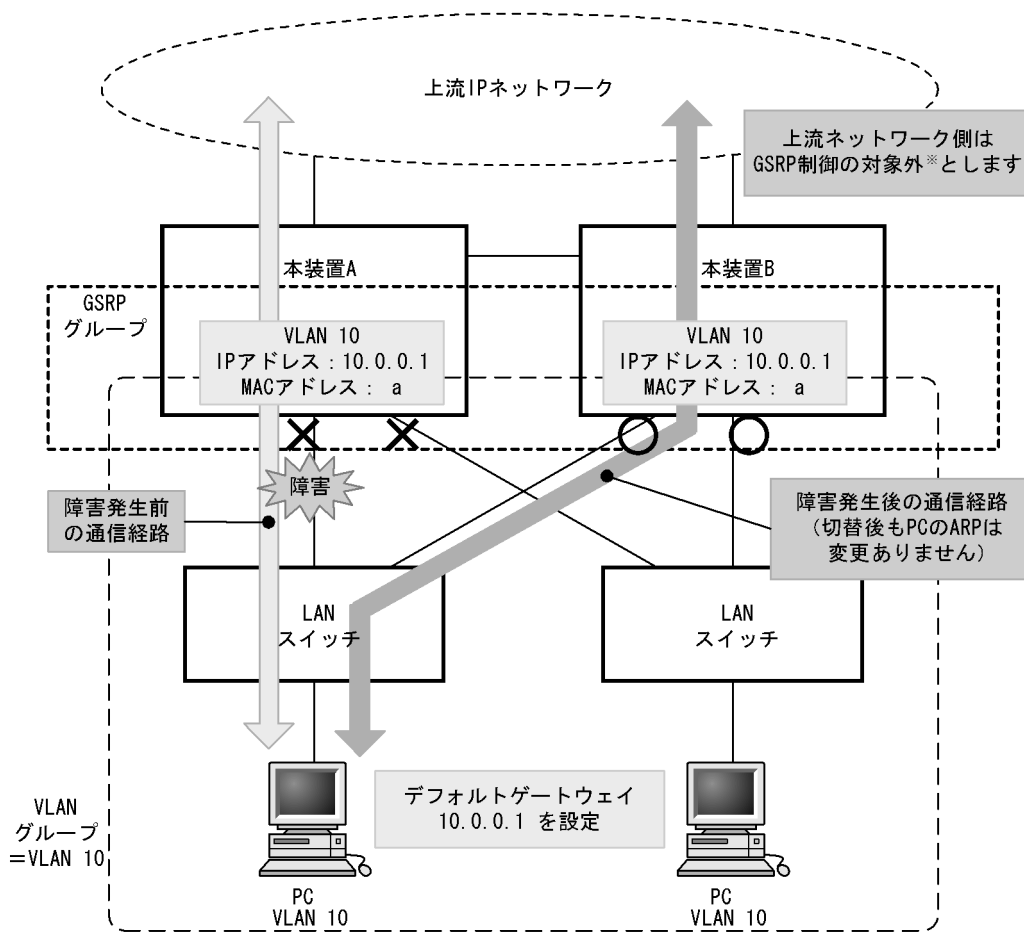
21.4 レイヤ 3 冗長切替機能

21.4.1 概要

レイヤ 3 冗長切替機能は、2 台のスイッチが同一の IP アドレスと MAC アドレスを引き継いで切り替えることで、PC などからのデフォルトゲートウェイを経由した通信を継続できるようにします。

GSRP レイヤ 3 冗長切替機能の概要を次の図に示します。なお、ここでは PC などを接続するネットワークを下流ネットワークと呼び、そこから IP 中継する先のネットワークを上流ネットワークと呼びます。GSRP のマスタ/バックアップ切り替えは下流ネットワーク側に反映します。

図 21-8 GSRP レイヤ 3 冗長切替機能の概要



(凡例)

- : フォワーディング
- × : ブロッキング

注※ GSRP制御の対象外とするには次の方法があります。

- ・ 該当ポートにGSRP制御対象外ポートを設定する
- ・ GSRP VLANグループ限定制御機能を適用し、VLANグループに所属していないVLANを使用する

(1) デフォルトゲートウェイの IP アドレス

GSRP で冗長化するデフォルトゲートウェイの IP アドレスは、2 台の GSRP スイッチで同じ VLAN に同じアドレスを設定します。マスタ状態の GSRP スイッチは VLAN がアップ状態となり、デフォルトゲ

トウェイとして IP 中継を行います。バックアップ状態の GSRP スイッチの VLAN はダウン状態となり IP 中継を行いません。

(2) デフォルトゲートウェイの MAC アドレス

GSRP で冗長化するデフォルトゲートウェイの MAC アドレスは GSRP のプロトコル専用の仮想 MAC アドレスを使用します。仮想 MAC アドレスは、VLAN グループ ID ごとに異なるアドレスを使用します。

マスタ状態の装置は、下流の LAN スイッチに仮想 MAC アドレスを学習させるために、仮想 MAC アドレスを送信元 MAC アドレスとした GSRP 制御フレームを定期的送信します。

GSRP で使用する仮想 MAC アドレスを次の図と表に示します。

VLAN グループ ID が 8 以下の場合には、次に示す方法で仮想 MAC アドレスを生成します。

図 21-9 GSRP レイヤ 3 冗長切替機能の仮想 MAC アドレスの生成方法 (VLAN グループ ID が 8 以下)

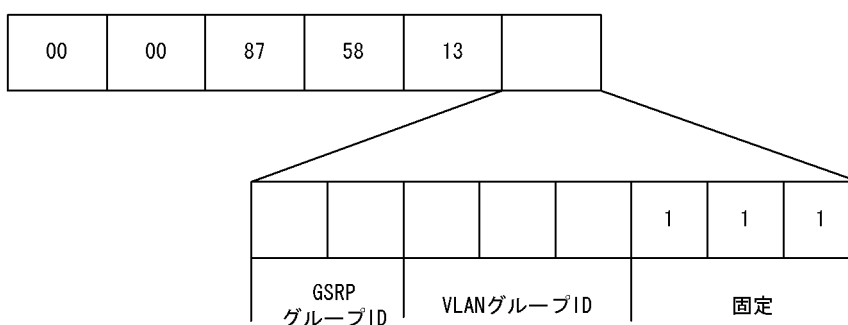


表 21-5 GSRP レイヤ 3 冗長切替機能の仮想 MAC アドレスの生成方法 (VLAN グループ ID が 8 以下)

項目	値
GSRP グループ ID	GSRP グループ ID1 ~ 4 に対して、0 ~ 3 の値を設定します。レイヤ 3 冗長切替機能では、GSRP グループ ID は 1 ~ 4 の値である必要があります。
VLAN グループ ID	VLAN グループ ID1 ~ 8 に対して、0 ~ 7 の値を設定します。
固定 (3 ビット)	最下位 3 ビットは 7 固定とします。

VLAN グループ ID が 9 以上の場合には、0000.8758.1311 ~ 0000.8758.1399 の範囲の仮想 MAC アドレスを VLAN グループ ID 9 ~ 128 に順番に割り当てます。

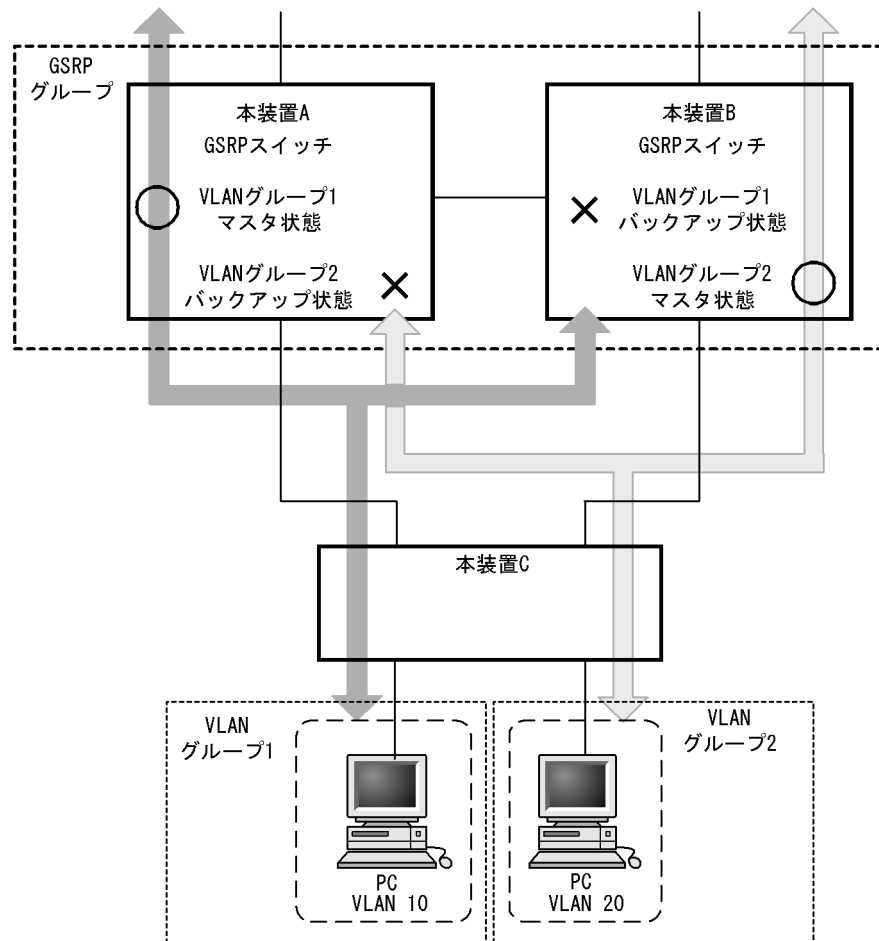
21.5 GSRP のネットワーク設計

21.5.1 VLAN グループ単位のロードバランス構成

GSRP では、VLAN グループ単位にマスタ状態、バックアップ状態の状態管理を行います。1 台の GSRP スイッチで最大 128 個の VLAN グループまで設定できます。複数の VLAN グループを同居させることで、VLAN グループ単位のロードバランス構成をとり、トラフィックの負荷分散を図ることができます。ロードバランス構成の概要を次の図に示します。

この図では、本装置 A が VLAN グループ 1 に対してマスタ状態、VLAN グループ 2 に対してバックアップ状態で動作、また本装置 B が VLAN グループ 1 に対してバックアップ状態、VLAN グループ 2 に対してマスタ状態で動作している例を示しています。

図 21-10 ロードバランス構成



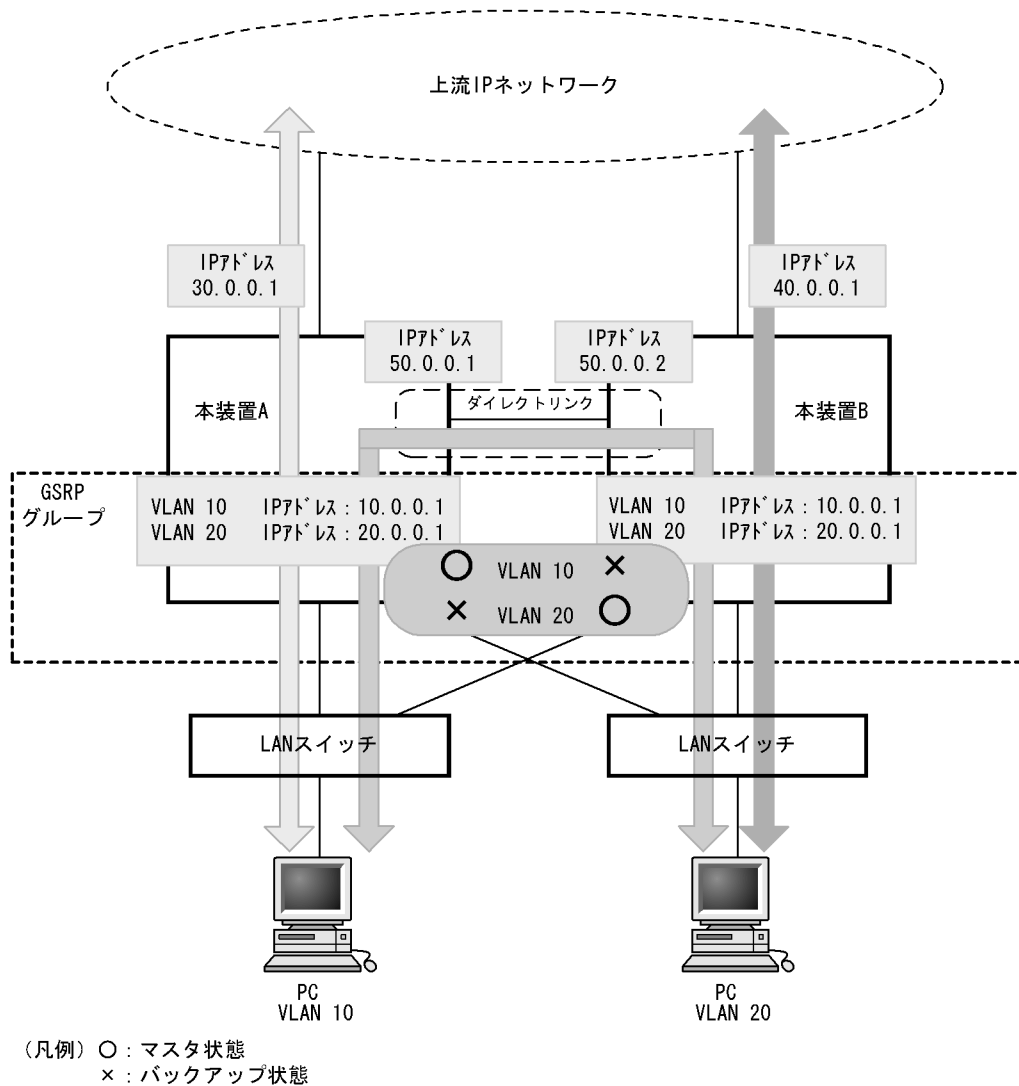
(凡例)

- : フォワーディング
- × : ブロッキング

レイヤ 3 冗長切替機能でロードバランス構成をとると、異なる装置がマスタ状態の VLAN 間で通信するためには GSRP スイッチ間で通信経路を確保する必要があります。この通信は、「21.5.3 レイヤ 3 冗長切替機能での上流ネットワーク障害による切り替え」で示したダイレクトリンク上の VLAN で行います。レイヤ 3 冗長切替機能を使用する場合のロードバランス構成の概要を次の図に示します。

この図では、本装置 A が VLAN 10 に対してマスタ状態、本装置 B が VLAN 20 に対してマスタ状態で作っています。上流 IP ネットワークへの通信はそれぞれマスタ状態の装置を経由します。VLAN10 と VLAN20 の間での通信はダイレクトリンク上の VLAN を経由します。

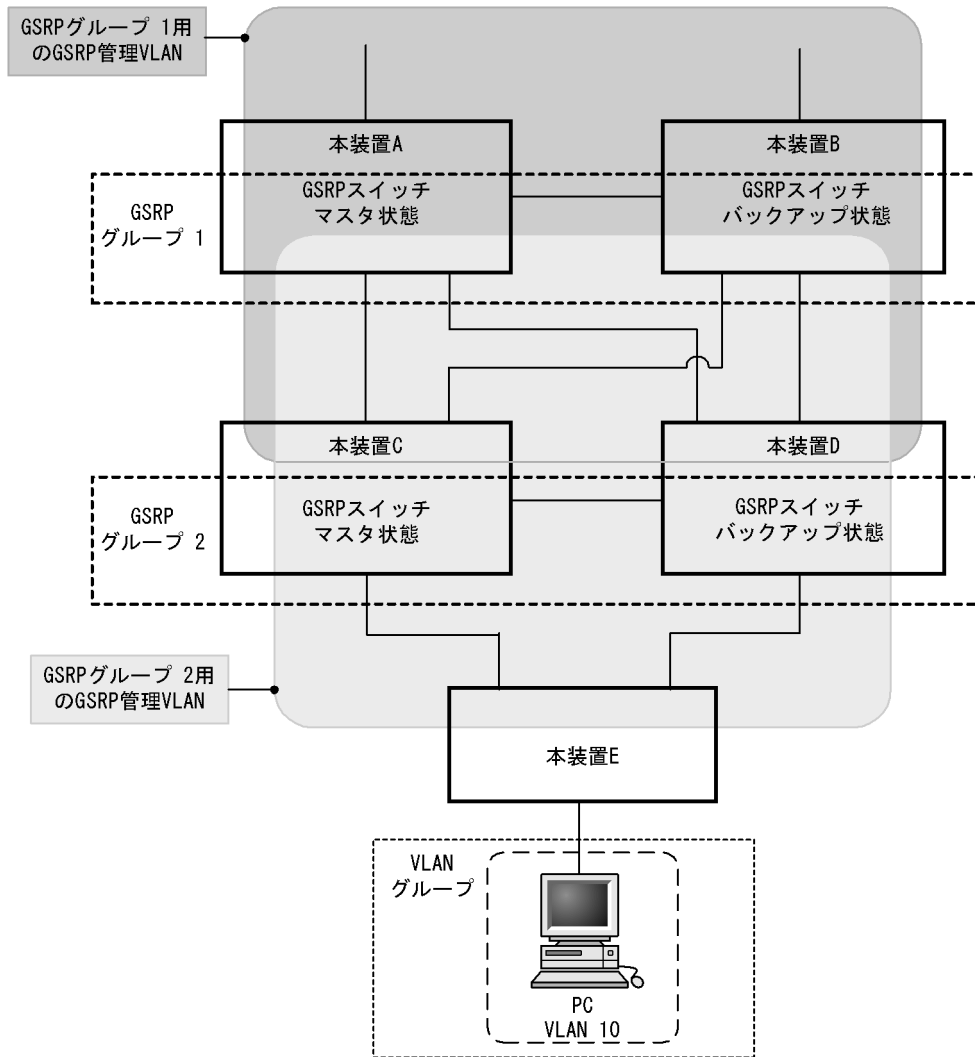
図 21-11 レイヤ 3 冗長切替機能使用時のロードバランス構成



21.5.2 GSRP グループの多段構成

GSRP では、同一のレイヤ 2 ネットワーク内に複数の GSRP グループを多段にした構成をとることができます。これによって大規模ネットワークでも、冗長性を確保できます。GSRP グループを多段構成にする場合、GSRP の制御フレームの送信範囲を限定するため、GSRP グループごとに GSRP 管理 VLAN を設定します。GSRP グループの多段構成の概要を次の図に示します。

図 21-12 GSRP グループの多段構成



この図では、本装置 A と本装置 B で GSRP グループ 1 を、本装置 C と本装置 D で GSRP グループ 2 を構成したケースを示しています。各 GSRP グループはそれぞれ独立して動作するため、ある GSRP グループでマスタ状態とバックアップ状態の切り替えが発生しても、ほかの GSRP グループでの動作には影響しません。GSRP 管理 VLAN は GSRP スイッチを中心に周囲のスイッチを含めた VLAN として設定します。

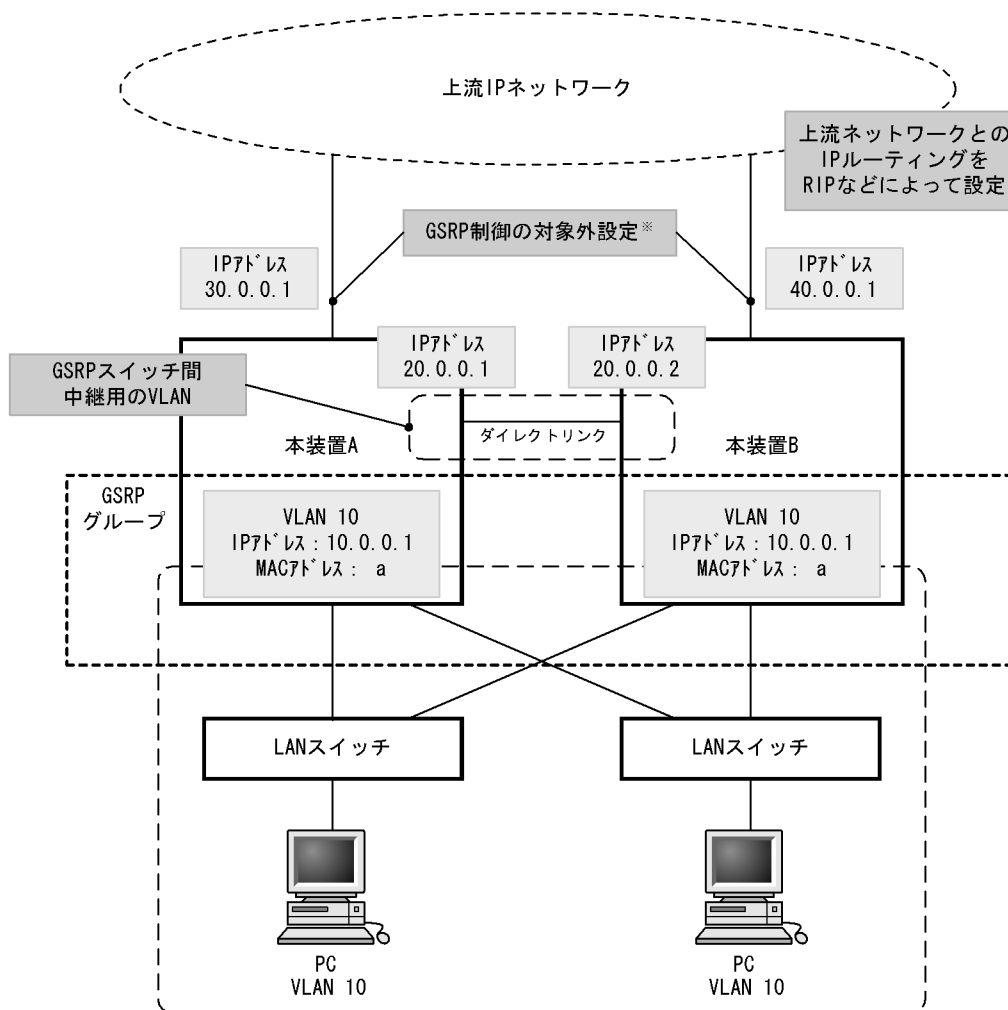
21.5.3 レイヤ 3 冗長切替機能での上流ネットワーク障害による切り替え

上流ネットワーク側は GSRP の制御対象から外し、IP ルーティングを設定します。レイヤ 3 冗長切替機能を使用する場合、上流ネットワーク側の障害は IP ルーティング機能によって検出して経路を切り替えます。

上流ネットワーク側は、2 台の GSRP スイッチがどちらも上流ネットワークへ接続し、また一方のポートなどに障害が発生した場合はもう一方の GSRP スイッチを経由して通信を継続できるように GSRP スイッチ間の通信経路も確保します。

上流ネットワークの障害に対応した設定の概要と、障害時の通信経路の例を、次の図に示します。

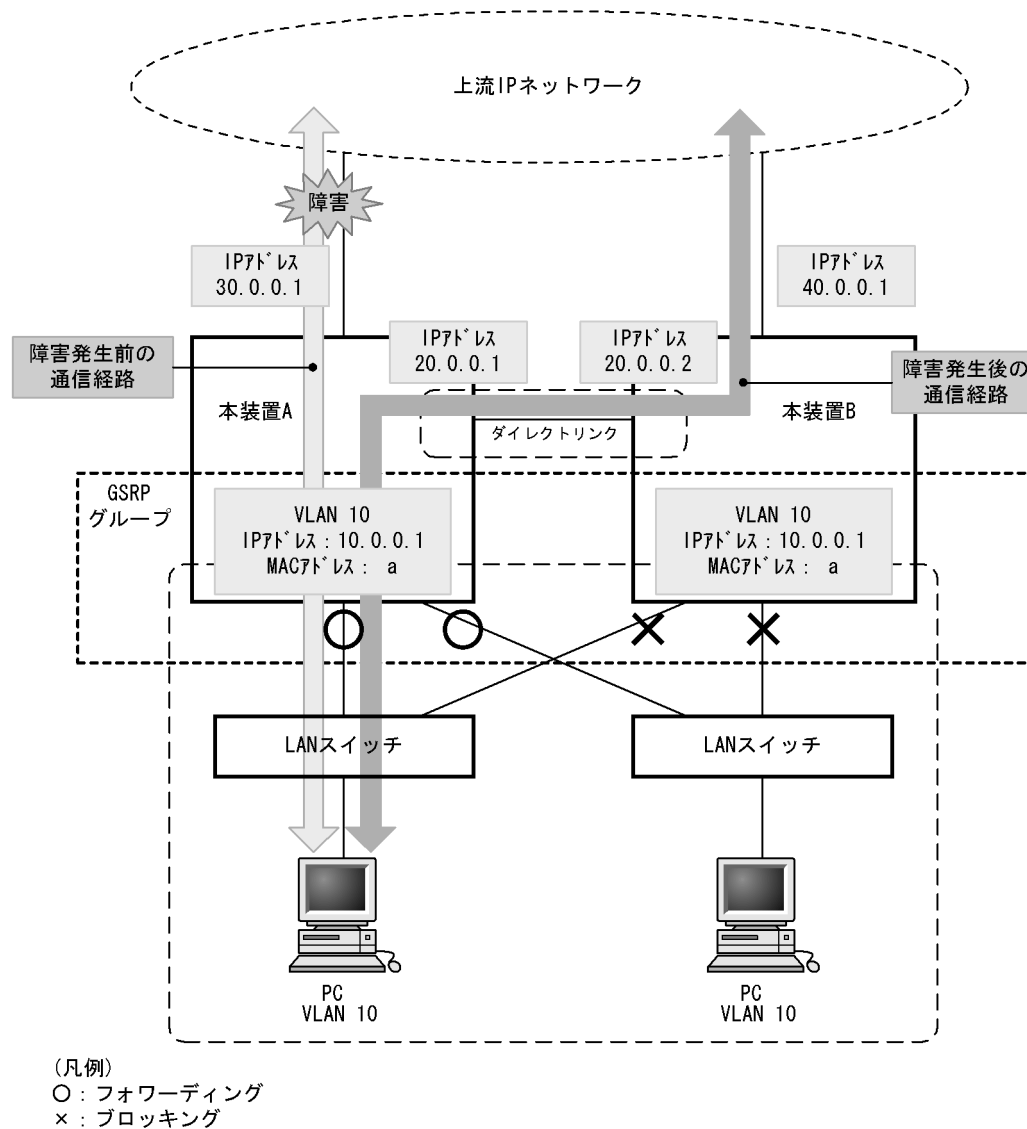
図 21-13 上流ネットワークの障害に対応した設定



注※ GSRP制御の対象外とするには次の方法があります。

- ・ 該当ポートにGSRP制御対象外ポートを設定する
- ・ GSRP VLANグループ限定制御機能を適用し、VLANグループに所属していないVLANを使用する

図 21-14 上流ネットワークの障害発生時の通信経路



（1）上流ネットワーク側の設定

次に示す方法で、上流ネットワーク側のポートまたは VLAN をマスタ/バックアップどちらの状態でも通信可能とします。

- 上流ネットワーク側のポートを、GSRP 制御対象外ポート（コンフィグレーションコマンド `gsrp exception-port`）として設定する
- GSRP VLAN グループ限定制御機能（コンフィグレーションコマンド `gsrp limit-control`）を適用して、上流ネットワーク側の VLAN を、VLAN グループに所属しない GSRP の制御対象外の VLAN とする

そこに IP アドレスおよび IP ルーティングを設定することで上流ネットワークと接続します。

IP ルーティングは、2 台の GSRP スイッチがどちらも上流ネットワークと通信できるように設定します。また、上流ネットワーク向けの障害を検出できるように、ダイナミックルーティングまたはスタティックルーティングの動的監視機能を設定します。

通常は、上流ネットワークとの通信を各 GSRP スイッチが直接行うようにします。上流ネットワーク側で

障害が発生した場合に、隣接の GSRP スイッチを経由して上流ネットワークとの通信が継続できるようにします。そのために、上流ネットワークへの経路が隣接する GSRP スイッチを経由する場合の方が優先度が低くなるように IP ルーティングを設定します。また、スタティックルーティングの場合は障害を検出するために動的監視機能を設定して、到達確認を定期的に行うようにします。

(2) GSRP スイッチ間の設定

上流ネットワークとは 2 台の GSRP スイッチ両方を通信可能な状態とするため、バックアップ側の GSRP スイッチに上流ネットワークからパケットが届く場合があります。そのようなパケットをマスタ側の GSRP スイッチに中継するために、GSRP スイッチ間にレイヤ 3 での通信経路を設定します。

GSRP スイッチ間はダイレクトリンクを接続し、GSRP 管理 VLAN 上で GSRP Advertise フレームのやり取りをします。このダイレクトリンク上に GSRP 管理 VLAN 以外の VLAN と IP ルーティングを設定することで、GSRP スイッチ間の中継ができます。ただし、下流からのトラフィックを直接上流ネットワークに中継するために、GSRP スイッチ間の中継する経路は優先度の低い経路となるように IP ルーティングを設定してください。

21.6 GSRP 使用時の注意事項

(1) 他機能との共存について

GSRP との共存で制限のある機能を次の表に示します。

表 21-6 GSRP との共存で制限のある機能

制限のある機能	制限の内容
シングルスパニングツリー	共存不可
PVST+	
マルチプルスパニングツリー	
VRRP	
IEEE802.1X	

(2) ポートリセット機能を使用する場合について

ポートリセット機能を設定したポートと対向のスイッチとの間に伝送装置などを設置した場合、対向のスイッチで正しくポートのリンクダウンを検出できないおそれがあります。

ポートリセット機能を使用する場合は、対向のスイッチでポートのリンクダウンが直接検出できるようにネットワークの設計を行ってください。

(3) ポートリセット機能をロードバランス構成で使用する場合について

同一のポートを複数の VLAN グループで共有し、かつその物理ポートに対してポートリセット機能を設定した場合、ある VLAN グループでマスタ状態からバックアップ状態に切り替わった際、別の VLAN グループではマスタ状態として稼働しているにもかかわらずポートのリンクをダウンさせるため通信断となります。このダウンによる一時的な通信断を回避したい場合は、複数の VLAN グループで同一の物理ポートを共有しないようにネットワークの設計をしてください。

ポートリセット機能によって一時的にダウンさせているポートは、マスタ、バックアップの選択ではアクティブポートとして扱います。マスタ状態として稼働している VLAN グループのマスタ、バックアップの選択には影響しません。

(4) GSRP 使用時の VLAN 構成について

GSRP 使用時は、すべての VLAN が GSRP によって制御されます。そのため、VLAN グループに属していない VLAN のポートは、ブロッキング状態になります。VLAN グループに属している VLAN だけを制御する場合は、GSRP VLAN グループ限定制御機能を使用してください。

(5) GSRP VLAN グループ限定制御機能について

次に示す動作が行われた場合、GSRP VLAN グループ限定制御機能を設定していても、すべての VLAN が一時的にダウンします。このとき VLAN のポートはブロッキング状態になります。

- 系切替
- コンフィグレーションコマンド `gsrp` で、GSRP グループ ID を設定
- 運用コマンド `restart gsrp` の実行

(6) ダイレクトリンク障害検出機能について

ダイレクトリンクで本装置との間に伝送装置などを設置した構成で伝送装置の障害が発生した場合、マスタ状態で稼働中の本装置は正常に動作しているにもかかわらず、バックアップ状態で稼働中の別の本装置は対向の本装置で障害が発生したと認識し、自動でマスタ状態へ切り替わる可能性があります。この結果、2台の本装置で同時にマスタ状態となります。また、ダイレクトリンクの片線切れ障害が発生した場合でも同様の現象が発生するおそれがあります。そのため、コンフィグレーションコマンド `no-neighbor-to-master` で `direct-down` を指定する場合は、ダイレクトリンクを冗長構成にし、複数経路で GSRP advertise フレームの送受信ができるようネットワークの設計をしてください。なお、ダイレクトリンクを冗長構成にするためには、リンクアグリゲーションを使用する方法、通常のポートを複数使用する方法などがありますが、どちらも効果は同じです。

レイヤ 3 冗長切替機能でダイレクトリンク上の VLAN を通信に用いる場合、ダイレクトリンクを冗長構成にするときは、リンクアグリゲーションを使用してください。

(7) GSRP 使用時のネットワークの構築について

GSRP 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。フレームのループを防止するため、GSRP を使用するネットワークの構築時には、次に示すような対応をしてください。

- GSRP のコンフィグレーションを設定する際、事前に本装置のポートを `shutdown` に設定するなどダウン状態にしてください。コンフィグレーション設定後、GSRP の状態遷移が安定したあとで、運用を開始してください。
- GSRP グループを構成する 2 台の本装置のうち 1 台だけを起動させて、コンフィグレーションを設定し、バックアップ状態に切り替わったことを確認したあとで、もう一方の GSRP スイッチを起動してコンフィグレーションを設定してください。
- GSRP VLAN グループ限定制御機能を設定している場合、VLAN グループに属していない VLAN はアップ状態です。VLAN グループに VLAN を所属させる場合は、その VLAN の状態をあらかじめ `disable` にして、VLAN グループの状態が定まったあとに VLAN の状態を `enable` にしてください。VLAN グループから VLAN を削除する場合も、その VLAN の状態をあらかじめ `disable` にして、ループが発生しないように運用してください。

(8) GSRP 使用中の VLAN 構成の変更について

GSRP では、マスタ状態とバックアップ状態の選択基準としてアクティブポート数を使います。アクティブポート数は VLAN グループに所属している VLAN のポート数であり、VLAN にポートを追加するときやネットワーク構成を変更するときは、アクティブポート数の増減が伴います。このようなとき、通常はマスタ状態およびバックアップ状態の両方の装置に同じ変更が反映されますが、作業中、一時的にバックアップ状態の装置のアクティブポート数がマスタ状態の装置を超えると、マスタ状態とバックアップ状態の切り替えが発生します。

このような切り替えを防止するためには、VLAN の構成を変更する際には次に示すような対応をください。

- マスタ、バックアップの選択基準の優先順（コンフィグレーションコマンド `selection-pattern`）を、優先度を最高優先順とするように設定し、優先度の設定でマスタを固定にした状態でコンフィグレーションを設定してください。
- ケーブル配線の変更や装置の再起動を伴うような大きな構成変更が必要な場合などには、バックアップ固定機能を使って片方の GSRP スイッチを強制的にバックアップ状態にし、もう一方の GSRP スイッチをすべての VLAN グループのマスタとした状態で構成変更を行ってください。

(9) GSRP unaware での GSRP の制御フレームの中継について

GSRP スイッチの周囲のスイッチが GSRP unaware である場合、GSRP の制御フレームはフラッディングされます。この結果、トポロジー上、不要なところまで制御フレームが中継されていくおそれがあります。制御フレームの不要な中継を防止するため、GSRP unaware でも GSRP 管理 VLAN を正しく設定してください。

(10) GSRP Flush request フレームの中継について

GSRP aware は GSRP Flush request フレームをフラッディングします。GSRP aware で GSRP Flush request フレームを中継させるネットワーク構成では、GSRP aware のソフトウェアバージョンを Ver.10.4 以降にする必要があります。GSRP スイッチは GSRP Flush request フレームをフラッディングしないので、GSRP グループの多段構成などで GSRP スイッチでの GSRP Flush request フレームを中継させる構成はできません。

(11) GSRP 使用時の本装置のリモート管理について

GSRP を使用する本装置に対して、telnet や SNMP などのリモート管理をする場合、次に示す方法を使用してください。

- マネージメントポート
- GSRP 制御対象外ポート
- GSRP VLAN グループ限定制御機能を設定し、VLAN グループに属さない VLAN の VLAN インタフェース

(12) GSRP 制御対象外ポートについて

GSRP 制御対象外ポートに設定したポートは、マスタ/バックアップ状態に関係なく、常時通信可能なポートとなります。このため、GSRP 制御対象外ポートに設定したポートに属する VLAN の IP インタフェースもアップ状態となります。レイヤ 3 冗長切替機能を使用する場合など、IP インタフェースのダウンを期待するネットワーク構成では注意が必要です。

(13) 相互運用

GSRP は、本装置独自仕様の機能です。Extreme Networks 社 LAN スイッチに搭載されている ESRP (Extreme Standby Router Protocol) および Brocade Communications Systems 社 LAN スイッチに搭載されている VSRP (Virtual Switch Redundant Protocol) とは相互運用できません。

(14) 二重化構成でポトリセットを使用する場合について

VLAN グループがマスタ状態からバックアップ状態に切り替わった際、ポトリセット機能によってポートをダウンさせているときに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ることがあります。その場合、運用コマンド activate によってそのポートを active 状態にしてください。

(15) CPU 過負荷時

CPU が過負荷状態となった場合、本装置が送受信する GSRP advertise フレームの廃棄または処理遅延が発生し、タイムアウトのメッセージ出力や、状態遷移が発生するおそれがあります。過負荷状態が頻発する場合は、GSRP advertise フレームの送信間隔および保有時間を大きい値に設定して運用してください。

(16) VLAN グループ設定上の注意

レイヤ 3 冗長切替機能使用時に 9 以上の VLAN グループ ID を設定すると、GSRP の多段構成などで

GSRP グループが異なる場合でも、同じ MAC アドレスが設定されます。

(17) 仮想 MAC アドレスの学習について

レイヤ 3 冗長切替機能使用時、GSRP で冗長化するデフォルトゲートウェイの MAC アドレスは仮想 MAC アドレスを使用します。これに対し、IP 中継および本装置が自発的に送信するパケット/フレームの送信元 MAC アドレスは、仮想 MAC アドレスではなく、装置 MAC アドレス、または VLAN ごとの MAC アドレスになります。

GSRP では、GSRP スイッチをデフォルトゲートウェイとする装置に仮想 MAC アドレスを学習させるため、GSRP 制御フレームを定期的送信しています。GSRP 制御フレームは、送信元 MAC アドレスを仮想 MAC アドレスとした非 IP のユニキャストフレームです。

GSRP スイッチをデフォルトゲートウェイとするすべての装置に GSRP 制御フレームが転送されるネットワーク設計を行ってください。GSRP 制御フレームがファイアウォールなどでフィルタリングされた場合、仮想 MAC アドレスを学習できないため、フレームがフラッディングし、ネットワーク運用に影響が出るおそれがあります。

22 GSRP の設定と運用

この章では、GSRP 機能の設定例について説明します。

22.1 コンフィグレーション

22.2 オペレーション

22.1 コンフィグレーション

22.1.1 コンフィグレーションコマンド一覧

GSRP 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 22-1 コンフィグレーションコマンド一覧

コマンド名	説明
advertise-holdtime	GSRP Advertise フレームの保持時間を設定します。
advertise-interval	GSRP Advertise フレームの送信間隔を設定します。
backup-lock	バックアップ固定機能を設定します。
flush-request-count	GSRP Flush request フレームの送信回数を設定します。
gsrp	GSRP を設定します。
gsrp-vlan	GSRP 管理 VLAN を設定します。
gsrp direct-link	ダイレクトリンクを設定します。
gsrp exception-port	GSRP 制御対象外ポートを設定します。
gsrp limit-control	GSRP VLAN グループ限定制御機能を設定します。
gsrp no-flush-port	GSRP Flush request フレームを送信しないポートを設定します。
gsrp reset-flush-port	ポートリセット機能を使用するポートを設定します。
layer3-redundancy	レイヤ 3 冗長切替機能を設定します。
no-neighbor-to-master	バックアップ (隣接不明) 状態となったときの切り替え方法を設定します。
port-up-delay	リンク不安定時の連続切り替え防止機能を設定します。
reset-flush-time	ポートリセット機能使用時のリンクダウン時間を設定します。
selection-pattern	マスタ、バックアップの選択基準の優先順を設定します。
vlan-group disable	VLAN グループを無効にします。所属している VLAN は通信が停止します。
vlan-group priority	VLAN ごとの優先度を設定します。
vlan-group vlan	VLAN グループに所属する VLAN を設定します。

22.1.2 GSRP の基本的な設定

(1) GSRP グループの設定

[設定のポイント]

GSRP を使用するために、本装置の GSRP グループ ID を設定します。GSRP グループ ID を設定すると本装置で GSRP の動作を開始します。番号は隣接する GSRP スイッチと合わせて設定します。レイヤ 3 冗長切替機能を使用する場合は、1 ~ 4 から選択して設定します。そのほかの GSRP グループ ID ではレイヤ 3 冗長切替機能は使用できません。

GSRP を設定するためには、事前にスパンニングツリーを停止する必要があります。

[コマンドによる設定]

1. (config)# spanning-tree disable

スパンニングツリーを停止します。

2. (config)# gsrp 1

GSRP グループ ID を 1 に設定します。本コマンドによって、本装置は GSRP の動作を開始します。

[注意事項]

GSRP VLAN グループ限定制御機能を設定していない場合、GSRP グループ ID を設定すると、すべての VLAN を GSRP で制御します。VLAN グループを設定していない状況では、すべての VLAN のポートがブロッキング状態になります。

(2) GSRP 管理 VLAN の設定

[設定のポイント]

GSRP 管理 VLAN として使用する VLAN を指定します。設定しない場合、GSRP 管理 VLAN は 1 となります。

GSRP 管理 VLAN は GSRP の制御フレームをやり取りするための VLAN です。この VLAN には、GSRP スイッチ間のダイレクトリンクと、GSRP aware を使用する場合はそのスイッチとの接続ポートを設定してください。また、GSRP aware にも GSRP スイッチと接続しているポートで同じ VLAN を設定してください。

[コマンドによる設定]

1. (config)# gsrp 1

GSRP コンフィグレーションモードに移行します。

2. (config-gsrp)# gsrp-vlan 5

GSRP 管理 VLAN として VLAN 5 を使用します。

(3) ダイレクトリンクの設定

[設定のポイント]

GSRP のダイレクトリンクに使用するポートを設定します。ダイレクトリンクは、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に設定します。

ダイレクトリンク障害検出機能を使用する場合、対向装置の装置障害以外でダイレクトリンク障害となる可能性を少なくするため、ダイレクトリンクを冗長構成にすることをお勧めします。ダイレクトリンクを冗長構成にするためには、リンクアグリゲーションを使用する方法と通常のリンクを複数使用する方法があり、どちらも効果は同じです。レイヤ 3 冗長切替機能でダイレクトリンク上の VLAN を通信に用いる場合、ダイレクトリンクを冗長構成にするときは、リンクアグリゲーションを使用してください。

[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。ダイレクトリンクを冗長化するために複数のポートを指定します。

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。

3. (config)# interface port-channel 10
(config-if)# gsrp 1 direct-link

GSRP グループ ID1 のダイレクトリンクとしてチャンネルグループ 10 を設定します。

(4) VLAN グループの設定

[設定のポイント]

GSRP で運用する VLAN グループと VLAN グループに所属する VLAN を設定します。マスタ状態の VLAN グループに所属した VLAN で通信可能となります。VLAN グループは複数設定でき、VLAN グループごとにマスタ、バックアップを制御します。VLAN グループと所属する VLAN は、隣接する GSRP スイッチと同じ設定をしてください。

VLAN グループへの VLAN の追加および削除は、vlan-group vlan add コマンドおよび vlan-group vlan remove コマンドで行います。vlan-group vlan コマンドを設定済みの状態でもう一度 vlan-group 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。

VLAN グループの通信を停止したい場合、vlan-group disable コマンドで VLAN グループを無効にできます。

[コマンドによる設定]

1. (config)# gsrp 1
GSRP コンフィギュレーションモードに移行します。
2. (config-gsrp)# vlan-group 1 vlan 10,20
VLAN グループ 1 を設定し、VLAN 10, 20 を VLAN グループ 1 に所属させます。
3. (config-gsrp)# vlan-group 1 vlan add 30
VLAN グループ 1 に所属する VLAN に VLAN 30 を追加します。
4. (config-gsrp)# vlan-group 1 vlan remove 20
VLAN グループ 1 に所属する VLAN から VLAN 20 を削除します。
5. (config-gsrp)# vlan-group 1 vlan 100,200
VLAN グループ 1 に所属する VLAN を VLAN 100, 200 に設定します。以前の設定はすべて上書きされて、VLAN 100, 200 が所属する VLAN となります。

[注意事項]

VLAN グループに属していない VLAN の動作は、GSRP VLAN グループ限定制御機能の設定によって異なります。

GSRP VLAN グループ限定制御機能を設定していない場合は、GSRP ではすべての VLAN が GSRP によって制御されます。そのため、VLAN グループに属していない VLAN のポートは、ブロッキング状態になります。

GSRP VLAN グループ限定制御機能を設定している場合は、VLAN グループに所属している VLAN だけを GSRP の制御対象にします。そのため、VLAN グループに属していない VLAN のポートは、フォワーディング状態になります。

22.1.3 マスタ，バックアップの選択に関する設定

(1) マスタ，バックアップの選択方法の設定

[設定のポイント]

GSRP のマスタ，バックアップ状態を切り替えるときの，選択基準（アクティブポート数，優先度，装置 MAC アドレス）の優先順を設定します。優先順は，アクティブポート数 優先度 装置 MAC アドレスの順番と優先度 アクティブポート数 装置 MAC アドレスの順番のどちらかを選択します。通常，アクティブポート数を最優先とすることをお勧めします。ネットワーク構成を変更する際に VLAN のポート数の増減やリンクダウンなどを伴う作業を行う場合，優先度を最優先とする設定によってマスタ，バックアップの状態を固定したまま作業を行えます。

[コマンドによる設定]

1. `(config)# gsrp 1`
GSRP コンフィグレーションモードに移行します。
2. `(config-gsrp)# selection-pattern priority-ports-mac`
選択基準の優先順位を，優先度 アクティブポート数 装置 MAC アドレスの順に設定します。

(2) VLAN グループの優先度の設定

[設定のポイント]

VLAN グループごとに，優先度を設定します。数字が大きいほど優先度が高くなります。優先度を設定することによって，アクティブポート数が同じ状態でマスタにしたい装置を設定します。複数の VLAN グループを作成し，VLAN グループごとに優先度を変えることで，VLAN グループごとのロードバランス構成をとることができます。

[コマンドによる設定]

1. `(config)# gsrp 1`
GSRP コンフィグレーションモードに移行します。
2. `(config-gsrp)# vlan-group 1 priority 80`
VLAN グループ 1 の優先度を 80 に設定します。

(3) バックアップ固定機能の設定

[設定のポイント]

バックアップ固定機能は，片方の GSRP スイッチの全 VLAN グループを強制的にバックアップ状態にします。ケーブル配線の変更や装置の再起動を伴うような大きな構成変更を行いたい場合などに，本機能によって対向の GSRP スイッチをすべての VLAN グループのマスタとした状態で構成変更を行えます。

[コマンドによる設定]

1. `(config)# gsrp 1`
GSRP コンフィグレーションモードに移行します。
2. `(config-gsrp)# backup-lock`
バックアップ固定機能を設定します。すべての VLAN グループがバックアップになり，対向の GSRP

スイッチがマスタになります。

22.1.4 レイヤ 3 冗長切替機能の設定

[設定のポイント]

本装置の GSRP でレイヤ 3 冗長切替機能を設定します。レイヤ 3 冗長切替機能は、GSRP グループ ID が 1 ~ 4 のときだけ使用できます。

レイヤ 3 冗長切替機能を使用するとき、VLAN の IP アドレスは対向の GSRP スイッチと同じ IP アドレスを設定します。IP アドレスの設定方法については、マニュアル「コンフィグレーションガイド Vol.1 19.9 VLAN インタフェース」を参照してください。また、レイヤ 3 冗長切替機能を使用する際には、上流ネットワークの切り替えに関する設定が必要です。詳細は「21.5.3 レイヤ 3 冗長切替機能での上流ネットワーク障害による切り替え」を参照してください。

[コマンドによる設定]

1. `(config)# gsrp 1`
GSRP コンフィグレーションモードに移行します。
2. `(config-gsrp)# layer3-redundancy`
レイヤ 3 冗長切替機能を設定します。

22.1.5 GSRP VLAN グループ限定制御機能の設定

[設定のポイント]

GSRP VLAN グループ限定制御機能を設定します。GSRP VLAN グループ限定制御機能は、VLAN グループに所属している VLAN だけを GSRP の制御対象にします。VLAN グループに所属していない VLAN のポートは、常にフォワーディング状態になります。

GSRP VLAN グループ限定制御機能は、次の用途で使用できます。

- レイヤ 3 冗長切替機能の上流ネットワークへの接続
- GSRP の VLAN グループに所属していない VLAN を GSRP 制御の対象外として運用
- 本装置のリモート管理

[コマンドによる設定]

1. `(config)# gsrp limit-control`
GSRP VLAN グループ限定制御機能を設定します。

22.1.6 GSRP 制御対象外ポートの設定

[設定のポイント]

ポートまたはリンクアグリゲーションに対して GSRP 制御対象外ポートを設定します。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に対して設定し、設定すると GSRP の状態に関係なく常にフォワーディング状態になります。

GSRP 制御対象外ポートは、次の用途で使用できます。

- レイヤ 3 冗長切替機能の上流ネットワークへの接続ポート
- 本装置のリモート管理用ポート

[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ギュレーションモードに移行します。
2. `(config-if)# gsrp exception-port`
ポート 1/1 を GSRP 制御対象外ポートとして設定します。

22.1.7 GSRP のパラメータの設定

(1) リンク不安定時の連続切り替え防止機能の設定

GSRP ではマスタ、バックアップの選択要因として、アクティブポート数を使用します。そのため、ポートのアップ、ダウンが頻発するなどのポートが不安定な状態となった場合にアクティブポート数の増減が多発し、その結果、マスタ状態とバックアップ状態の切り替えが連続して発生するおそれがあります。ポートが不安定な状態の際、本コマンドで遅延時間を指定することで、不要な切り替えを抑制できます。

[設定のポイント]

ポートがアップした場合にアクティブポート数のカウント対象に反映するまでの遅延時間を設定します。パラメータに `infinity` を指定した場合は、遅延時間を無限とし、自動ではアクティブポートにカウントしません。設定しない場合、ポートがアップするとアクティブポート数のカウント対象に即時反映 (0 秒) します。

[コマンドによる設定]

1. `(config)# gsrp 1`
GSRP コンフィギュレーションモードに移行します。
2. `(config-gsrp)# port-up-delay 10`
アクティブポート数へのカウント対象に反映する遅延時間を 10 秒に設定します。
3. `(config-gsrp)# port-up-delay infinity`
アクティブポート数へのカウント対象に反映する遅延時間を無限に変更します。この設定の場合、ポートのアップ後にカウント対象に反映するためには `clear gsrp port-up-delay` コマンドを使用してください。

(2) GSRP Advertise フレームの送信間隔、保持時間の設定

[設定のポイント]

GSRP Advertise フレームの送信間隔および保持時間を設定します。 `advertise-holdtime` は `advertise-interval` より大きな値を設定してください。 `advertise-interval` 以下の値を設定した場合、GSRP Advertise フレームの受信タイムアウトを検出します。

[コマンドによる設定]

1. `(config)# gsrp 1`
GSRP コンフィギュレーションモードに移行します。
2. `(config-gsrp)# advertise-interval 5`

GSRP Advertise フレームの送信間隔を 5 秒に設定します。

3. (config-gsrp)# advertise-holdtime 20

GSRP Advertise フレームの保持時間を 20 秒に設定します。この場合、GSRP Advertise フレームの未到達を 3 回まで許容します。

[注意事項]

CPU が過負荷状態となった場合、本装置が送受信する GSRP advertise フレーム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や、状態遷移が発生するおそれがあります。過負荷状態が頻発する場合は、GSRP advertise フレームの送信間隔、保持時間を大きい値に設定して運用してください。

(3) GSRP Flush request フレームを送信しないポートの設定

[設定のポイント]

ポートまたはリンクアグリゲーションに対して GSRP Flush request フレームを送信しないポートを設定します。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に対して設定します。GSRP Flush request は GSRP 管理 VLAN のうちダイレクトリンクおよびポートリセット機能を設定しているポート以外の全ポートに送信します。本機能は GSRP unaware との接続でポートリセット機能を使用したくない場合に設定します。ただし、このような構成ではマスタ、バックアップの切り替え時に GSRP unaware の MAC アドレステーブルがエージングによってクリアされるまで通信が復旧しないことに注意してください。通常は、GSRP unaware との接続にはポートリセット機能を使用することをお勧めします。

[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)# gsrp 1 no-flush-port

ポート 1/1 から GSRP Flush request フレームを送信しないように設定します。

(4) GSRP Flush request フレームの送信回数の設定

[設定のポイント]

周囲のスイッチに対して MAC アドレステーブルのクリアを行う GSRP Flush request フレームの送信回数を指定します。

デフォルトは 3 回 GSRP Flush request を送信します。回数を増やすと、フレームのロスに対して耐性を高めることができます。

[コマンドによる設定]

1. (config)# gsrp 1

GSRP コンフィグレーションモードに移行します。

2. (config-gsrp)# flush-request-count 5

GSRP Flush request フレームの送信回数を 5 回に設定します。

22.1.8 ポートリセット機能の設定

本機能は GSRP unaware との接続に使用します。マスタ、バックアップの切り替えでバックアップ状態になった装置はポートリセット機能を設定したポートを一時的にリンクダウンします。

(1) 適用するポートの設定

[設定のポイント]

ポートリセット機能を設定します。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に対して設定します。

[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)# gsrp 1 reset-flush-port
ポート 1/1 にポートリセット機能を設定します。

(2) ポートダウン時間の設定

[設定のポイント]

ポートリセット機能使用時のポートダウン時間を設定します。デフォルトは 3 秒です。ポートリセット機能を使用する場合に、対向装置のリンクダウン検出時間が長いときに設定します。本装置のリンクダウン検出タイマ機能 (コンフィグレーションコマンド link debounce) のようにリンクダウン検出時間を設定できる装置と接続している場合、その時間より長く設定してください。

[コマンドによる設定]

1. (config)# gsrp 1
GSRP コンフィグレーションモードに移行します。
2. (config-gsrp)# reset-flush-time 5
ポートダウン時間を 5 秒に設定します。

22.1.9 ダイレクトリンク障害検出の設定

[設定のポイント]

ダイレクトリンクの障害によってバックアップ (隣接不明) 状態からマスタ状態に切り替えるときに、手動 (マスタ遷移コマンド入力) で切り替えるか、自動 (ダイレクトリンク障害検出機能) で切り替えるかを選択します。

ダイレクトリンク障害検出機能を使用し自動で切り替える場合、対向装置の装置障害以外でダイレクトリンク障害と検出する可能性を少なくするため、ダイレクトリンクを冗長構成にすることをお勧めします。ダイレクトリンクを冗長構成にするためには、リンクアグリゲーションを使用する方法と通常のリンクを複数使用する方法があり、どちらも効果は同じです。レイヤ 3 冗長切替機能でダイレクトリンク上の VLAN を通信に用いる場合、ダイレクトリンクを冗長構成にするときは、リンクアグリゲーションを使用してください。

[コマンドによる設定]

1. (config)# gsrp 1

GSRP コンフィグレーションモードに移行します。

2. `(config-gsrp)# no-neighbor-to-master direct-down`

ダイレクトリンク障害検出機能を設定し、ダイレクトリンクの障害時に自動でマスタ状態に遷移します。

22.2 オペレーション

22.2.1 運用コマンド一覧

GSRP の運用コマンド一覧を次の表に示します。

表 22-2 運用コマンド一覧

コマンド名	説明
show gsrp	GSRP 情報を表示します。
show gsrp aware	GSRP の aware 情報を表示します。
clear gsrp	GSRP の統計情報をクリアします。
set gsrp master	バックアップ (隣接不明) 状態をマスタ状態に遷移させます。
clear gsrp port-up-delay	VLAN グループに定義されている VLAN に属しているポートでアップ状態となったポートを、コンフィグレーションコマンド port-up-delay で指定された遅延時間を待たないで、即時アクティブポートへ反映します。
clear gsrp forced-shift	GSRP スイッチ単独起動時のマスタ遷移機能による、自動マスタ遷移待ち状態を解除します。
restart gsrp	GSRP プログラムを再起動します。
dump protocols gsrp	GSRP 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。

22.2.2 GSRP の状態の確認

本装置で GSRP の機能を使用した場合の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 gsrp コマンドで GSRP の設定の状態を確認できます。コンフィグレーションで設定した GSRP 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。また、本装置と同一 GSRP グループを構成する相手装置との間でマスタ、バックアップ選択方法 (Selection Pattern)、レイヤ 3 冗長切替機能の設定、VLAN グループ ID (VLAN Group ID)、および VLAN グループに所属する VLAN が同一であることを確認してください。レイヤ 3 冗長切替機能を設定している場合は、VLAN グループに所属する VLAN で IP アドレスの設定が相手装置と一致していることを確認してください。IP アドレスに関する確認は、マニュアル「コンフィグレーションガイド Vol.1 19.11.2 VLAN の状態の確認」、および「コンフィグレーションガイド Vol.3 2.2.2 IPv4 インタフェースの up/down 確認」または「コンフィグレーションガイド Vol.3 18.2.2 IPv6 インタフェースの up/down 確認」を参照してください。なお、バックアップ状態の VLAN グループに所属する VLAN はインタフェース状態がダウン状態であることに注意してください。

show gsrp detail コマンド、show gsrp vlan-group コマンドの表示例を次に示します。

図 22-1 show gsrp detail コマンドの実行結果

```

> show gsrp detail
Date 2008/11/07 22:24:36 UTC

GSRP ID: 1
Local MAC Address      : 0012.e205.0000
Neighbor MAC Address   : 0012.e205.0011
Total VLAN Group Counts : 2
GSRP VLAN ID          : 105
Direct Port            : 1/10-11
Limit Control          : Off
GSRP Exception Port    : 1/1-5
No Neighbor To Master  : manual
Backup Lock            : disable
Port Up Delay          : 0
Last Flush Receive Time : -
Forced Shift Time      : -
Layer 3 Redundancy     : On

                    Local           Neighbor
Advertise Hold Time  : 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
8                   Master           Backup
>

```

図 22-2 show gsrp vlan-group コマンドの実行結果

```

> show gsrp 1 vlan-group 1
Date 2006/03/07 22:25:13 UTC

GSRP ID: 1
Local MAC Address      : 0012.e205.0000
Neighbor MAC Address   : 0012.e205.0011
Total VLAN Group Counts : 1
Layer 3 Redundancy     : On

VLAN Group ID : 1
VLAN ID       : 110,200-210
Member Port   : 1/6-8
Last Transition : 2006/03/07 22:20:11 (Master to Backup)
Transition by reason : Priority was lower than neighbor's
Master to Backup Counts : 4
Backup to Master Counts : 4
Virtual MAC Address : 0000.8758.1307

                    Local           Neighbor
State                : Backup           Master
Acknowledged State   : Backup           -
Advertise Hold Timer : 3               -
Priority              : 100            101
Active Ports         : 3               3
Up Ports             : 3               -
>

```

(2) 運用中の確認

本装置および本装置と同一 GSRP グループを構成する相手装置で、VLAN グループの状態がどれかの装置で Master になっていること、および同一 VLAN グループで複数のマスタが存在しないことを確認してください。本装置での VLAN グループの状態確認には show gsrp コマンドを使用してください。

図 22-3 show gsrp コマンドの実行例

```

> show gsrp
Date 2006/03/07 22:28:38 UTC

GSRP ID: 10
Local MAC Address      : 0012.e205.0000
Neighbor MAC Address   : 0012.e205.0011
Total VLAN Group Counts : 2
Layer 3 Redundancy     : On

VLAN Group ID      Local State      Neighbor State
1                  Backup          Master
8                  Master          Backup
>

```

22.2.3 コマンドによる状態遷移

set gsrp master コマンドで、バックアップ（隣接不明）状態をマスタ状態に遷移させることができます。

このコマンドは、バックアップ（隣接不明）状態のときだけ有効なコマンドです。対向装置の該当する VLAN グループ状態がバックアップになっていることを確認したあとに実行してください。

図 22-4 set gsrp master コマンドの実行結果

```

> set gsrp master 1 vlan-group 1
Transit to Master. Are you sure? (y/n):y
>

```

22.2.4 遅延状態のポートのアクティブポート即時反映

clear gsrp port-up-delay コマンドで、リンク不安定時の連続切り替え防止機能（コンフィグレーションコマンド port-up-delay）を使用している場合に、ポートアップ後の遅延時間を待たないですぐにアクティブポートへ反映できます。

図 22-5 clear gsrp port-up-delay コマンドの実行結果

```

> clear gsrp port-up-delay port 1/1
>

```


23 VRRP

VRRP (Virtual Router Redundancy Protocol) はルータに障害が発生した場合でも、同一イーサネット上の別ルータを経由して端末の通信経路を確保することを目的としたホットスタンバイ機能です。この章では VRRP について説明します。

23.1 解説

23.2 コンフィグレーション

23.3 オペレーション

23.1 解説

VRRP (Virtual Router Redundancy Protocol) はルータに障害が発生した場合でも、同一イーサネット上の別ルータを経由して端末の通信経路を確保することを目的としたホットスタンバイ機能です。

VRRP を使用すると、同一イーサネット上の複数のルータから構成される仮想ルータを設定できます。端末がデフォルトゲートウェイとしてこの仮想ルータを設定しておくことによって、ルータに障害が発生したときの別ルータへの切り替えを意識することなく、通信を継続できます。

仮想ルータは 1 から 255 までの仮想ルータ ID を持ち、同一イーサネット上の同一の仮想ルータ ID を持つ仮想ルータ同士が、パケットのルーティングを行う 1 台のマスタの仮想ルータと、パケットのルーティングを行わないホットスタンバイである 1 台以上のバックアップの仮想ルータを構成します。

23.1.1 仮想ルータの MAC アドレスと IP アドレス

仮想ルータは自身の物理的な MAC アドレスとは別に、仮想ルータ用の MAC アドレスとして仮想 MAC アドレスを持ちます。仮想 MAC アドレスは、仮想ルータ ID から自動的に生成されます。

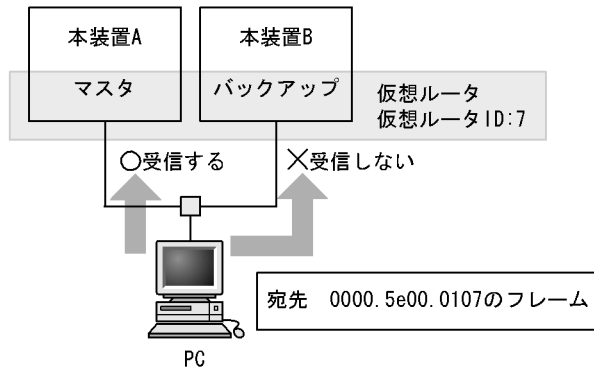
サポートしている VRRP の規格と仮想 MAC アドレスの対応を次の表に示します。

表 23-1 VRRP の規格と仮想 MAC アドレスの対応

規格		仮想 MAC アドレス
IPv4	RFC3768	0000.5e00.01{ 仮想ルータ ID}
	draft-ietf-vrrp-unified-spec-02	0000.5e00.01{ 仮想ルータ ID}
IPv6	draft-ietf-vrrp-ipv6-spec-02	0000.5e00.01{ 仮想ルータ ID}
	draft-ietf-vrrp-ipv6-spec-07	0000.5e00.02{ 仮想ルータ ID}
	draft-ietf-vrrp-unified-spec-02	0000.5e00.02{ 仮想ルータ ID}

マスタの仮想ルータは仮想 MAC アドレス宛てのイーサネットフレームを受信してパケットをフォワーディングする能力を持ちますが、バックアップの仮想ルータは仮想 MAC アドレス宛てのフレームを受信しません。VRRP は仮想ルータの状態に応じて仮想 MAC アドレス宛てイーサネットフレームを受信するかどうかを制御します。マスタの仮想ルータは仮想 MAC 宛てフレームを受信すると、ルーティングテーブルに従って IP パケットのフォワーディング処理を行います。そのため、端末は仮想 MAC アドレスを宛先としてフレームを送信することで、マスタとバックアップが切り替わったあとも通信を継続できます。仮想 MAC アドレス宛てフレームの受信を次の図に示します。

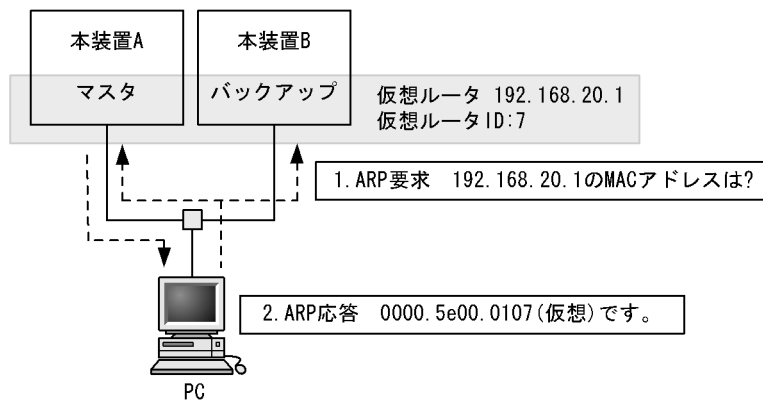
図 23-1 仮想 MAC 宛てフレームの受信



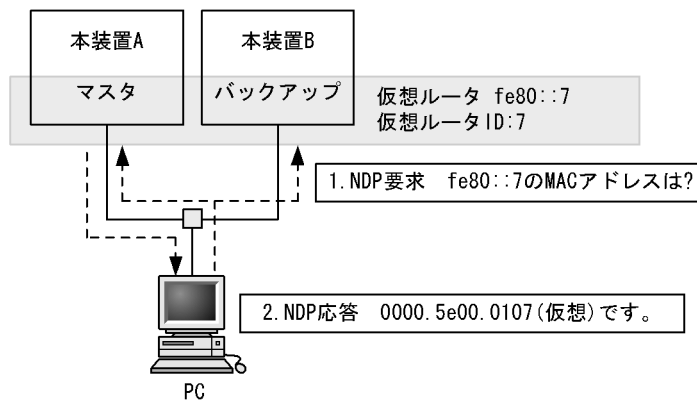
仮想ルータは仮想ルータ用の IP アドレスである仮想 IP アドレスを持ちます。マスターの仮想ルータは、仮想 IP アドレスに対する ARP 要求パケットまたは NDP 要求パケットを受信すると、常に仮想 MAC アドレスを使用して ARP 応答または NDP 応答します。仮想 MAC アドレスによる ARP 応答および NDP 応答を次の図に示します。

図 23-2 仮想 MAC アドレスによる ARP 応答および NDP 応答

●ARP 応答



●NDP 応答

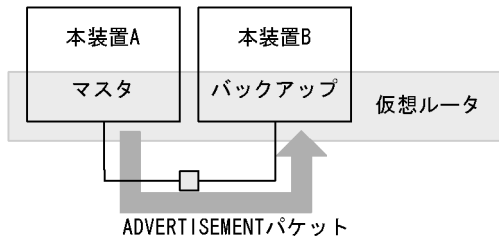


仮想ルータをデフォルトルータとして使用する PC などのホストは、自 ARP キャッシュテーブル内に仮想 IP アドレス宛てのフレームは仮想 MAC アドレス宛てに送信するように学習します。このように学習されたホストは常に仮想ルータへフレームを送信するときに仮想 MAC アドレスを宛先に指定するようになるため、VRRP のマスター/バックアップの切り替えが発生した場合でも、通信を継続できます。

23.1.2 VRRP における障害検出の仕組み

マスタの仮想ルータは定期的な周期（デフォルト 1 秒）で ADVERTISEMENT パケットと呼ばれる稼働状態確認用のパケットを、仮想ルータを設定した IP インタフェースから送信します。バックアップの仮想ルータはマスタの仮想ルータが送信する ADVERTISEMENT パケットを受信することによって、マスタの仮想ルータに障害がないことを確認します。ADVERTISEMENT パケットの送信を次の図に示します。

図 23-3 ADVERTISEMENT パケットの送信



マスタの仮想ルータに障害が発生した場合、ADVERTISEMENT パケットを送信できません。例えば、装置全体がダウンしてしまった場合や、仮想ルータが設定されている IP インタフェースからパケットを送信できなくなるような障害が発生した場合、ケーブルの抜けなどの場合です。

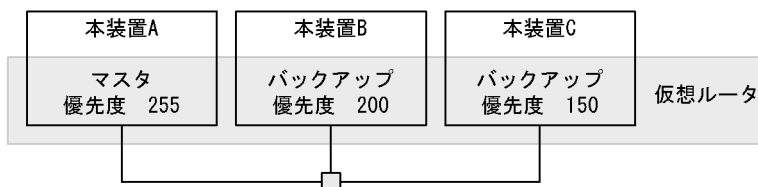
バックアップの仮想ルータは一定の間 ADVERTISEMENT パケットをマスタの仮想ルータから受信しなかった場合に、マスタの仮想ルータに障害が発生したと判断し、バックアップからマスタへと状態を変化させます。

23.1.3 マスタの選出方法

(1) 優先度

複数の仮想ルータの中からマスタの仮想ルータを選出するために、VRRP では優先度を使用します。この優先度は仮想ルータに設定できます。設定できる値は 1 から 255 までの数値で、デフォルトは 100 です。この数値が大きいほど優先度は高くなります。インタフェースに付与されている IP アドレスと仮想ルータの IP アドレスが等しい（IP アドレスの所有者）場合、最も優先度が高い 255 に自動的に設定されます。マスタの仮想ルータの選出を次の図に示します。

図 23-4 マスタの選出



この図の場合、優先度が最も高い仮想ルータ A がマスタになります。仮想ルータ A がダウンした場合は、次に優先度の高い仮想ルータ B がマスタへと変化します。仮想ルータ A と仮想ルータ B の両方がダウンした場合にだけ仮想ルータ C がマスタになります。

マスタになる装置を明確にするため、同じイーサネット上の同じ仮想ルータ ID の仮想ルータには、異なる優先度を設定してください。優先度の同じ仮想ルータが存在する場合は、どちらがマスタになるか不定のため、動作が期待どおりにならないおそれがあります。

(2) 自動切り戻しおよび自動切り戻しの抑止

VRRP では、優先度の高いバックアップの仮想ルータが、自ルータよりも優先度の低いマスタの仮想ルータを検出すると、自動的にマスタへ状態を変化させます。逆に、マスタの仮想ルータが、自ルータよりも優先度の高い仮想ルータの存在を検出したときは自動的にバックアップへと状態を変化させます。

「図 23-4 マスタの選出」の構成を例にしてみると、仮想ルータ A と仮想ルータ B がダウンし仮想ルータ C がマスタになっている状態から、仮想ルータ B が復旧すると、仮想ルータ C よりも優先度の高い仮想ルータ B がマスタに変化し、仮想ルータ C がマスタからバックアップへ状態を変化させることとなります。

この自動切り戻しを抑止する設定ができます。切り戻し抑止には、次の 2 とおりの方法があります。

PREEMPT モードによる抑止

自動切り戻しさせたくない場合には、コンフィグレーションコマンド `no vrrp preempt` で PREEMPT モードを OFF に設定してください。PREEMPT モードを OFF に設定すれば、バックアップの仮想ルータが自ルータよりも優先度の低い仮想ルータがマスタになっていることを検出しても、状態をマスタへ変化させることはありません。

抑止タイマによる抑止

自動切り戻しの開始を任意の時間遅延させたい場合には、コンフィグレーションコマンド `vrrp preempt delay` で抑止タイマを設定してください。本タイマ値は、自動切り戻し要因を検出してから自動切り戻し処理の開始時間を遅らせるものであり、状態が完全に切り変わるまでには、設定した時間プラス数秒の時間を要します。

PREEMPT モードを設定した場合も抑止タイマを設定した場合も、対象となる仮想ルータが IP アドレスの所有者（優先度 255）の場合は、切り戻しの抑止は有効になりません。

マスタの仮想ルータが故障などによって運用不可状態になったことを検出し、かつ残った仮想ルータの中で自ルータの優先度が最も高いことを検出した場合には、切り戻し抑止中であってもマスタに遷移します。

手動による切り戻し

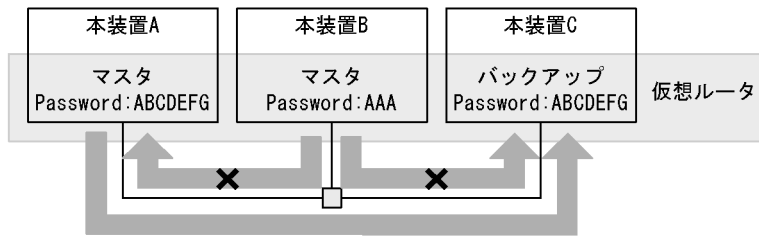
自動切り戻し抑止中状態でも、運用コマンド `swap vrrp` によって仮想ルータの切り戻し処理を起動できます。

自動切り戻し抑止によってバックアップ状態に留まっている装置に対して本コマンドを指定すると、コマンド実行時にマスタの仮想ルータよりコマンドを指定したバックアップの仮想ルータの優先度が高い場合は、コマンドを指定した仮想ルータがマスタ状態に遷移します。

23.1.4 ADVERTISEMENT パケットの認証

ADVERTISEMENT パケットはリンクローカルスコープのマルチキャストアドレス（IPv4 では 224.0.0.18，IPv6 では ff02::12）を使用します。また、仮想ルータは IP ヘッダの TTL または HopLimit が 255 以外のパケットを受信しないため、ルータ越えを伴う遠隔からの攻撃を防ぐことができます。さらに、本装置ではテキストパスワードによる VRRP の ADVERTISEMENT パケットの認証をサポートします。8 文字以内のパスワードを仮想ルータに設定すると、パスワードが異なる ADVERTISEMENT パケットを廃棄します。パスワードの不一致を次の図に示します。

図 23-5 パスワードの不一致



この図の例では仮想ルータ B のパスワードが仮想ルータ A および仮想ルータ C と異なっているため、仮想ルータ B から送信された ADVERTISEMENT パケットを仮想ルータ A や仮想ルータ C が受け取っても廃棄します。この場合、仮想ルータ C は仮想ルータ A からの ADVERTISEMENT パケットだけを受信して処理します。そのため、ADVERTISEMENT パケット認証に失敗するような、不正に設置された仮想ルータの動作を防止できます。

23.1.5 アクセプトモード

IP アドレス所有者でない仮想ルータは、マスターであっても仮想 IP アドレス宛てのパケットに対して応答しません。しかし、ping によってネットワーク機器の状態を確認することは一般的に行われます。

本装置は、アクセプトモードをサポートします。アクセプトモードは、マスターの仮想ルータが仮想 IP アドレス宛てのパケットに対して応答できるようにする機能です。仮想ルータの状態を外部から監視するために、コンフィグレーションコマンド `vrp accept` でアクセプトモードを設定することで、マスターの仮想ルータがアドレス所有者でなくても、ICMP echo request パケットを受信し、ICMP echo reply パケットを返信できます。

23.1.6 トラッキング機能

本装置では、ネットワークの障害を監視して、仮想ルータの優先度を動的に操作する機能（トラッキング機能）として、障害監視インタフェースと VRRP ポーリングをサポートしています。

仮想ルータを設定したインタフェースに障害が発生した場合、マスターの切り替えが行われます。しかし、パケットルーティング先の IP インタフェース、ポートチャネルインタフェース、イーサネットインタフェースなど、仮想ルータが設定されていないほかのインタフェースで障害が発生した場合は、通信が不可能な状態であってもマスターの切り替えが行われません。

本装置では独自の付加機能として、本装置内の VLAN インタフェース、ポートチャネルインタフェース、およびイーサネットインタフェースを監視して、そのインタフェースがダウンした場合に、仮想ルータの優先度を下げて運用する機能を使用できます。このトラッキング機能を障害監視インタフェースと呼びます。ただし、障害監視を行う VLAN インタフェースには、IP アドレスが設定されている必要があります。

障害監視インタフェースでは、インタフェースのダウンで検出できるレベルの障害しか監視できないため、ルータをまたいだ先の障害を検出できません。本装置では独自の付加機能として、指定した VLAN インタフェースを監視するとともに、指定した宛先へ ping で疎通確認を行い、応答がない場合に仮想ルータの優先度を下げて運用する機能を使用できます。このトラッキング機能を VRRP ポーリングと呼びます。

障害監視インタフェースは本装置と隣接する機器間の障害監視に、VRRP ポーリングはルータをまたいだ先にある機器との間の障害監視に利用できます。

また、仮想ルータの優先度を操作する方式は 2 とおりあります。

一つは、トラッキング機能によって障害を検出したときに仮想ルータの優先度をコンフィグレーションコ

マンド `vrrp track priority` であらかじめ設定しておいた切替優先度に変更して運用する優先度切替方式です。

もう一つは、トラッキング機能によって障害を検出したときに、コンフィグレーションコマンド `vrrp track decrement` であらかじめ障害監視インタフェースに設定した優先度減算値を仮想ルータの優先度から引いて運用する優先度減算方式です。

優先度切替方式の場合、障害監視インタフェースまたは VRRP ポーリングのどちらかを一つだけ設定できます。優先度減算方式の場合、障害監視インタフェースと VRRP ポーリングを複数設定できます。

トラッキング機能によって仮想ルータの優先度が 0 となった場合、仮想ルータを設定した IP インタフェースはダウン状態になります。ただし、仮想ルータ名を設定している場合は、ダウン状態になりません。

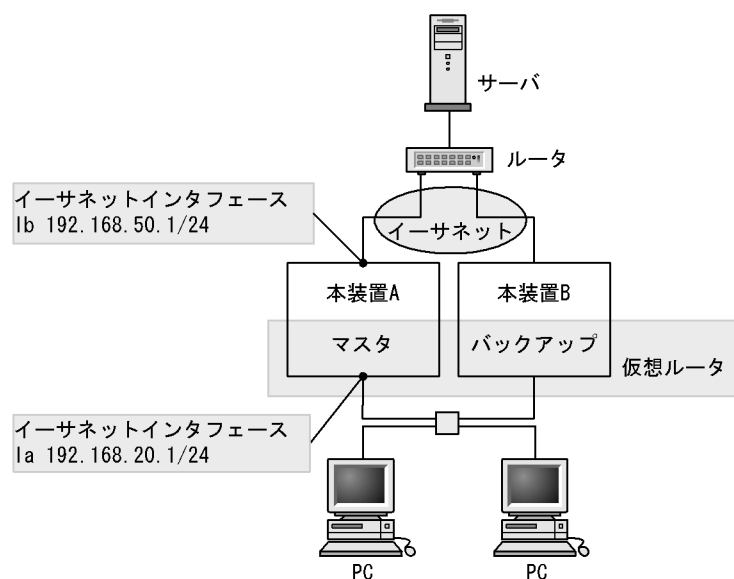
表 23-2 優先度操作方式と監視方法組み合わせ

優先度操作方式	障害監視インタフェース	VRRP ポーリング
優先度切替方式	一つだけ設定可	一つだけ設定可
優先度減算方式	複数設定可	複数設定可

(1) 障害監視インタフェース

仮想ルータの障害監視インタフェースを次の図に示します。

図 23-6 障害監視インタフェース



この図を例にして、障害監視インタフェースに VLAN インタフェースを指定した場合を説明します。本装置 A には Ia という VLAN インタフェースと Ib という VLAN インタフェースの二つが設定されています。仮想ルータはインタフェース Ia に設定されています。通常の VRRP の動作では VLAN の障害によってインタフェース Ib がダウンしても、仮想ルータの動作には影響を与えません。しかし、本装置では障害監視インタフェースと障害監視インタフェースダウン時の切替優先度、または優先度減算値を指定することによって、仮想ルータの動作状態を変更させることができます。

本装置 A の仮想ルータの障害監視インタフェースを Ib、そして障害監視インタフェースダウン時の優先度を 0 に設定した場合、インタフェース Ib のダウン時には自動的にマスターが本装置 A の仮想ルータから本

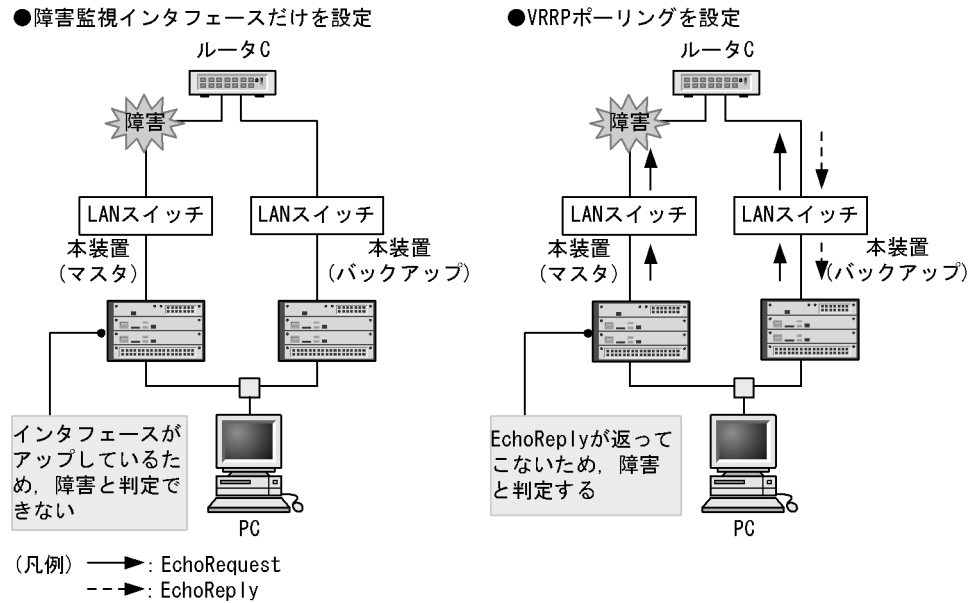
装置 B の仮想ルータへ切り替わります。

同様に、障害監視インタフェースにポートチャンネルインタフェース、イーサネットインタフェースを設定して、仮想ルータの動作状態を変更させることができます。

(2) VRRP ポーリング

VRRP ポーリングを設定した場合と設定していない場合の比較を次の図に示します。

図 23-7 VRRP ポーリングを設定した場合と設定していない場合の比較



VRRP ポーリングの宛先の機器で障害が発生したり、ネットワーク上で障害が発生したりして応答が返らなくなると、あらかじめ指定された切替優先度または優先度減算値によって、仮想ルータの優先度を下げて運用できます。

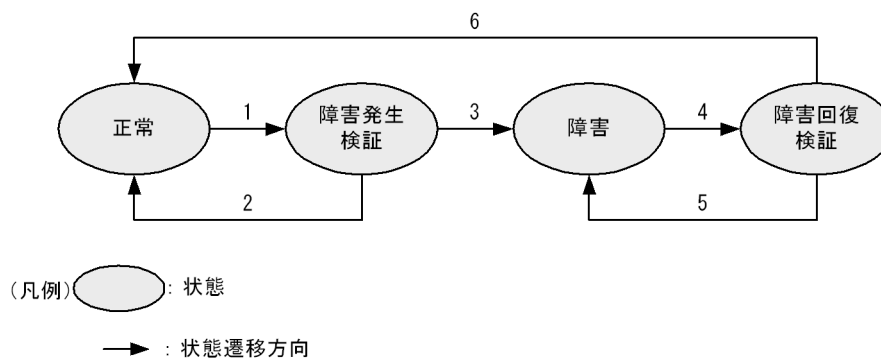
VRRP ポーリングでの状態と、優先度およびポーリング試行間隔の組み合わせを次の表に示します。

表 23-3 VRRP ポーリングでの状態と優先度およびポーリング試行間隔の組み合わせ

状態	優先度	ポーリング試行間隔
正常	コンフィグレーションコマンド <code>vrrp priority</code> で設定した優先度	<code>track check-status-interval</code>
障害発生検証		<code>track failure-detection-interval</code>
障害	コンフィグレーションコマンド <code>vrrp track priority</code> で設定した切替優先度、またはコンフィグレーションコマンド <code>vrrp track decrement</code> で設定した優先度減算値によって、優先度を下げる	<code>track check-status-interval</code>
障害回復検証		<code>track recovery-detection-interval</code>

VRRP ポーリングでの状態遷移と状態遷移条件を次に示します。

図 23-8 VRRP ポーリングでの状態遷移



1. 応答が返らないままタイムアウト
2. ポーリング試行回数 ¹ に対して、ポーリング成功回数 ² を満たす応答を受信
3. ポーリング試行回数 ¹ に対して、ポーリング成功回数 ² を満たす応答を受信できないと判明した時点
4. 応答を受信
5. ポーリング試行回数 ¹ に対して、ポーリング成功回数 ³ を満たす応答を受信できないと判明した時点
6. ポーリング試行回数 ¹ に対して、ポーリング成功回数 ³ を満たす応答を受信

注 1 コンフィグレーションコマンド track check-trial-times で設定できます。

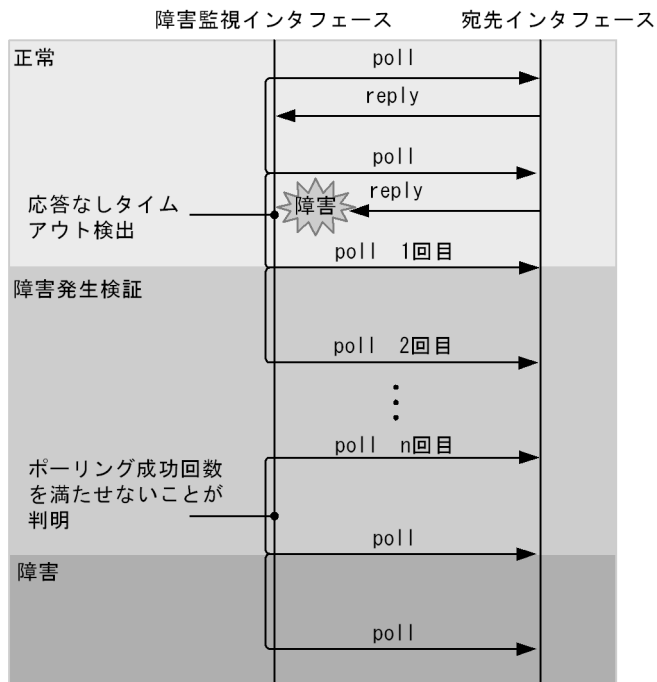
注 2 コンフィグレーションコマンド track failure-detection-times で設定できます。

注 3 コンフィグレーションコマンド track recovery-detection-interval で設定できます。

障害発生検証動作

障害発生検証動作シーケンスを次の図に示します。

図 23-9 障害発生検証動作シーケンス



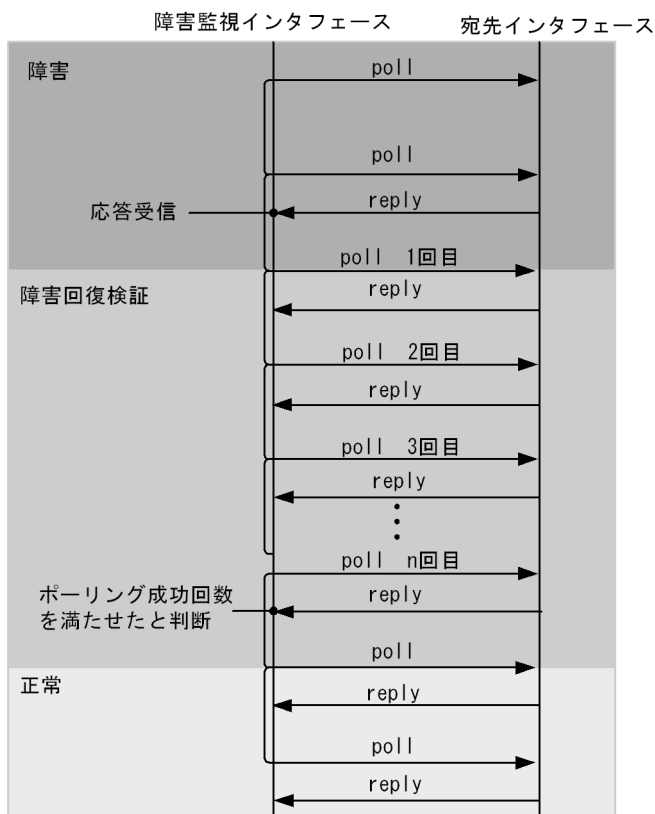
障害発生検証動作では、障害検証用の試行間隔でポーリングを行います。ポーリング試行回数に対して、ポーリング成功回数を満たせないと判明した時点（この図では、 n 回応答がタイムアウトした時点）で障害中と判定して、優先度を下げて運用します。

初期導入時のコンフィギュレーションで運用して障害状態が継続している場合は、ポーリング試行回数 4 回に対して、2 回応答がタイムアウトした時点（障害発生検証動作開始後 4 秒）でポーリング成功回数を満たせないと判断して、優先度を下げて運用します。

障害回復検証動作

障害回復検証動作シーケンスを次の図に示します。

図 23-10 障害回復検証動作シーケンス



障害回復検証動作では、回復検証用の試行間隔でポーリングを行います。ポーリング試行回数に対して、ポーリング成功回数を満たせた時点（この図では n 回応答を受信した時点）で正常と判定して、自装置の優先度を戻して運用します。

初期導入時のコンフィギュレーションで運用している場合、ポーリング試行回数 4 回に対して、3 回応答が返ってきた時点（障害回復検証動作開始後 6 秒）でポーリング成功回数を満たせたと判断して、優先度を戻して運用します。

インタフェースがダウンした場合、VRRP ポーリングは障害中と判断し、インタフェースがアップするまで待機します。インタフェースがアップしたとき、再度ポーリングを始め、障害回復検証によって正常時と判断した場合、切り戻しを行います。

VRRP ポーリングの宛先 IP アドレスが、ルータをまたいだ先のネットワーク上にある場合は、各ルータのルーティングテーブルに依存します。このため、「図 23-11 送受信インタフェースが一致しない場合」のように VRRP ポーリングの応答を受信するインタフェースが VRRP ポーリングを送信したインタフェースと一致しない場合があります。この場合、受信インタフェースチェック（コンフィギュレーションコマンド `track check-reply-interface`）を指定することで、送信インタフェースと受信インタフェースをチェックできます。送信インタフェースと受信インタフェースが不一致の場合に該当するパケットを廃棄します。なお、「図 23-12 自装置配下ではないネットワーク上のインタフェース不一致」のような自装置配下でないネットワーク上のインタフェースが不一致の場合は、保証しません。

図 23-11 送受信インタフェースが一致しない場合

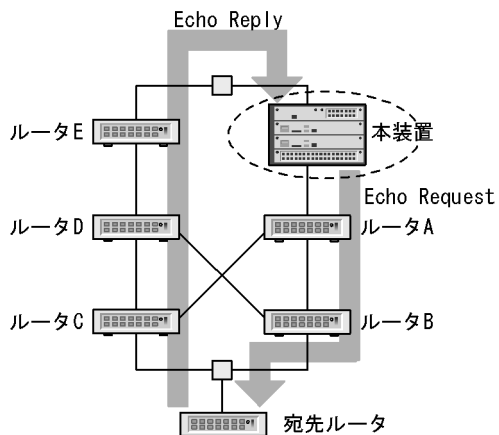
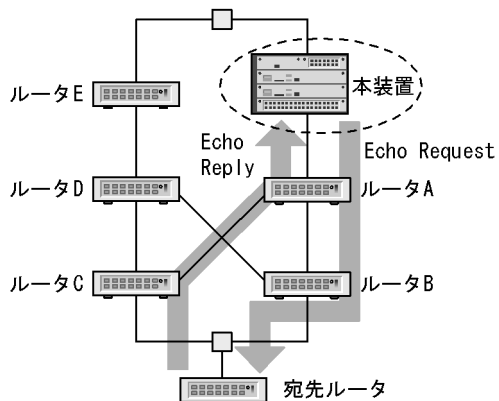


図 23-12 自装置配下ではないネットワーク上のインタフェース不一致



23.1.7 VRRP のサポート規格

本装置では複数の VRRP の規格をサポートしているため、既存システムで採用されている規格に合わせて、柔軟に仮想ルータを設定できます。VRRP の規格を仮想ルータに適用するには、VRRP 動作モードを設定してください。

サポートしている VRRP の規格と VRRP 動作モード設定のコマンドの対応を次の表に示します。

表 23-4 VRRP の規格と VRRP 動作モード設定のコマンドの対応

規格		VRRP 動作モード設定のコマンド
IPv4	RFC3768	IPv4 仮想ルータのデフォルト動作
	draft-ietf-vrrp-unified-spec-02	vrrp ietf-unified-spec-02-mode
IPv6	draft-ietf-vrrp-ipv6-spec-02	IPv6 仮想ルータのデフォルト動作
	draft-ietf-vrrp-ipv6-spec-07	vrrp ietf-ipv6-spec-07-mode
	draft-ietf-vrrp-unified-spec-02	vrrp ietf-unified-spec-02-mode

ADVERTISEMENT パケットのフォーマットやフィールドの意味は規格ごとに異なります。そのため、仮想ルータを構成する装置間で異なった設定をすると、ADVERTISEMENT パケットを不正パケットと判断して破棄してしまい、お互いがマスタ状態になることがあります。したがって、コンフィギュレーションの

設定時は、仮想ルータを構成する装置間で VRRP 動作モードを一致させてください。

(1) IPv4 仮想ルータのデフォルト動作概要

VRRP パケット Ver.2 (RFC3768 で規定されているパケットフォーマット) を使用して ADVERTISEMENT を行い、ADVERTISEMENT パケットの認証機能が利用できます。

本装置に設定された ADVERTISEMENT パケットの送信間隔を基に、障害検出時間を決定します。

(2) IPv6 仮想ルータのデフォルト動作概要

VRRP パケット Ver.3 (draft-ietf-vrrp-ipv6-spec-02 で規定されているパケットフォーマット) を使用して ADVERTISEMENT を行い、ADVERTISEMENT パケットの認証機能が利用できます。

本装置に設定された ADVERTISEMENT パケットの送信間隔を基に、障害検出時間を決定します。

(3) vrrp ietf-ipv6-spec-07-mode の動作概要

IPv6 仮想ルータでサポートしている VRRP 動作モードです。

VRRP パケット Ver.3 (draft-ietf-vrrp-ipv6-spec-07 で規定されているパケットフォーマット) を使用して ADVERTISEMENT を行います。

本装置に設定された ADVERTISEMENT パケットの送信間隔を基に、障害検出時間を決定します。

ADVERTISEMENT パケットの認証機能は利用できません。

(4) vrrp ietf-unified-spec-02-mode の動作概要

IPv4/IPv6 仮想ルータでサポートしている VRRP 動作モードです。

VRRP パケット Ver.3 (draft-ietf-vrrp-unified-spec-02 で規定されているパケットフォーマット) を使用して ADVERTISEMENT を行います。

マスタ装置からの ADVERTISEMENT パケットの受信によって得られるマスタ装置の ADVERTISEMENT パケットの送信間隔を基に、障害検出時間を決定します。

ADVERTISEMENT パケットの認証機能は利用できません。

(5) 障害検出時間について

本装置では、仮想ルータが draft-ietf-vrrp-ipv6-spec-07 または draft-ietf-vrrp-unified-spec-02 に従って動作している場合、ADVERTISEMENT パケットの送信間隔をミリ秒単位で指定すると、すばやく障害を検出して、仮想ルータを切り替えられます。

すばやく VRRP を切り替えるためには、障害検出時間を短くする必要があります。障害検出時間は、ADVERTISEMENT パケットの送信間隔を基に、次の式で算出されます。

$$\text{障害検出時間} = \text{ADVERTISEMENT パケット送信間隔} \times 3 + \text{Skew_Time}$$

なお、Skew_Time の算出方法は VRRP の規格ごとに異なります。VRRP の規格と Skew_Time の算出方法を次の表に示します。

表 23-5 VRRP の規格と Skew_Time 算出方法

VRRP の規格	ADVERTISEMENT パケット送信間隔の指定単位	Skew_Time
RFC3768	秒	$(256 - \text{Priority}^1) / 256$ (単位：秒)
draft-ietf-vrrp-ipv6-spec-02	秒	
draft-ietf-vrrp-ipv6-spec-07	1/100 秒	$((256 - \text{priority}^1) * \text{Advertisement_Interval}^2) / 256$ (単位：Advertisement_Interval ² と同じ)
draft-ietf-vrrp-unified-spec-02	1/100 秒	$((256 - \text{priority}^1) * \text{Master_Adver_Interval}^3) / 256$ (単位：Master_Adver_Interval ³ と同じ)

注 1 仮想ルータの優先度

注 2 自装置に設定された ADVERTISEMENT パケット送信間隔

注 3 マスタ装置の ADVERTISEMENT パケット送信間隔

本装置では、仮想ルータが draft-ietf-vrrp-ipv6-spec-07 または draft-ietf-vrrp-unified-spec-02 で動作している場合、ADVERTISEMENT パケットの送信間隔に 250 ミリ秒を指定すると、障害検出時間を 1 秒以内に設定できます。

23.1.8 グループ切替機能

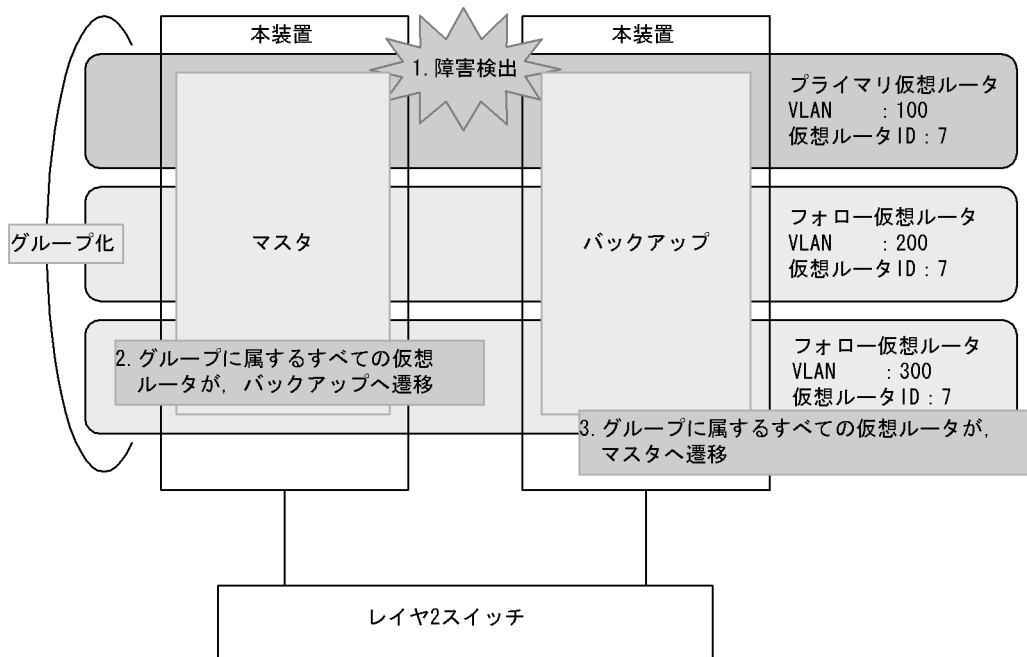
(1) 概要

本装置では独自の付加機能として、仮想ルータをグループ化できます。そのグループ単位で、マスタ / バックアップの切り替えができます。グループは、プライマリ仮想ルータとフォロー仮想ルータから構成されます。

グループ化することで、最大 4095 の仮想ルータを使用できます。

グループ切替機能の構成と切り替えの概要を次の図に示します。

図 23-13 グループ切替機能の構成と切り替えの概要



- (凡例)
- : プライマリ仮想ルータの構成
 - : フォロー仮想ルータの構成
 - : グループの状態

1. マスタ/バックアップ装置のそれぞれの監視機能によって、障害を検出
2. マスタ装置では、障害を検出したグループの全仮想ルータがバックアップへ遷移
3. バックアップ装置では、障害を検出したグループの全仮想ルータがマスタへ遷移

(2) プライマリ仮想ルータ

ADVERTISEMENT パケットの送受信やトラッキング機能が動作し、マスタ/バックアップを切り替える仮想ルータを、プライマリ仮想ルータと呼びます。プライマリ仮想ルータの状態が、グループに属するすべての仮想ルータの状態を決定します。

(3) フォロー仮想ルータ

プライマリ仮想ルータの状態に従い自身の状態を決定する仮想ルータを、フォロー仮想ルータと呼びます。フォロー仮想ルータは、ADVERTISEMENT パケットの送受信やトラッキング機能による障害検出・状態遷移は行わず、プライマリ仮想ルータの状態に従います。プライマリ仮想ルータが動作していない場合は、イニシャル状態となります。また、自分自身を含むフォロー仮想ルータの状態に従うことはできません。フォロー仮想ルータはプライマリ仮想ルータの状態に従うため、アドレス所有者にはなれません。

フォロー仮想ルータのプライマリ仮想ルータと異なる機能について次の表に示します。

表 23-6 フォロー仮想ルータの機能

プライマリ仮想ルータと異なる機能	動作
マスタ/バックアップの切り替え	ADVERTISEMENT パケット送受信、トラッキング機能による障害検出・状態遷移は行わず、プライマリ仮想ルータの状態に従います。

プライマリ仮想ルータと異なる機能	動作
コンフィグレーション設定	マスタの選出方法のために利用する次のコンフィグレーションコマンドは、無効です。 vrrp authentication vrrp preempt vrrp preempt delay vrrp timers non-preempt-swap vrrp priority vrrp track
運用ログ	状態遷移に伴う運用ログは出力しません。 グループを構成するプライマリ仮想ルータが設定されていない場合、フォロワー仮想ルータが無効である旨のログを出力し注意を促します。また、プライマリ仮想ルータが設定された場合に回復メッセージを出力します。
MIB 情報の取得	未サポートです。プライマリ仮想ルータだけ取得できます。
trap 発行	未サポートです。プライマリ仮想ルータだけ発行します。

(4) MAC Learning フレーム

マスタ状態の仮想ルータは、下流の LAN スイッチに仮想 MAC アドレスを学習させる必要があります。

- プライマリ仮想ルータ
プライマリ仮想ルータは ADVERTISEMENT パケットを送信します。下流の LAN スイッチは、それを受信することで仮想 MAC アドレスを学習します。
- フォロワー仮想ルータ
フォロワー仮想ルータは ADVERTISEMENT パケットを送信しません。その代わりに、定期的に送信元 MAC アドレスを仮想 MAC アドレスとした MAC Learning フレームを送信します。下流の LAN スイッチは、この MAC Learning フレームを受信することで、仮想 MAC アドレスを学習します。

(5) 注意事項

1. グループ化する仮想ルータは、同じ仮想ルータ ID に設定することを推奨します。異なる仮想ルータ ID でグループ化した場合、同じ仮想ルータ ID でグループ化した場合に比べて、通信の再開に時間が掛かることがあります。
2. 仮想ルータを構成する装置間では、仮想ルータのコンフィグレーションは同一にしてください。例えば、ある仮想ルータが、一方の装置でプライマリ仮想ルータ、他方の装置でフォロワー仮想ルータとした場合、正しく動作しません。
3. プライマリ仮想ルータは、グループに属するフォロワー仮想ルータのすべての障害を検出できるように設定してください。プライマリ仮想ルータのトラッキング機能で障害を検出できないフォロワー仮想ルータは、障害発生時に状態遷移ができないで通信できなくなります。
例えば、プライマリ仮想ルータとフォロワー仮想ルータで ADVERTISEMENT パケットの通信経路が異なる場合や監視を必要とする VLAN が異なる場合、プライマリ仮想ルータはそれらすべてを監視する必要があります。
4. グループ切替機能を利用している場合、トラッキング機能で障害を検出し仮想ルータの優先度が 0 になっても IP インタフェースはダウンしません。
5. MAC Learning フレームは、1 フォロワー仮想ルータ当たり 2 分周期で送信されます。下流の LAN スイッチでは、MAC アドレステーブルのエイジング時間を 2 分以下に設定した場合、エイジングと MAC アドレス学習を繰り返します。エイジング時間は 4 分以上に設定することを推奨します。

23.1.9 Flush Request 機能

(1) 概要

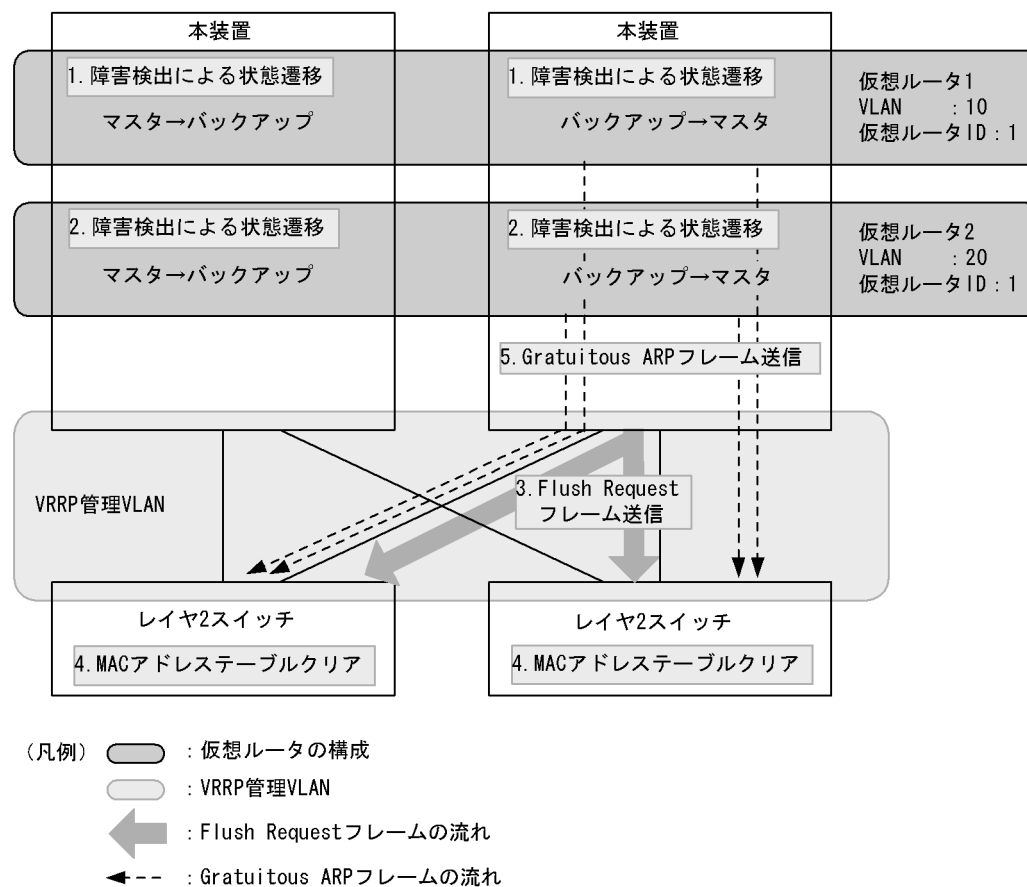
VRRP は、仮想ルータがマスタへ切り替わった際、マスタ装置から Gratuitous ARP フレームを送信し、下流の LAN スイッチの MAC アドレスエントリの更新を促します。

本機能では、仮想ルータがマスタへ切り替わったとき、Gratuitous ARP フレームを送信する前に、Flush Request フレームを送信します。Flush Request フレームは、下流の LAN スイッチに対して MAC アドレステーブルエントリのクリアを促すフレームで、VRRP 管理 VLAN と呼ばれる専用の VLAN に対してフラッシングされます。VRRP 管理 VLAN にはすべての下流の LAN スイッチを所属させることを推奨します。

本機能を設定しない場合、複数の仮想ルータが同時に状態遷移した際、すべての Gratuitous ARP フレームの送信が完了するまで MAC アドレスエントリは切り替わりません。そのため、仮想ルータ数の増加に伴い、MAC アドレスエントリの切り替えに時間が掛かります。しかし、本機能を設定した場合、複数の仮想ルータが一度にマスタへ切り替わったとき、すべての Gratuitous ARP フレームを受信する前に Flush Request フレームによって MAC アドレステーブルが更新されるため、すばやく通信を再開できるようになります。

Flush Request 機能の動作を次の図に示します。

図 23-14 Flush Request 機能の動作



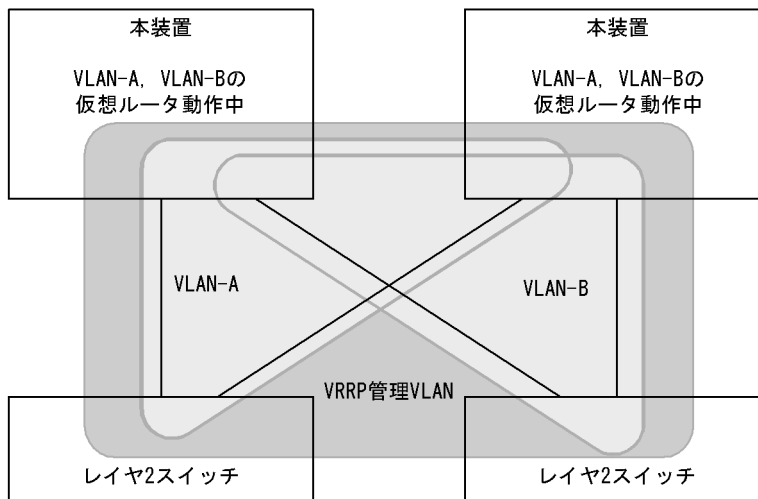
1. 仮想ルータ 1 が障害検出によって、マスタ/バックアップの切り替わり発生

2. 仮想ルータ 2 が障害検出によって、マスタ/バックアップの切り替わり発生
3. 切り替わったマスタ側の装置から、VRRP 管理 VLAN へ Flush Request フレームをフラッディング
4. 下流の LAN スイッチは、MAC アドレステーブルをクリア
5. マスタ装置から、Gratuitous ARP フレームを送信

(2) 注意事項

1. グループ切替機能を利用する場合、本機能を設定することを推奨します。グループに属する仮想ルータが多い場合、本機能によってすべての仮想ルータが同時に通信を再開できます。
2. ほかの仮想ルータの状態遷移に関係なく下流の LAN スイッチの MAC アドレステーブルを維持したい場合、その装置は VRRP 管理 VLAN に属さないようにしてください。
3. 物理的な構成が異なる複数の VLAN に対して Flush Request 機能を適用する場合、それらの VLAN すべてを含むように VRRP 管理 VLAN を設定すると、VRRP 管理 VLAN でレイヤ 2 ループが発生する構成になるおそれがあります。
VRRP 管理 VLAN でレイヤ 2 ループが発生する構成例を次に示します。

図 23-15 VRRP 管理 VLAN でレイヤ 2 ループが発生する構成例



上記の構成では、VLAN-A、VLAN-B それぞれにはレイヤ 2 ループはありませんが、VLAN-A、VLAN-B の両方に Flush Request 機能を適用する VRRP 管理 VLAN (すべての装置が属する VLAN) を設定すると、VRRP 管理 VLAN でレイヤ 2 ループが発生します。

このような場合、次のどちらかの方法でレイヤ 2 ループを防止してください。

- スパニングツリーや Ring Protocol などの L2 プロトコルを動作させる。
- VRRP 管理 VLAN に廃棄フィルタを設定して、パケットを中継しない構成にする。この場合、VRRP 管理 VLAN は Flush Request 機能以外の用途と併用できません。

4. 下流の LAN スイッチは、本機能に対応した装置である必要があります。

23.1.10 VRRP 使用時の注意事項

(1) VRRP と GSRP との混在利用について

同一装置内で VRRP と GSRP は同時に使用できません。

(2) ADVERTISEMENT パケット送信間隔について

次に示す状態の場合、本装置が送受信する VRRP ADVERTISEMENT パケットの破棄または処理遅延が発生し、状態遷移が発生するおそれがあります。状態遷移が頻発する場合は、VRRP ADVERTISEMENT パケットの送信間隔を大きい値に設定して運用してください。

- 本装置の CPU が過負荷状態の場合
- 本装置に設定した仮想ルータ数が多い場合
- ネットワークが過負荷状態の場合
- 仮想ルータを 3 台以上で構成している場合

(3) VRRP ポーリングによるマルチパス経路の監視について

VRRP ポーリング機能はマルチパス経路に対する監視ができません。

(4) IPv6 VRRP と RA の連携について

IPv6 VRRP を設定したインタフェースで RA (Router Advertisement) が有効になっている場合、RA は VRRP と連携して次のように動作します。

- RA は IPv6 VRRP のマスタールータとなっている場合だけ情報を配布します。
- RA パケットの MAC ヘッダの送信元 MAC アドレスは、仮想ルータに設定した仮想 MAC アドレスになります。
- RA パケットの IPv6 ヘッダの送信元 IPv6 アドレスは、仮想ルータに設定した仮想 IPv6 アドレスになります。

これによって、端末は IPv6 自動構成機能で、仮想ルータをデフォルトルータとすることができます。

ただし、次のような場合、端末の動作によっては RA を使用したネットワーク運用に支障があるので注意してください。

- 一つのインタフェースに複数の仮想ルータを設定した場合、最小の VRID を使用しているマスタールータとだけ連携します。したがって、負荷分散のために VRRP を使用する場合、各端末でデフォルトルータを手動で設定してください。
- 仮想 IPv6 アドレスにリンクローカルアドレスではなくグローバルアドレスを設定した場合、RA の送信元 IPv6 アドレスにはリンクローカルアドレスが必要なため、RA の送信元 IPv6 アドレスには仮想 IPv6 アドレスではなくインタフェースに固有のリンクローカルアドレスを使用します。このため、VRRP と RA の連携動作はできません。VRRP と RA を連携させる運用をする場合は、仮想 IPv6 アドレスにグローバルアドレスを設定しないでください。

(5) VRID について

仮想ルータが動作している VLAN が設定されたポート上で、ほかの VLAN も動作していて、かつその VLAN 上でも仮想ルータが動作している場合、VRID が重複しないようにしてください。

(6) VRRP 状態遷移時間について

仮想ルータの状態遷移には、本装置内で同時に遷移する仮想ルータ数に応じて、次に示す状態遷移時間が必要です。

仮想ルータのアクセプトモードが無効の場合の目安値

仮想ルータ数が 512 未満では 1 秒、1024 以上では 2 秒以上

仮想ルータのアクセプトモードが有効の場合の目安値

仮想ルータ数が 128 未満では 1 秒 , 512 以上では 2 秒以上

23.2 コンフィグレーション

VRRP の設定を行う VLAN には、IP アドレスが設定されている必要があります。VLAN に IP アドレスが設定されていない場合、VRRP のコンフィグレーションコマンドを入力しても仮想ルータは動作しません。

仮想ルータを実際に運用する場合には、同様の仮想ルータの設定を本装置だけでなく、仮想ルータを構成するほかの装置にも行う必要があります。また、仮想ルータの設定のほかにルーティングの設定も必要です。

23.2.1 コンフィグレーションコマンド一覧

VRRP 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 23-7 VRRP 設定用コンフィグレーションコマンド一覧

コマンド名	説明
vrrp accept	アクセプトモードを設定します。
vrrp authentication	ADVERTISEMENT バケット認証のパスワードを設定します。
vrrp follow	プライマリ仮想ルータを指定し、仮想ルータをフォロー仮想ルータに設定します。
vrrp ietf-ipv6-spec-07-mode	IPv6 の仮想ルータへ draft-ietf-vrrp-ipv6-spec-07 に準拠した動作となるよう設定します。
vrrp ietf-unified-spec-02-mode	draft-ietf-vrrp-unified-spec-02 に準拠した動作となるよう設定します。
vrrp ip vrrp ipv6	仮想ルータへ IP アドレスを設定します。
vrrp name	仮想ルータに名称を設定します。
vrrp preempt	自動切り戻しを設定します。
vrrp preempt delay	自動切り戻し抑止時間を設定します。
vrrp priority	仮想ルータの優先度を設定します。
vrrp timers advertise	仮想ルータの ADVERTISEMENT バケット送信間隔を設定します。
vrrp timers non-preempt-swap	自動切り戻し抑止中に切り戻し処理を行う場合の切り戻し抑止時間を設定します。
vrrp-vlan	VRRP 管理 VLAN として使用する VLAN を指定します。

表 23-8 障害監視インタフェース設定用コマンド一覧

コマンド名	説明
track check-reply-interface	VRRP ポーリングで送受信インタフェースの一致を確認するか設定します。
track check-status-interval	VRRP ポーリング間隔を設定します。
track check-trial-times	VRRP ポーリングの判定回数を設定します。
track failure-detection-interval	障害発生検証中の VRRP ポーリング間隔を設定します。
track failure-detection-times	障害発生検証中の VRRP ポーリング判定回数を設定します。
track interface	障害監視を行うインタフェースと障害監視方法を設定します。
track ip route	track で VRRP ポーリングを行う宛先を指定します。

コマンド名	説明
track recovery-detection-interval	障害回復検証中の VRRP ポーリング間隔を設定します。
track recovery-detection-times	障害回復検証中の VRRP ポーリング判定回数を設定します。
vrrp track	track を仮想ルータに割り当てます。

23.2.2 VRRP のコンフィギュレーションの流れ

(1) あらかじめ、IP インタフェースを設定します。

VLAN に対して、仮想ルータに設定しようとしている IP アドレスと同一アドレスファミリの IP アドレスを設定します。

VLAN に初めて IPv6 アドレスを設定する場合は、続けて `ipv6 enable` コマンドを実行して IPv6 アドレスを有効にする必要があります。

(2) 仮想ルータへ IP アドレスを設定します。

IP インタフェースに設定した IP アドレスと同一の IP アドレスを仮想ルータへ設定すると、仮想ルータはアドレス所有者となり、優先度が 255 固定となります。

仮想ルータへ IPv6 アドレスを設定する場合、規格上はリンクローカルユニキャストアドレスだけ指定できますが、本装置ではグローバルアドレス（サイトローカルアドレスも含む）も指定できます。

(3) 仮想ルータの優先度を設定します。

IP アドレス所有者でない同一仮想ルータ ID の仮想ルータの優先度を、それぞれ異なる値に設定します。

(4) ADVERTISEMENT パケット送信間隔を設定します。

バックアップの仮想ルータが ADVERTISEMENT パケットを頻繁に取りこぼす場合は、ADVERTISEMENT パケットの送信間隔をマスタとバックアップの仮想ルータに設定します。

(5) 障害監視インタフェースと VRRP ポーリングを設定します。

必要に応じて、仮想ルータが設定されているインタフェース以外の障害で仮想ルータの切り替えが行われるように、仮想ルータへ障害監視インタフェースや VRRP ポーリングを設定します。

23.2.3 仮想ルータへの IPv4 アドレス設定

[設定のポイント]

仮想ルータへ仮想 IPv4 アドレスを設定します。仮想ルータへ仮想 IP アドレスを設定することで、仮想ルータは動作を開始します。仮想ルータへ設定できる IP アドレスは一つだけです。

仮想ルータに設定する IP アドレスと仮想ルータを設定する VLAN の IP アドレスが同一の場合、仮想ルータは IP アドレス所有者となり、優先度が 255（固定）となります。

仮想 IP アドレスを設定する仮想ルータ ID は、同一 IP サブネットワーク内でユニークとなるように設定してください。

[コマンドによる設定]

1. (config)# interface vlan 10
(config-if)# ip address 192.168.10.10 255.255.255.0

例えば、VLAN 10 に仮想ルータを設定する場合、まず vlan 10 の VLAN コンフィグレーションモードに入ります。VLAN へ IP アドレスを設定していない場合は、ここで IP アドレスを設定します。

2. (config-if)# vrrp 1 ip 192.168.10.1

仮想ルータ ID1 の仮想ルータへ仮想 IP アドレスとして 192.168.10.1 を設定します。

[注意事項]

- 仮想ルータへ IP アドレスを設定すると、仮想ルータは動作を始めます。ほかの仮想ルータの優先度設定によっては、仮想ルータがマスタとして追加される場合もあります。
- 装置に仮想ルータを 64 個以上設定する場合は、「表 23-9 ADVERTISEMENT パケット送信間隔の設定目安値」を参照して ADVERTISEMENT パケットの送信間隔を調整してください。

23.2.4 仮想ルータへの IPv6 アドレス設定

[設定のポイント]

仮想ルータへ仮想 IPv6 アドレスを設定します。仮想ルータへ仮想 IPv6 アドレスを設定することで、仮想ルータは動作を開始します。仮想ルータへ設定できる IPv6 アドレスは一つだけです。

仮想ルータに設定する IP アドレスと仮想ルータを設定する VLAN の IP アドレスが同一の場合、仮想ルータは IP アドレス所有者となり、優先度が 255 (固定) となります。

仮想 IP アドレスを設定する仮想ルータ ID は、同一 IP サブネットワーク内でユニークとなるように設定してください。

[コマンドによる設定]

1. (config)# interface vlan 50

(config-if)# ipv6 enable

(config-if)# ipv6 address 2001:100::1/64

例えば、VLAN 50 に仮想ルータを設定する場合、まず vlan 50 の VLAN コンフィグレーションモードに入ります。VLAN へ IPv6 アドレスを設定していない場合は、ここで IPv6 アドレスを設定します。

2. (config-if)# vrrp 3 ipv6 fe80::10

仮想ルータ ID3 の仮想ルータへ仮想 IPv6 アドレス fe80::10 を設定します。

[注意事項]

- 「23.2.3 仮想ルータへの IPv4 アドレス設定」の注意事項と同じです。

23.2.5 優先度の設定

仮想ルータの優先度を 1 から 254 の間で設定します。優先度のデフォルト値は、IP アドレス所有者でない場合は 100 です。仮想ルータが IP アドレス所有者の場合は優先度が 255 (固定) となって変更できません。

仮想ルータを構成する装置のうちで最も優先度の大きい装置がマスタになります。また、マスタの仮想ルータがダウンした場合、バックアップの仮想ルータのうちで最も優先度の高い仮想ルータがマスタになります。

[設定のポイント]

マスタになる装置を明確にするために、同じ仮想ルータ ID の仮想ルータには異なる優先度を設定し

てください。

[コマンドによる設定]

1. (config-if)# vrrp 1 priority 150
仮想ルータ ID1 の仮想ルータの優先度を 150 に設定します。

23.2.6 ADVERTISEMENT パケット送信間隔の設定

(1) ADVERTISEMENT パケット送信間隔設定

ネットワークの負荷が高く、ADVERTISEMENT パケットの損失が多いため、仮想ルータのマスタとバックアップがたびたび切り替わる場合は、ADVERTISEMENT パケットの送信間隔を長くすることで、現象を軽減できることがあります。ただし、バックアップの仮想ルータは、ADVERTISEMENT パケットを 3 回続けて受信できないときにマスタに変わるため、ADVERTISEMENT パケットの送信間隔を長くすると、マスタの仮想ルータで障害が発生した場合に、バックアップの仮想ルータがマスタに変わるまでの時間も長くなります。

また、装置に多くの仮想ルータを設定した場合、上記と同様にマスタとバックアップが切り替わることがあります。その場合は、次の表を基に ADVERTISEMENT パケット送信間隔を調整してください。

表 23-9 ADVERTISEMENT パケット送信間隔の設定目安値

装置当たりの仮想ルータ数	ADVERTISEMENT パケット送信間隔
1 ~ 64	1 秒以上
65 ~ 128	2 秒以上
129 ~ 192	3 秒以上
193 ~ 255	4 秒以上

注 グループ切替機能使用時は、プライマリ仮想ルータ数

[設定のポイント]

ADVERTISEMENT パケット送信間隔は、マスタおよびバックアップの仮想ルータへ同一の値を設定してください。

[コマンドによる設定]

1. (config-if)# vrrp 1 timers advertise 3
仮想ルータ ID1 の仮想ルータの ADVERTISEMENT パケット送信間隔を 3 (秒) に設定します。

(2) 仮想ルータの高速切替設定

本装置では、仮想ルータが draft-ietf-vrrp-ipv6-spec-07 または draft-ietf-vrrp-unified-spec-02 に従って動作している場合、ADVERTISEMENT パケットの送信間隔をミリ秒単位で指定すると、すばやく障害を検出して、仮想ルータを切り替えられます。

装置に多くの仮想ルータを設定した場合、マスタとバックアップが切り替わることがあります。その場合は、次の表を基に ADVERTISEMENT パケット送信間隔を調整してください。

表 23-10 高速切替機能使用時の ADVERTISEMENT パケット送信間隔の設定目安値

装置当たりの仮想ルータ数	ADVERTISEMENT パケット送信間隔
1 ~ 64	0.25 秒以上
65 ~ 128	0.50 秒以上
129 ~ 192	0.75 秒以上
193 ~ 255	1.00 秒以上

注 グループ切替機能使用時は、プライマリ仮想ルータ数

[設定のポイント]

VRRP の仮想ルータを高速切替するためには、対応した VRRP 動作モードを設定して、ADVERTISEMENT パケット送信間隔をミリ秒単位で指定する必要があります。ADVERTISEMENT パケット送信間隔は、マスタおよびバックアップの仮想ルータへ同一の値を設定してください。

[コマンドによる設定]

1. `(config-if)# vrrp 1 ietf-unified-spec-02-mode`
仮想ルータが、draft-ietf-vrrp-unified-spec-02 に従った動作になるように設定します。
2. `(config-if)# vrrp 1 timers advertise msec 250`
仮想ルータの ADVERTISEMENT パケット送信間隔を 250 ミリ秒に設定します。

23.2.7 自動切り戻し抑止の設定

自動切り戻しはデフォルトで動作し、マスタの仮想ルータに障害が発生してバックアップに切り替わったあと、障害が復旧すると、はじめにマスタであった優先度の高いバックアップの仮想ルータが自動的にマスタに切り替わります。自動切り戻しを抑止すると、優先度の高いバックアップの仮想ルータが自動的にマスタに切り替わらなくなります。

[設定のポイント]

自動切り戻し抑止の設定を行う場合は、IP アドレス所有者でないマスタの仮想ルータに対して行ってください。

[コマンドによる設定]

1. `(config-if)# no vrrp 1 preempt`
仮想ルータ ID1 の仮想ルータの自動切り戻しを抑止します。

23.2.8 自動切り戻し抑止時間の設定

マスタの仮想ルータに障害が発生してバックアップに切り替わったあと、障害が復旧した場合、優先度の高いバックアップの仮想ルータが自動的にマスタに切り替え処理を開始するまでの時間を設定します。自動切り戻し抑止時間のデフォルト値は 0 (秒) で、自動切り戻しを抑止しません。

[設定のポイント]

自動切り戻し抑止時間の設定を行う場合は、IP アドレス所有者でないマスタの仮想ルータに対して行ってください。

[コマンドによる設定]

1. (config-if)# vrrp 1 preempt delay 60

仮想ルータ ID1 の仮想ルータの自動切り戻し抑止時間を 60 秒に設定します。

23.2.9 障害監視インタフェースと VRRP ポーリングの設定

本装置では、障害監視インタフェースと VRRP ポーリングの設定を、番号付けした track で管理します。track の設定は、コンフィグレーションコマンド track で track 番号を指定します。track を仮想ルータに割り当てることで、仮想ルータは指定された track 番号の track に保存された障害監視インタフェースの設定に従い、障害監視インタフェースを利用します。仮想ルータに track を割り当てるには、コンフィグレーションコマンド vrrp track を利用します。

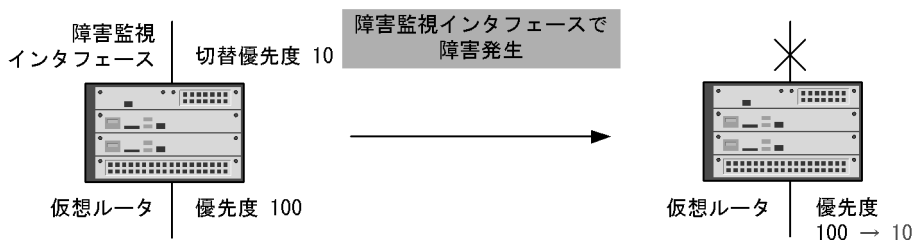
一つの仮想ルータには、優先度切替方式の track と優先度減算方式の track のどちらか一方だけを設定できます。

一つの仮想ルータに対して track を複数割り当てる場合は、優先度操作方式として優先度減算方式だけ設定できます。

優先度切替方式の場合、障害発生時に仮想ルータの優先度を指定した切替優先度に変更します。切替優先度の指定を省略または仮想ルータの優先度より大きい値を指定した場合は、デフォルト値の 0 が使用されます。優先度切替方式を指定した場合は、一つの仮想ルータに track を一つだけ割り当てることができます。

優先度切替方式で「図 23-16 優先度切替方式」のように、仮想ルータの優先度を 100、障害監視インタフェースの切替優先度として 10 を指定した場合、障害監視インタフェースで障害が発生すると、仮想ルータの優先度は切替優先度の 10 に設定されます。

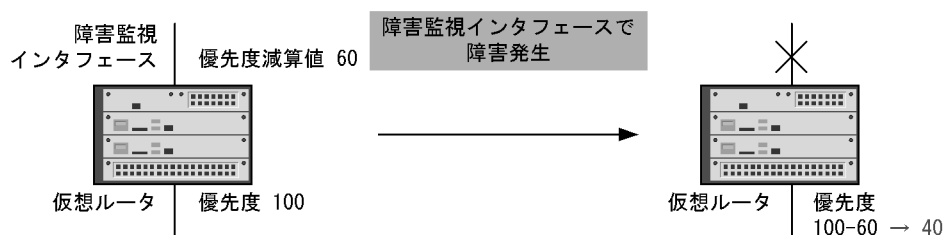
図 23-16 優先度切替方式



優先度減算方式の場合、障害発生時に仮想ルータの優先度を指定した優先度減算値だけ減算した値に変更します。優先度の指定を省略した場合は、デフォルト値の 255 が使用されます。decrement を指定した場合は、一つの仮想ルータに最大 16 の track を割り当てることができます。

優先度減算方式で「図 23-17 優先度減算方式」のように、仮想ルータの優先度を 100、障害監視インタフェースの優先度減算値として 60 を指定した場合、障害監視インタフェースで障害が発生すると、仮想ルータの優先度は元々の優先度 100 から優先度減算値 60 を引いた 40 に設定されます。

図 23-17 優先度減算方式



(1) 障害監視インタフェースを行う track の設定

[設定のポイント]

コンフィギュレーションコマンド `track interface` で `line-protocol` を指定すると、指定した VLAN インタフェース、ポートチャンネルインタフェース、およびイーサネットインタフェースの状態を監視します。

track に監視する VLAN インタフェース、ポートチャンネルインタフェース、およびイーサネットインタフェースを設定します。

仮想ルータにコンフィギュレーションコマンド `vrrp track` で障害監視を行う track を設定します。

障害監視を行う VLAN インタフェースには、IP アドレスが設定されている必要があります。

[コマンドによる設定]

1. `(config)# track 20 interface vlan 30 line-protocol`

`(config)# track 30 interface gigabitethernet 6/8 line-protocol`

`(config)# track 40 interface port-channel 10 line-protocol`

- track 番号 20 の track に、障害監視インタフェースとして `vlan 30` の状態を監視するよう、設定します。
- track 番号 30 の track に、障害監視インタフェースとしてギガビット・イーサネットインタフェース `6/8` の状態を監視するよう、設定します。
- track 番号 40 の track に、障害監視インタフェースとしてチャンネルグループ `10` の状態を監視するよう、設定します。

2. `(config-if)# vrrp 1 track 20 decrement 60`

`(config-if)# vrrp 1 track 30 decrement 10`

`(config-if)# vrrp 1 track 40 decrement 40`

あらかじめ仮想ルータが設定してある VLAN の VLAN コンフィギュレーションモードにしておきます。

この場合、仮想ルータ ID1 の仮想ルータに、track 番号 20, 30, 40 の track を割り当てます。

- track 番号 20 の track に設定された障害監視インタフェースで障害が発生した場合、仮想ルータ 1 の優先度が 60 下がります。
- track 番号 30 の track に設定された障害監視インタフェースで障害が発生した場合、仮想ルータ 1 の優先度が 10 下がります。
- track 番号 40 の track に設定された障害監視インタフェースで障害が発生した場合、仮想ルータ 1 の優先度が 40 下がります。

(2) VRRP ポーリングを行う track の設定

[設定のポイント]

コンフィグレーションコマンド `track interface` で `ip routing` を指定すると、指定した VLAN を監視するとともに、コンフィグレーションコマンド `track ip route` で指定した宛先への ping による疎通を監視します。

VRRP ボーリングとして利用する VLAN インタフェースを `track` に設定します。

仮想ルータにコンフィグレーションコマンド `vrrp track` で VRRP ボーリングを行う `track` を設定します。

VRRP ボーリングによる障害監視を行う場合は、VRRP ボーリングを行う VLAN インタフェースに IP アドレスを設定し、`track ip route` コマンドで指定した宛先への経路情報が設定されている必要があります。

同一の `track` を複数の仮想ルータに設定した場合、それぞれの仮想ルータから VRRP ボーリングパケットを送信します。

[コマンドによる設定]

1.

```
(config)# track 50 interface vlan 34 ip routing
```

```
(config)# track 51 interface vlan 35 ip routing
```

```
(config)# track 52 interface vlan 36 ip routing
```

 - track 番号 50 の track に、VRRP ボーリングの送信インタフェースとして `vlan34` の状態を監視するように設定します。
 - track 番号 51 の track に、VRRP ボーリングの送信インタフェースとして `vlan35` の状態を監視するように設定します。
 - track 番号 52 の track に、VRRP ボーリングの送信インタフェースとして `vlan36` の状態を監視するように設定します。

2.

```
(config)# track 50 ip route 192.168.20.1 reachability
```

```
(config)# track 51 ip route 192.168.21.1 reachability
```

```
(config)# track 52 ip route 192.168.22.1 reachability
```

 - track 番号 50 の track に、VRRP ボーリングの宛先として `192.168.20.1` を設定します。
 - track 番号 51 の track に、VRRP ボーリングの宛先として `192.168.21.1` を設定します。
 - track 番号 52 の track に、VRRP ボーリングの宛先として `192.168.22.1` を設定します。

3.

```
(config-if)# vrrp 3 track 50 priority 10
```

```
(config-if)# vrrp 4 track 51 decrement 20
```

```
(config-if)# vrrp 4 track 52 decrement 50
```

 - あらかじめ仮想ルータが設定してある VLAN の VLAN コンフィグレーションモードにしておきます。
 - 仮想ルータ ID3 の仮想ルータに、track 番号 50 の track を割り当て、優先度操作方式に優先度切替方式、切替優先度に 10 を指定します。track 番号 50 の track に設定された VRRP ボーリングで障害が発生した場合、仮想ルータ 3 の優先度を 10 に切り替えます。
 - 仮想ルータ ID4 の仮想ルータに、track 番号 51 と 52 の track を割り当てます。優先度操作方式に優先度減算方式を設定します。track 番号 51 の優先度減算値に 20 を設定します。track 番号 52 の優先度減算値に 50 を設定します。track 番号 51 の track に設定された VRRP ボーリングで障害が発生した場合、仮想ルータ 4 の優先度が 20 下がります。track 番号 52 の track に設定された VRRP ボーリングで障害が発生した場合、仮想ルータ 4 の優先度が 50 下がります。track 番号 51 と 52 の両方の障害監視インタフェースで障害が発生した場合は仮想ルータ 4 の優先度が 70 下がります。

23.2.10 VRRP 動作モードの設定

本装置では複数の VRRP の規格をサポートしているため、既存システムに採用されている規格に合わせて柔軟に導入できます。

コンフィグレーションの設定時は、仮想ルータを構成する装置間で VRRP 動作モードを一致させてください。なお、仮想ルータに設定された IP プロトコルバージョンと VRRP 動作モードの IP プロトコルバージョンが異なる場合、設定は無効となります。

(1) draft-ietf-vrrp-ipv6-spec-07 に従った VRRP 動作モードの設定

[設定のポイント]

仮想ルータを構成する装置は、両装置とも draft-ietf-vrrp-ipv6-spec-07 で動作するようにコンフィグレーションを設定してください。

[コマンドによる設定]

1. (config-if)# vrrp 1 ietf-ipv6-spec-07-mode

IPv6 仮想ルータが、draft-ietf-vrrp-ipv6-spec-07 に従った動作になるように設定します。

(2) draft-ietf-vrrp-unified-spec-02 に従った VRRP 動作モードの設定

[設定のポイント]

仮想ルータを構成する装置は、両装置とも draft-ietf-vrrp-unified-spec-02 で動作するようにコンフィグレーションを設定してください。

[コマンドによる設定]

1. (config-if)# vrrp 1 ietf-unified-spec-02-mode

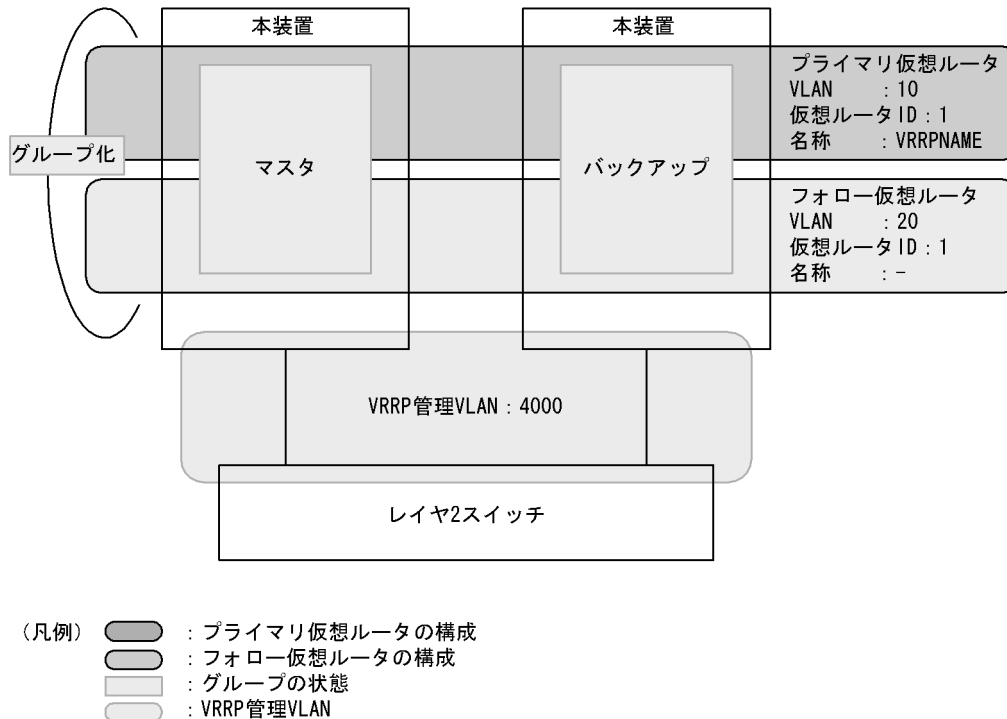
仮想ルータが、draft-ietf-vrrp-unified-spec-02 に従った動作になるように設定します。

23.2.11 仮想ルータのグループ化

複数の仮想ルータをグループ化することで、最大 4095 の仮想ルータを使用できます。

ここでは、次の図に示すグループ構成を設定する例を示します。

図 23-18 仮想ルータのグループ構成



(1) プライマリ仮想ルータの設定

[設定のポイント]

プライマリ仮想ルータの状態は、グループに属するすべての仮想ルータの状態を決定します。設定後、プライマリ仮想ルータが正しく動作し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)# interface vlan 10`
`(config-if)# ip address 192.168.10.1 255.255.255.0`
 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。VLAN へ IP アドレスを設定していない場合は、ここで IP アドレスを設定します。
2. `(config-if)# vrrp 1 ip 192.168.10.100`
 VLAN 10, 仮想ルータ ID 1 の仮想ルータに仮想 IP アドレスを設定します。
3. `(config-if)# vrrp 1 name VRRPNAME`
 VLAN 10, 仮想ルータ ID 1 の仮想ルータに仮想ルータ名称を設定します。

(2) フォロー仮想ルータの設定

[設定のポイント]

仮想ルータからプライマリ仮想ルータ名称を指定します。プライマリ仮想ルータを指定した仮想ルータはフォロー仮想ルータとなり、指定したプライマリ仮想ルータの状態に従います。

フォロー仮想ルータには、プライマリ仮想ルータと同じ仮想ルータ ID を設定することを推奨します。

[コマンドによる設定]

1. `(config)# interface vlan 20`
`(config-if)# ip address 192.168.20.1 255.255.255.0`
 VLAN 20 の VLAN 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。VLAN へ IP アドレスを設定していない場合は、ここで IP アドレスを設定します。
2. `(config-if)# vrrp 1 follow VRRPNAME`
 VLAN 20、仮想ルータ ID 1 のフォロー仮想ルータが従うプライマリ仮想ルータ名称に VRRPNAME を指定します。
3. `(config-if)# vrrp 1 ip 192.168.20.100`
 VLAN 20、仮想ルータ ID 1 の仮想ルータに仮想 IP アドレスを設定します。

[注意事項]

- プライマリ仮想ルータが 255 個設定されている状態でフォロー仮想ルータを追加する場合は、`vrrp follow` コマンドから設定を開始してください。
- 指定したプライマリ仮想ルータが存在しない場合、フォロー仮想ルータはイニシャル状態となります。
- フォロー仮想ルータは、アドレス所有者になれません。
- ほかの仮想ルータからプライマリ仮想ルータに指定されている場合、フォロー仮想ルータになれません。また、自分自身の仮想ルータ名称、およびほかのフォロー仮想ルータ名称を指定できません。
- `vrrp name` コマンドを設定した仮想ルータは、トラッキング機能で障害を検出し仮想ルータの優先度が 0 になっても IP インタフェースはダウンしません。

(3) VRRP 管理 VLAN の設定

[設定のポイント]

Flush Request 機能を使用してすばやく通信を再開できるように、VRRP 管理 VLAN を設定します。

[コマンドによる設定]

1. `(config)# vrrp-vlan 4000`
 VRRP 管理 VLAN として使用する VLAN を指定します。本装置に設定された仮想ルータがマスタへ遷移したときに、本コマンドで指定した VRRP 管理 VLAN に対して、Flush Request フレーム (MAC アドレステーブルのクリアを促すフレーム) を送信します。

[注意事項]

- VRRP 管理 VLAN は、すべての下流の LAN スイッチが所属する VLAN に指定してください。

(4) VRRP 管理 VLAN でのレイヤ 2 ループ回避

[設定のポイント]

物理的な構成が異なる複数の VLAN に対して Flush Request 機能を適用する場合、それらの VLAN すべてを含むように VRRP 管理 VLAN を設定すると、VRRP 管理 VLAN でレイヤ 2 ループが発生する構成になるおそれがあります。

このような場合、次のどちらかの方法でレイヤ 2 ループを防止してください。

1. スパニングツリーや Ring Protocol などの L2 プロトコルを動作させる。
2. VRRP 管理 VLAN に廃棄フィルタを設定して、パケットを中継しない構成にする。この場合、VRRP 管理 VLAN は Flush Request 機能以外の用途と併用できません。

ここでは、2の廃棄フィルタの設定方法を示します。

[コマンドによる設定]

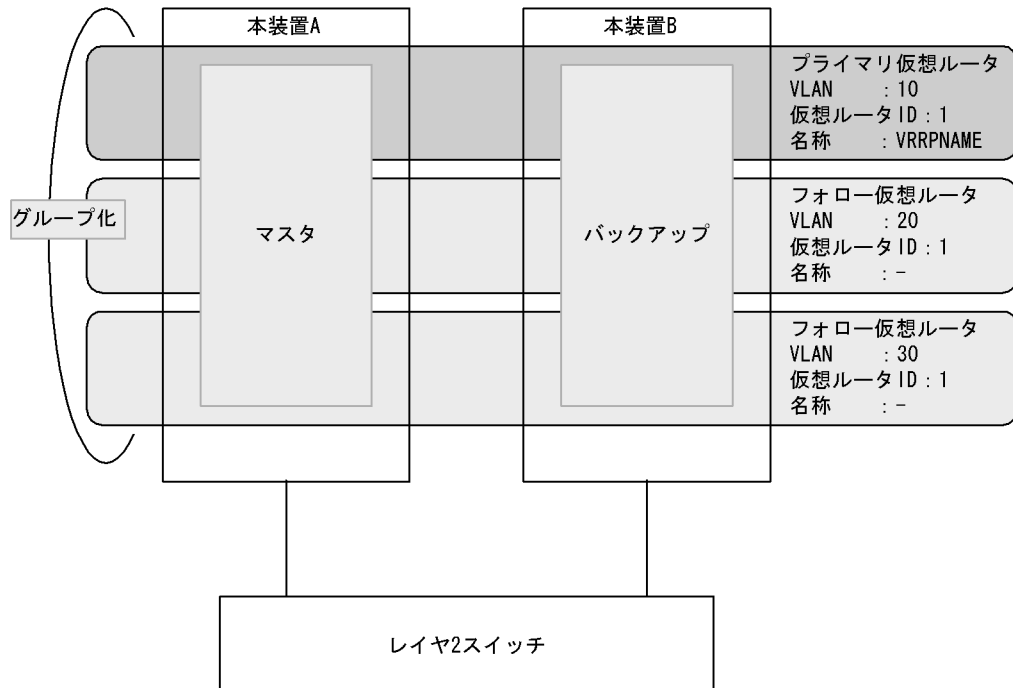
1. (config)# mac access-list extended VRRP-VLAN-MAC
 (config-ext-macl)# deny any any
 VRRP 管理 VLAN に設定する MAC フィルタを設定します。
2. (config)# ip access-list extended VRRP-VLAN-IP
 (config-ext-nacl)# deny ip any any
 VRRP 管理 VLAN に設定する IP フィルタを設定します。
3. (config)# ipv6 access-list VRRP-VLAN-IPv6
 (config-ipv6-acl)# deny ipv6 any any
 VRRP 管理 VLAN に設定する IPv6 フィルタを設定します。
4. (config)# interface vlan 4000
 (config-if)# mac access-group VRRP-VLAN-MAC in layer2-forwarding
 (config-if)# ip access-group VRRP-VLAN-IP in layer2-forwarding
 (config-if)# ip access-group VRRP-VLAN-IP in layer3-forwarding
 (config-if)# ipv6 traffic-filter VRRP-VLAN-IPv6 in layer2-forwarding
 (config-if)# ipv6 traffic-filter VRRP-VLAN-IPv6 in layer3-forwarding
 各フィルタを、VRRP 管理 VLAN へ設定します。

23.2.12 グループ構成の変更

プライマリ仮想ルータを別の仮想ルータへ変更する場合の手順を次に示します。この手順に従わない場合、両装置の仮想ルータがマスタ状態になるおそれがあります。

変更前と変更後の仮想ルータのグループ構成を次の図に示します。なお、本装置 A がマスタ装置、本装置 B がバックアップ装置とします。

図 23-19 仮想ルータのグループ構成（変更前）






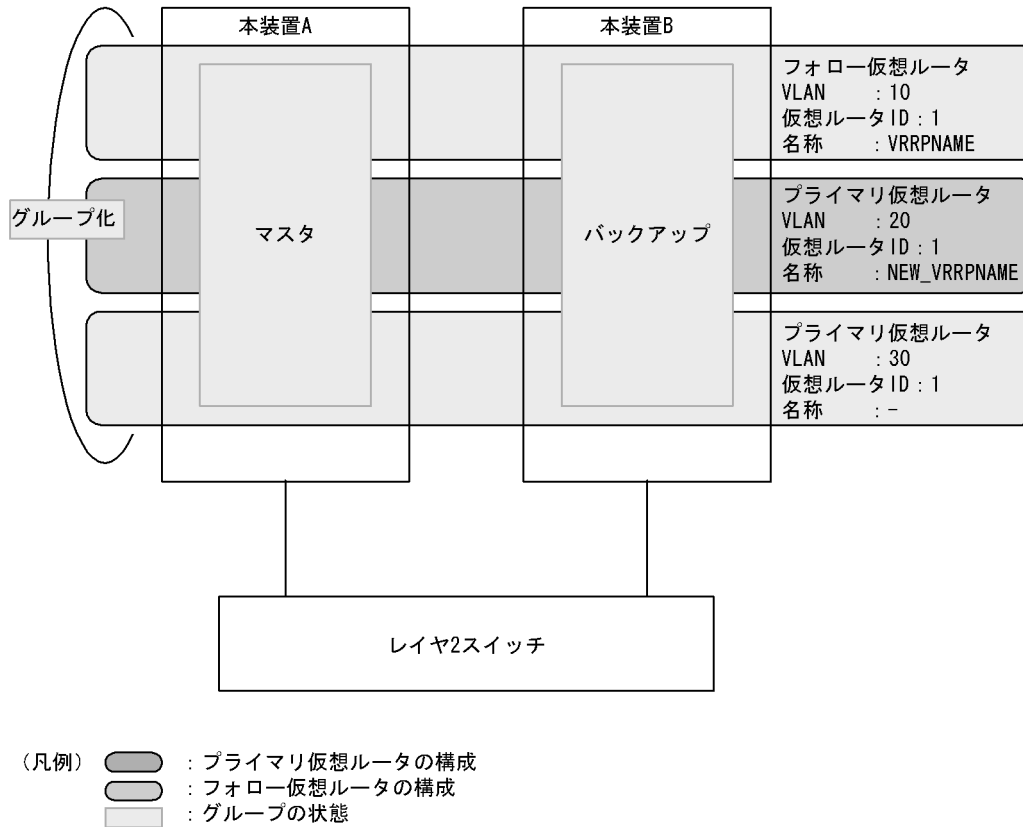
- (凡例)
-  : プライマリ仮想ルータの構成
 -  : フォロワー仮想ルータの構成
 -  : グループの状態

図 23-20 仮想ルータのグループ構成（変更後）



(1) フォロー仮想ルータからプライマリ仮想ルータへ変更

[設定のポイント]

フォロー仮想ルータをプライマリ仮想ルータに変更します。マスタ装置（本装置 A）から設定を変更する必要があります。

バックアップ装置（本装置 B）から変更した場合、バックアップ装置（本装置 B）の仮想ルータは ADVERTISEMENT パケットを受信しないため、マスタ状態へ遷移します。また、マスタ装置（本装置 A）はマスタ状態であるプライマリ仮想ルータに従ってマスタ状態のままとなるため、両装置の仮想ルータがマスタ状態になります。

[コマンドによる設定]

1. `(config)# interface vlan 20`
VLAN 20 の VLAN 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。
2. `(config-if)# no vrrp 1 follow`
VLAN 20, 仮想ルータ ID 1 のフォロー仮想ルータをプライマリ仮想ルータとして動作させます。
本装置 A, 本装置 B の順に変更します。
3. `(config-if)# vrrp 1 name NEW_VRRPNAME`
VLAN 20, 仮想ルータ ID 1 のプライマリ仮想ルータに仮想ルータ名称を設定します。

(2) フォロー仮想ルータの設定変更

[設定のポイント]

フォロー仮想ルータの従っているプライマリ仮想ルータを変更します。

フォロー仮想ルータは ADVERTISEMENT パケットを送受信しないでプライマリ仮想ルータの状態に従うため、どちらの装置からでも設定を変更できます。動作していないプライマリ仮想ルータを指定した場合、フォロー仮想ルータはイニシャル状態となります。

[コマンドによる設定]

1. `(config)# interface vlan 30`
VLAN 30 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。
2. `(config-if)# vrrp 1 follow NEW_VRRPNAME`
VLAN 30、仮想ルータ ID 1 の仮想ルータが従うプライマリ仮想ルータを変更します。

(3) プライマリ仮想ルータからフォロー仮想ルータへ変更

[設定のポイント]

プライマリ仮想ルータをフォロー仮想ルータに変更します。バックアップ装置側から設定を変更する必要があります。

マスタ装置（本装置 A）から変更した場合、バックアップ装置（本装置 B）の仮想ルータは、ADVERTISEMENT パケットを受信しないためマスタ状態へ遷移します。また、マスタ装置（本装置 A）はマスタ状態であるプライマリ仮想ルータに従ってマスタ状態のままとなるため、両装置の仮想ルータがマスタ状態になります。

[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。
2. `(config-if)# vrrp 1 follow NEW_VRRPNAME`
VLAN 10、仮想ルータ ID 1 の仮想ルータをフォロー仮想ルータとして動作させます。
本装置 B、本装置 A の順に変更します。

23.3 オペレーション

23.3.1 運用コマンド一覧

VRRPの運用コマンド一覧を次の表に示します。

表 23-11 運用コマンド一覧

コマンド名	説明
show vrrpstatus	仮想ルータの動作状態を表示します。
clear vrrpstatus	仮想ルータの統計情報を初期化します。
swap vrrp	自動切り戻しが抑止されているときに切り戻し処理を起動します。
show track	track に保存されている障害監視方法の設定を表示します。

23.3.2 仮想ルータの設定確認

仮想ルータの設定確認は、運用コマンド show vrrpstatus で行います。

(1) 詳細情報の確認

detail パラメータを指定すると、仮想ルータの設定の詳細情報を取得できます。

図 23-21 show vrrpstatus コマンドの実行結果

```
> show vrrpstatus detail interface vlan 10 vrid 1
Date 2009/07/15 12:00:00 UTC
VLAN0010: VRID 1 VRF 2
  Virtual Router IP Address : 170.10.10.2
  Virtual MAC Address : 0000.5e00.0101
  Virtual Router Name : VRRPNAME1 (primary)
  Virtual Router Follow : -
  Number of Follow virtual routers : 4
  Current State : MASTER
  Admin State : enable
  Priority : 80 /100
  IP Address Count : 1
  Master Router's IP Address : 170.10.10.2
  Primary IP Address : 170.10.10.1
  Authentication Type : SIMPLE TEXT PASSWORD(Disable)
  Authentication Key : ABCDEFG(Disable)
  Advertisement Interval : 250 msec
  Master Advertisement Interval : 1000 msec
  Preempt Mode : ON
  Preempt Delay : 60
  Non Preempt swap timer : 30
  Accept Mode : ON
  Virtual Router Up Time : Tue Feb 22 13:05:53 2000
  track 10 VLAN0022 VRF 3 Status : (IF UP) Down Priority : 50
    Target Address : 192.168.0.20
    Vrrp Polling Status : reachable
  track 20 VLAN0023 Status : (IF UP) Down Priority : 40
  track 30 gigabitethernet 1/10 Status : (IF DOWN) Down Priority : 20
  track 40 port-channel 2 Status : (IF UP) Down Priority : 20
  IPv4 Advertisement Type : ietf-unified-spec-02-mode
>
```


(2) グループ情報の確認

group パラメータを指定すると、仮想ルータの設定のグループ情報を取得できます。仮想ルータ名称がわかる場合、name パラメータを指定して仮想ルータ情報を取得できます。

図 23-22 show vrrpstatus group コマンドの実行結果 (プライマリ仮想ルータの場合)

```
> show vrrpstatus group name VRRPNAME1
Date 2008/12/15 12:00:00 UTC
VLAN0010: VRID 1 VRF 2
  Virtual Router Name           : VRRPNAME1 (primary)
  Virtual Router Follow         : -
  Number of Follow virtual routers : 4
  Followed by virtual routers  :
    VLAN0020: VRID 1 VRF 2
    VLAN0030: VRID 1 VRF 2
    VLAN0040: VRID 1 VRF 2
    VLAN0050: VRID 1 VRF 2
```

図 23-23 show vrrpstatus group コマンドの実行結果 (フォロー仮想ルータの場合)

```
> show vrrpstatus group interface vlan 20 vrid 1
Date 2008/12/15 12:00:00 UTC
VLAN0020: VRID 1 VRF 2
  Virtual Router Name           : VRRPNAME2 (follow)
  Virtual Router Follow         : VRRPNAME1 (VLAN0010: VRID 1 VRF 2 )
  Number of Follow virtual routers: 0
  Followed by virtual routers  : -
```

23.3.3 track の設定確認

track の設定確認は、運用コマンド show track で行います。

図 23-24 show track コマンドの実行結果

```
> show track detail
Date 2008/12/15 12:00:00 UTC
track : 20 interface : VLAN0030 Mode : (polling)
  Target Address : 192.168.20.1
  Assigned to :
    VLAN0010: VRID 1
track : 30 interface : VLAN0031 Mode : (interface)
  Assigned to :
    VLAN0010: VRID 1
track : 40 interface : VLAN0032 Mode : (polling)
  Target Address : 192.168.40.1
  Assigned to :
    VLAN0010: VRID 1
track : 50 interface : VLAN0034 Mode : (polling)
  Target Address : 192.168.20.1
track : 60 interface : gigabitethernet 1/1 Mode : (interface)
  Assigned to :
    VLAN0020: VRID 1
track : 70 interface : port-channel 2 Mode : (interface)
  Assigned to :
    VLAN0030: VRID 1
>
```

23.3.4 切り戻し処理の実行

自動切り戻しが抑止されている、マスタより優先度が高いにもかかわらずバックアップに留まっている仮想ルータへ swap vrrp コマンドを実行すると、切り戻し処理を起動できます。ただし、swap vrrp コマン

ドを実行しても、優先度の低い仮想ルータをマスタにすることはできません。

24 IEEE802.3ah/UDLD

IEEE802.3ah/UDLD 機能は、片方向リンク障害を検出し、それに伴うネットワーク障害の発生を事前に防止する機能です。
この章では、IEEE802.3ah/UDLD 機能の解説と操作方法について説明します。

24.1 解説

24.2 コンフィグレーション

24.3 オペレーション

24.1 解説

24.1.1 概要

UDLD (Uni-Directional Link Detection) とは、片方向リンク障害を検出する機能です。

片方向リンク障害が発生すると、一方の装置では送信はできるが受信ができず、もう一方の装置では受信はできるが送信ができない状態になり、上位プロトコルで誤動作が発生し、ネットワーク上でさまざまな障害が発生します。よく知られている例として、スパンニングツリーでのループ発生や、リンクアグリゲーションでのフレーム紛失が挙げられます。これらの障害は、片方向リンク障害を検出した場合に該当するポートを inactivate することによって未然に防ぐことができます。

IEEE802.3ah (Ethernet in the First Mile) で slow プロトコルの一部として位置づけられた OAM (Operations, Administration, and Maintenance) プロトコル (以下、IEEE802.3ah/OAM と示す) では、双方向リンク状態の監視を行うために、制御フレームを用いて定期的に対向装置と自装置の OAM 状態情報の交換を行い、相手装置とのフレームの到達性を確認する方式が述べられています。本装置では IEEE802.3ah/OAM 機能を用いて双方向リンク状態の監視を行い、その確認がとれない場合に片方向リンク障害を検出する方式で UDLD 機能を実現しています。本装置の UDLD 機能では、片方向リンク障害の検出のほかに、自装置から送信した制御フレームを同一装置で受信した場合はループと判断して、受信したポートを inactivate します。

また、IEEE802.3ah/OAM プロトコルでは、Active モードと Passive モードの概念があり、Active モード側から制御フレームの送信が開始され、Passive モード側では、制御フレームを受信するまで制御フレームの送信は行いません。本装置では工場出荷時の設定で IEEE802.3ah/OAM 機能が有効になっていて、全ポートが Passive モードで動作します。

Ethernet ケーブルで接続された双方の装置のポートにコンフィグレーションコマンド `efmoam active udld` を設定することで、片方向リンク障害の検出動作を行います。efmoam active udld コマンドを設定したポートで片方向リンク障害を検出した場合、該当するポートを inactivate することで対向装置側のポートでもリンクダウンが検出され、接続された双方の装置で該当ポートでの運用を停止します。

24.1.2 サポート仕様

IEEE802.3ah/UDLD 機能では、次の表に示すとおり IEEE802.3ah/OAM 機能をサポートしています。

表 24-1 IEEE802.3ah/UDLD でサポートする IEEE802.3ah OAMPDU

名称	説明	サポート
Information	相手装置に OAM 状態情報を送信する。	
Event Notification	相手装置に Link Event の警告を送信する。	×
Variable Request	相手装置に MIB 変数を要求する。	×
Variable Response	要求された MIB 変数を送信する。	×
Loopback Control	相手装置の Loopback 状態を制御する。	×
Organization Specific	機能拡張用。	×

(凡例) : サポート × : 未サポート

24.1.3 IEEE802.3ah/UDLD 使用時の注意事項

(1) IEEE802.3ah/UDLD 機能を設定した装置間に IEEE802.3ah/OAM 機能をサポートしない装置を接続した場合

一般的なスイッチでは、IEEE802.3ah/OAM 機能で使用する制御フレームは中継しません。このため、装置間で情報の交換ができず、コンフィグレーションコマンド `efmoam active udld` を設定したポートで片方向リンク障害を検出してしまいます。IEEE802.3ah/UDLD 機能の運用はできません。

(2) IEEE802.3ah/UDLD 機能を設定した装置間にメディアコンバータなどの中継装置を接続した場合

片方のリンク状態が切断された場合に、もう片方のリンク状態を自動的に切断しないメディアコンバータを装置間に設置した場合、装置間でリンク状態の認識にずれが生じます。このため、コンフィグレーションコマンド `efmoam active udld` を設定したポートで相手装置が動作していない状態でも片方向リンク障害を検出してしまいます。復旧する際にも、双方の装置で同期をとる必要があり、運用が困難になります。片方のリンク状態が切断された場合に、もう片方のリンク状態を自動的に切断する機能のあるメディアコンバータを使用してください。

(3) 他社の UDLD 機能との接続について

UDLD 機能はそれぞれ各社の独自仕様で機能を実装しているため、本装置の IEEE802.3ah/UDLD 機能と他社装置の UDLD 機能の相互接続はできません。

24.2 コンフィグレーション

24.2.1 コンフィグレーションコマンド一覧

IEEE802.3ah/UDLD 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 24-2 コンフィグレーションコマンド一覧

コマンド名	説明
efmoam active	物理ポートで IEEE802.3ah/OAM 機能の active モードにします。
efmoam disable	IEEE802.3ah/OAM 機能を無効にします。
efmoam udld-detection-count	片方向リンク障害とするためのカウンタ値を指定します。

24.2.2 IEEE802.3ah/UDLD の設定

(1) IEEE802.3ah/UDLD 機能の設定

[設定のポイント]

IEEE802.3ah/UDLD 機能を運用するには、先ず装置全体で IEEE802.3ah/OAM 機能を有効にしておく必要があります。本装置では工場出荷時の設定で IEEE802.3ah/OAM 機能が有効となっている状態（全ポート Passive モード）です。次に、実際に片方向リンク障害検出機能を動作させたいポートに対し、UDLD パラメータを付加した Active モードの設定をします。

ここでは、gigabitethernet 1/1 で IEEE802.3ah/UDLD 機能を運用させます。

[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)# efmoam active udld

ポート 1/1 で IEEE802.3ah/OAM 機能の Active モード動作を行い、片方向リンク障害検出動作を開始します。

(2) 片方向リンク障害検出カウンタの設定

[設定のポイント]

片方向リンク障害は、相手からの情報がタイムアウトして双方向リンク状態の確認ができない状態が、決められた数だけ連続して発生した場合に検出します。この数が片方向リンク障害検出カウンタです。双方向リンク状態は、1 秒に 1 回確認しています。

片方向リンク障害検出カウンタを変更すると、実際に片方向リンク障害が発生してから検出するまでの時間を調整できます。片方向リンク障害検出カウンタを少なくすると障害を早く検出する一方で、誤検出のおそれがあります。通常、本設定は変更する必要はありません。

片方向リンク障害発生から検出までのおよその時間を次に示します。なお、最大 10% の誤差が生じます。

5+ (片方向リンク障害検出カウンタ)[秒]

[コマンドによる設定]

1. (config)# efmoam udld-detection-count 60

片方向リンク障害検出とするための相手からの情報タイムアウト発生連続回数を 60 回に設定します。

24.3 オペレーション

24.3.1 運用コマンド一覧

IEEE802.3ah/OAM 機能の運用コマンド一覧を次の表に示します。

表 24-3 運用コマンド一覧

コマンド名	説明
show efmoam	IEEE802.3ah/OAM の設定情報およびポートの設定情報を表示します。
show efmoam statistics	IEEE802.3ah/OAM に関する統計情報を表示します。
clear efmoam statistics	IEEE802.3ah/OAM に関する統計情報をクリアします。
restart efmoam	IEEE802.3ah/OAM プログラムを再起動します。
dump protocols efmoam	IEEE802.3ah/OAM 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。

24.3.2 IEEE802.3ah/OAM 情報の表示

IEEE802.3ah/OAM 情報の表示は、運用コマンド show efmoam で行います。show efmoam コマンドは、IEEE802.3ah/OAM の設定情報と active モードに設定されたポートの情報を表示します。show efmoam detail コマンドは、active モードに設定されたポートに加え、相手装置を認識している passive モードのポートの情報を表示します。また、show efmoam statistics コマンドでは、IEEE802.3ah/OAM プロトコルの統計情報に加え、IEEE802.3ah/UDLD 機能で検出した障害状況を表示します。

図 24-1 show efmoam コマンドの実行結果

```
> show efmoam
Date 2006/10/02 23:59:59 UTC
Status: Enabled
udld-detection-count: 30
Port   Link status   UDLD status   Dest MAC
1/1    Up            detection     * 0012.e298.dc20
1/2    Down         active        unknown
1/4    Down(uni-link) detection     unknown
>
```

図 24-2 show efmoam detail コマンドの実行結果

```
> show efmoam detail
Date 2006/10/02 23:59:59 UTC
Status: Enabled
udld-detection-count: 30
Port   Link status   UDLD status   Dest MAC
1/1    Up            detection     * 0012.e298.dc20
1/2    Down         active        unknown
1/3    Up            passive       0012.e298.7478
1/4    Down(uni-link) detection     unknown
>
```


図 24-3 show efmoam statistics コマンドの実行結果

```

> show efmoam statistics
Date 2006/10/02 23:59:59 UTC
Port 1/1 [detection]
  OAMPDUs   :Tx      =      295 Rx      =      295
              Invalid =      0 Unrecogn.=      0
  TLVs      :Invalid =      0 Unrecogn.=      0
  Info TLV  :Tx_Local =     190 Tx_Remote=     105 Rx_Remote=     187
              Timeout =      3 Invalid  =      0 Unstable =      0
  Inactivate:TLV =      0 Timeout  =      0
Port 1/2 [active]
  OAMPDUs   :Tx      =     100 Rx      =     100
              Invalid =      0 Unrecogn.=      0
  TLVs      :Invalid =      0 Unrecogn.=      0
  Info TLV  :Tx_Local =     100 Tx_Remote=     100 Rx_Remote=     100
              Timeout =      0 Invalid  =      0 Unstable =      0
  Inactivate:TLV =      0 Timeout  =      0
Port 1/3 [passive]
  OAMPDUs   :Tx      =     100 Rx      =     100
              Invalid =      0 Unrecogn.=      0
  TLVs      :Invalid =      0 Unrecogn.=      0
  Info TLV  :Tx_Local =      0 Tx_Remote=     100 Rx_Remote=     100
              Timeout =      0 Invalid  =      0 Unstable =      0
  Inactivate:TLV =      0 Timeout  =      0
>

```


25 ストームコントロール

ストームコントロールはフラッディング対象フレーム中継の量を制限する機能です。この章では、ストームコントロール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

25.1 解説

25.1.1 ストームコントロールの概要

レイヤ2ネットワークでは、ネットワーク内にループが存在すると、ブロードキャストフレームなどがスイッチ間で無制限に中継されて、ネットワークおよび接続された機器に異常な負荷を掛けることとなります。このような現象はブロードキャストストームと呼ばれ、レイヤ2ネットワークでは避けなければならない問題です。マルチキャストフレームが無制限に中継されるマルチキャストストーム、ユニキャストフレームが無制限に中継されるユニキャストストームも防止する必要があります。

ネットワークおよび接続された機器への影響を抑えるために、スイッチでフラッディング対象フレーム中継の量を制限する機能がストームコントロールです。

本装置では、ストームコントロールの対象とするフレーム種別を設定します。この設定は、装置全体で有効になります。また、イーサネットインタフェースごとに、閾値として受信する最大帯域を設定でき、その値を超えたフレームを廃棄します。閾値の設定は、ブロードキャストフレーム、マルチキャストフレーム、ユニキャストフレームの3種類のフレームのうち、ストームコントロールの対象として設定されているフレームの帯域の合計値です。

さらに、受信した帯域が閾値を超えた場合、そのポートを閉塞したり、プライベートトラップやログメッセージを出力したりできます。

ストームコントロールの運用コマンドはありません。

25.1.2 ストームコントロール使用時の注意事項

(1) ストームの検出と回復の検出

本装置は、受信帯域がコンフィグレーションで設定された閾値を超えたときに、ストームが発生したと判定します。ストームが発生したあと、受信帯域が閾値以下の状態が30秒続いたときに、ストームが回復したと判定します。なお、受信帯域が閾値を超えたときのフレームは廃棄せずに中継し、その後のフレームから廃棄します。

本装置のストームコントロール機能は、フロー制御の帯域制御機能を使用しています。フロー制御の帯域制御機能については、「5.4 帯域監視解説」を参照してください。ストームコントロール機能のバーストサイズは16000byteで変更できません。

受信帯域の計算では、フレーム間ギャップからFCSまでのオクテット数を使用します。運用コマンド `show interfaces` や `interfaces` グループ MIB などの受信オクテット数はMACヘッダからFCSまでなので、受信するフレーム当たり20オクテットの違いがあります。`show interfaces` コマンドで表示された受信スループットが10Mbpsで、平均受信フレーム長(MACヘッダからFCSまで)が100オクテットの場合、ストームコントロール機能での受信帯域は12Mbpsとなります。

ストーム発生時にポートを閉塞する場合は、そのポートではフレームを受信しなくなるため、ストームの回復も検出できなくなります。ストーム発生時にポートの閉塞を設定した場合は、ネットワーク監視装置などの本装置とは別の手段でストームが回復したことを確認してください。

(2) フロー制御との関連

本装置のストームコントロール機能は、フロー制御の帯域制御機能を使用するため、ストームコントロール機能とフロー制御の帯域監視を同時に使用する場合は、帯域監視ストームコントロールモードを指定せずにデフォルトで使用するか、コンフィグレーションコマンド `upc-storm-control mode` で

upc-in-and-storm-control パラメータを指定する必要があります。

(3) ポリシーベーススイッチングを併用した場合の動作

ストームコントロールの対象となるフレームをポリシーベーススイッチングの対象とした場合、ポリシーベーススイッチングが優先的に動作して、ポリシーベーススイッチングで設定した送信先インターフェースに中継されます。

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

ストームコントロール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 25-1 コンフィグレーションコマンド一覧

コマンド名	説明
storm-control	装置でストームコントロールの対象とするフレーム種別を設定します。また、インタフェースでストームコントロールの閾値や、ストームを検出したときの動作を設定します。

25.2.2 ストームコントロールの設定

対象フレームの設定

本装置では、ブロードキャストフレーム、マルチキャストフレーム、ユニキャストフラディングフレームの3種類のフレームを、ストームコントロールの対象とすることが設定できます。例えば、IPマルチキャスト通信を使う場合、ブロードキャストフレームとユニキャストフラディングフレームだけをストームコントロールの対象とすることができます。

ブロードキャストフレームの抑制

ブロードキャストストームを防止するためには、イーサネットインタフェースで受信するブロードキャストフレームの帯域を閾値として設定します。ブロードキャストフレームには、ARPパケットなど通信に必要なフレームも含まれるので、閾値には通常使用するフレームの帯域を考慮して余裕のある値を設定します。

マルチキャストフレームの抑制

マルチキャストストームを防止するためには、イーサネットインタフェースで受信するマルチキャストフレームの帯域を閾値として設定します。マルチキャストフレームには、IPv4マルチキャストパケット、IPv6マルチキャストパケット、OSPFパケットなどの制御パケットなど通信に必要なフレームも含まれるので、閾値には通常使用するフレームの帯域を考慮して余裕のある値を設定します。

ユニキャストストームの抑制

ユニキャストストームを防止するためには、イーサネットインタフェースで受信するユニキャストフラディングフレームの帯域を閾値として設定します。閾値には通常使用するフレームの帯域を考慮して余裕のある値を設定します。

ストーム検出時の動作

ストームを検出したときの本装置の動作を設定します。ポートの閉塞、プライベートトラップの送信、ログメッセージの出力を、ポートごとに組み合わせて選択できます。

- ポートの閉塞
ストームを検出したとき、そのポートを `inactive` 状態にします。ストームが回復したあと、再びそのポートを `active` 状態に戻すには、`activate` コマンドを使用します。なお、リンクアグリゲーションでは、該当チャンネルグループ内のすべてのポートを `inactive` 状態にします。
- プライベートトラップの送信
ストームを検出したときおよびストームの回復を検出したとき、プライベートトラップを送信して通知します。
- ログメッセージの出力
ストームを検出したときおよびストームの回復を検出したとき、ログメッセージを出力して通知します。ただし、ポートの閉塞時のメッセージは必ず出力します。

[設定のポイント]

設定できるインタフェースはイーサネットインタフェースです。閾値の指定では、受信する最大帯域を指定します。この帯域の計算には、フレーム間ギャップから FCS までを使用します。

なお、帯域監視ストームコントロールモードを指定せずにデフォルトで使用するか、`upc-storm-control mode` コマンドで `upc-in-and-storm-control` パラメータを指定する必要があります。

[コマンドによる設定]

ブロードキャストおよびユニキャストフレームを監視し、ストーム検出時にポートを閉塞する場合の例を示します。

1. `(config)# no storm-control multicast`
マルチキャストフレームをストームコントロールの対象外に設定します。
2. `(config)# interface gigabitethernet 1/10`
`(config-if)# storm-control level 20`
ブロードキャストフレームおよびユニキャストフレームの閾値を帯域の 20% に設定します。
3. `(config-if)# storm-control action inactivate`
ストームを検出したときに、ポートを `inactive` 状態にします。

26 L2 ループ検知

L2 ループ検知機能は、レイヤ 2 ネットワークでループ障害を検知し、ループの原因となるポートを inactive 状態にすることでループ障害を解消する機能です。

この章では、L2 ループ検知機能の解説と操作方法について説明します。

26.1 解説

26.2 コンフィグレーション

26.3 オペレーション

26.1 解説

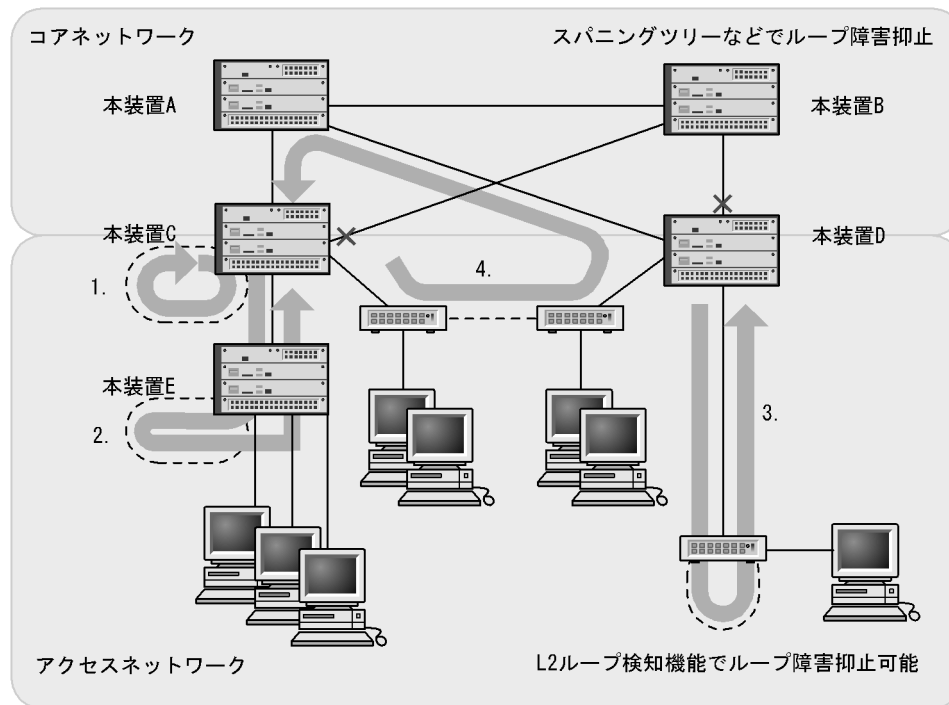
26.1.1 概要

レイヤ2ネットワークでは、ネットワーク内にループ障害が発生すると、MACアドレス学習が安定しなくなったり、装置に負荷が掛かったりして正常な通信ができない状態になります。このような状態を回避するためのプロトコルとして、スパンニングツリーや Ring Protocol などがありますが、L2 ループ検知機能は、一般的にそれらプロトコルを動作させているコアネットワークではなく、冗長化をしていないアクセスネットワークでのループ障害を解消する機能です。

L2 ループ検知機能は、自装置でループ障害を検知した場合、検知したポートを inactive 状態にすることで、原因となっている箇所をネットワークから切り離し、ネットワーク全体にループ障害が波及しないようにします。

ループ障害の基本パターンを次の図に示します。

図 26-1 ループ障害の基本パターン



(凡例) -----: 誤接続した回線
 →: ループの流れ
 X: ブロック状態

ループ障害のパターン例

1. 自装置で回線を誤接続し、ループ障害が発生している。
- 2, 3. 自装置から下位の本装置または L2 スイッチで回線を誤接続し、ループ障害が発生している。
4. 下位装置で回線を誤接続し、コアネットワークにわたるループ障害が発生している。

L2 ループ検知機能は、このような自装置での誤接続や他装置での誤接続など、さまざまな場所でのループ障害を検知できます。

26.1.2 動作仕様

L2 ループ検知機能では、コンフィグレーションで設定したポート（物理ポートまたはチャンネルグループ）から L2 ループ検知用の L2 制御フレーム（L2 ループ検知フレーム）を定期的送信します。L2 ループ検知機能が有効なポートでその L2 ループ検知フレームを受信した場合、ループ障害と判断し、受信したポートまたは送信元ポートを inactive 状態にします。

inactive 状態のポートは、ループ障害の原因を解決後に運用コマンドで active 状態にします。また、自動復旧機能を設定しておけば、自動的に active 状態にできます。

(1) L2 ループ検知機能のポート種別

L2 ループ検知機能で使用するポートの種別を次の表に示します。

表 26-1 ポート種別

種別	機能
検知送信閉塞ポート	<ul style="list-style-type: none"> ループを検知するための L2 ループ検知フレームを送信します。 ループ障害検知時は、運用ログを表示し、当該ポートを inactive 状態にします。
検知送信ポート	<ul style="list-style-type: none"> ループを検知するための L2 ループ検知フレームを送信します。 ループ障害検知時は、運用ログを表示します。inactive 状態にはしません。
検知ポート (コンフィグレーション省略時)	<ul style="list-style-type: none"> ループを検知するための L2 ループ検知フレームは送信しません。 ループ障害検知時は、運用ログを表示します。inactive 状態にはしません。
検知対象外ポート	<ul style="list-style-type: none"> 本機能の対象外ポートです。ループを検知するための L2 ループ検知フレームの送信やループ障害検知をしません。
アップリンクポート	<ul style="list-style-type: none"> ループを検知するための L2 ループ検知フレームは送信しません。 ループ障害検知時は、送信元ポートで、送信元のポート種別に従った動作をします。例えば、送信元が検知送信閉塞ポートであれば、運用ログを表示し、送信元ポートを inactive 状態にします。

(2) L2 ループ検知フレームの送信ポートについて

L2 ループ検知フレームは、検知送信閉塞ポートと検知送信ポートに所属しているすべての VLAN から、設定した送信間隔で送信します。本機能で送信できる最大フレーム数は決まっています、それを超えるフレームは送信しません。フレームを送信できなかったポートや VLAN では、ループ障害を検知できなくなります。そのため、送信できる最大フレーム数は、収容条件に従って設定してください。詳細については、マニュアル「コンフィグレーションガイド Vol.1 3. 収容条件」を参照してください。

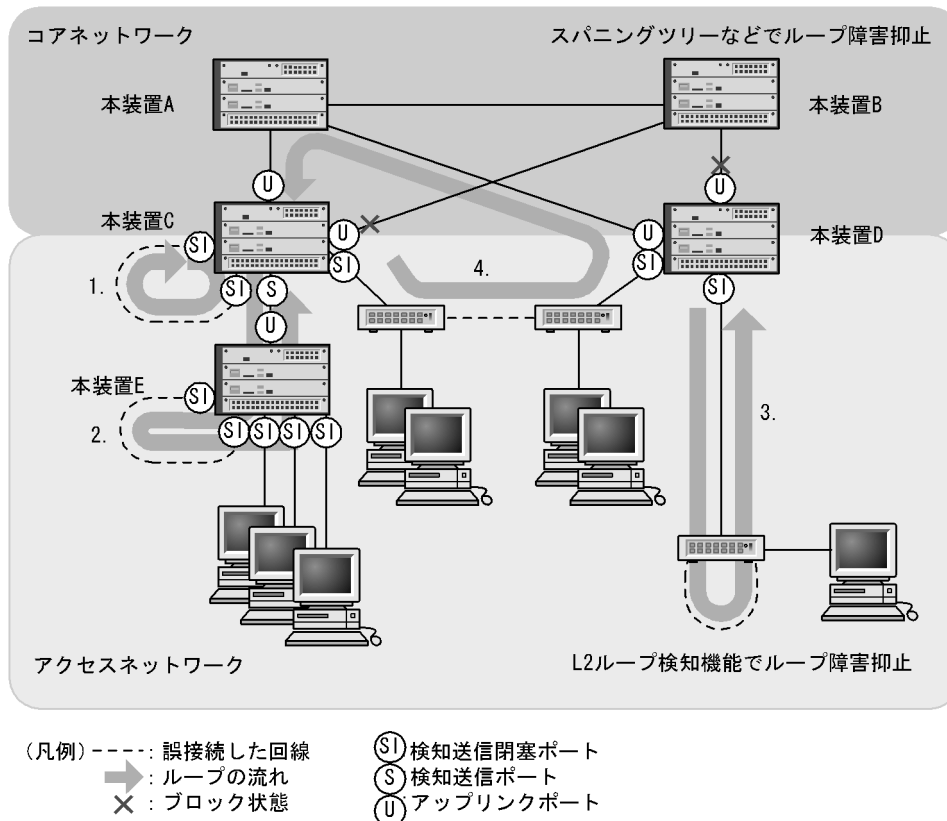
(3) ループ障害の検知方法とポートを inactive 状態にする条件

自装置から送信した L2 ループ検知フレームを受信した場合、ポートごとに受信数を計上し、コンフィグレーションで設定した L2 ループ検知フレーム受信数（初期値は 1）に達すると、該当するポートを inactive 状態（検知送信閉塞ポートだけ）にします。

26.1.3 適用例

L2 ループ検知機能を適用したネットワーク構成を示します。

図 26-2 L2 ループ検知機能を適用したネットワーク構成



(1) 検知送信閉塞ポートの適用

L2 ループ検知機能で一般的に設定するポート種別です。本装置 C, D, E で示すように、下位側のポートに設定しておくことで、1, 2, 3 のような下位側の誤接続によるループ障害に対応します。

(2) 検知送信ポートの適用

ループ障害の波及範囲を局所化するためには、できるだけ下位の装置で本機能を動作させるほうが有効です。本装置 C と本装置 E のように多段で接続している場合に、2. のような誤接続で本装置 C 側のポートを inactive 状態にすると、本装置 E のループ障害と関係しないすべての端末で上位ネットワークへの接続ができなくなります。そのため、より下流となる本装置 E で L2 ループ検知機能を動作させることを推奨します。

なお、その場合は、本装置 C 側のポートには検知送信ポートを設定しておきます。この設定によって、正常運用時は本装置 E でループ障害を検知しますが、本装置 E で L2 ループ検知機能の設定誤りなどでループ障害を検知できないときには、本装置 C でループ障害を検知 (inactive 状態にはならない) できます。

(3) アップリンクポートの適用

上位ネットワークに繋がっているポートまたはコアネットワークに接続するポートで設定します。この設定によって、4. のような誤接続となった場合、装置 C の送信元ポートが inactive 状態になるため、コアネットワークへの接続を確保できます。

26.1.4 L2 ループ検知使用時の注意事項

(1) L2 ループ検知運用時の物理ポート数

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。詳細については、マニュアル「コンフィグレーションガイド Vol.1 3. 収容条件」を参照してください。

(2) L2 ループ検知機能の ID 設定について

同一ネットワーク内の複数の本装置で L2 ループ検知機能を動作させる場合、ID には各装置でユニークな値を設定してください。同一の値を設定すると、ループ障害が発生しても検知できません。

(3) 二重化構成での自動 active 状態設定について

自動的に active 状態にする設定をしていますが、ループ障害検知でポートが inactive 状態のときに系切替が発生すると、新運用系システムではそのポートは inactive 状態のままです。その場合は、運用コマンド `activate` でそのポートを active 状態にしてください。

(4) プロトコル VLAN や MAC VLAN での動作について

L2 ループ検知フレームは、独自フォーマットの Untagged フレームです。プロトコルポートや MAC ポートではネイティブ VLAN として転送されるため、次に示す条件をどちらも満たしている場合、装置間にわたるループ障害が検知できないおそれがあります。

- コアネットワーク側のポートをアップリンクポートとして設定している
- コアネットワーク側にネイティブ VLAN を設定していない

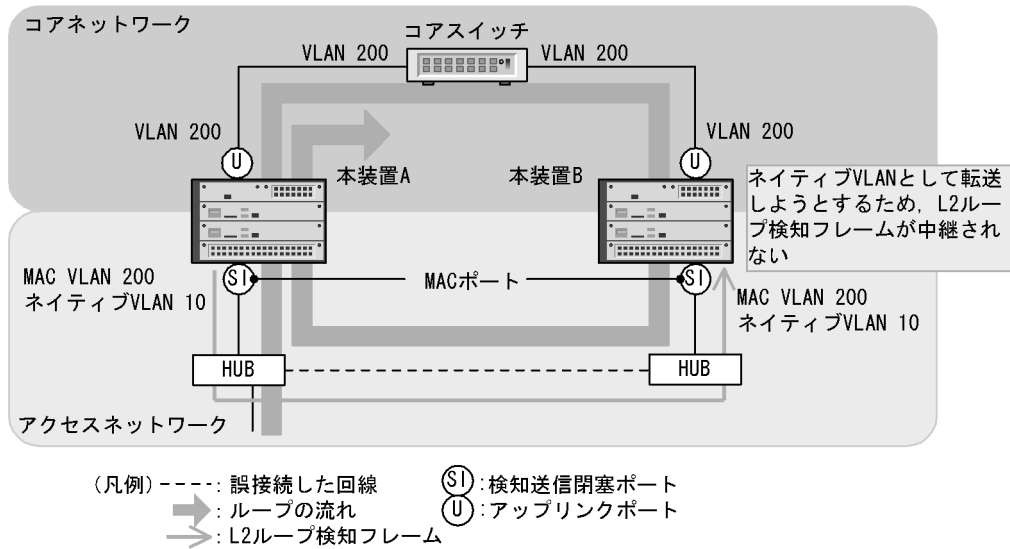
この場合は、アップリンクポートとして設定しているコアネットワーク側のポートを検知送信ポートに設定すると、ループ障害を検知できます。具体的な構成例を次に示します。

(a) ループ検知の制限となる構成例

次の図に示す構成で本装置配下の HUB 間を誤接続すると、装置間にわたるループが発生します。

本装置 A は HUB 側の検知送信閉塞ポートから L2 ループ検知フレームを送信し、コアスイッチ側のアップリンクポートからは送信しません。本装置 B は MAC ポートで受信した L2 ループ検知フレームをネイティブ VLAN として転送しようとするため、L2 ループ検知フレームはコアスイッチ側へ中継されません。この場合、L2 ループ検知フレームは本装置 A へ戻ってこないため、ループ障害を検知できません。

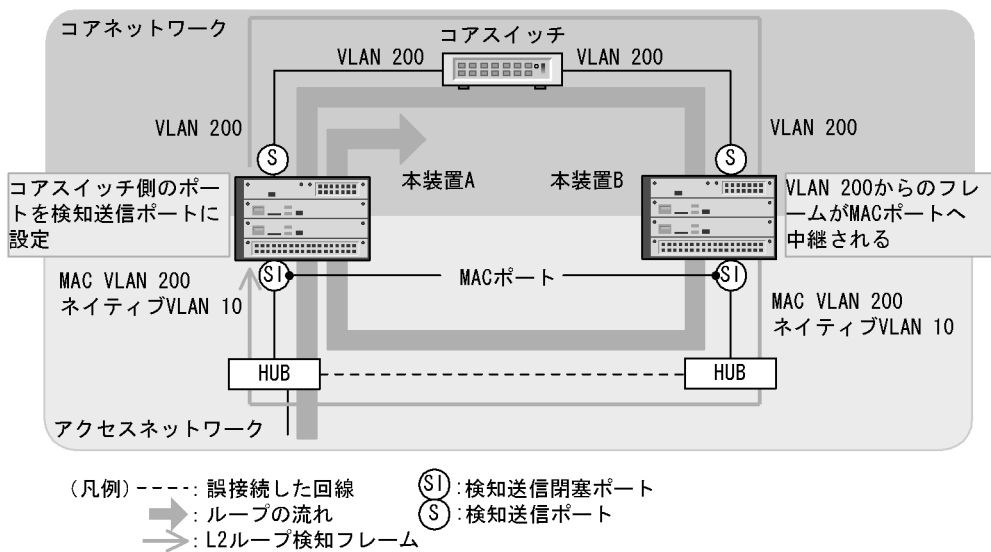
図 26-3 ループ検知の制限となる構成



(b) ループ検知可能な構成例

本装置 A のコアスイッチ側のポートを検知送信ポートに設定した場合、本装置 B はコアスイッチ側のポートから受信した L2 ループ検知フレームを MAC ポートへ中継するため、本装置 A でループ障害が検知できます。

図 26-4 ループ検知可能な構成



(5) Tag 変換使用時の動作について

本装置の Tag 変換ポートから送信した L2 ループ検知フレームを Tag 変換後の VLAN で受信した場合、ループ障害と判断します。また、他装置で Tag 変換されて本装置の別の VLAN として L2 ループ検知フレームを受信した場合もループ障害と判断します。

(6) L2 ループ検知機能の動作環境について

本機能を使用する場合に、同一ネットワーク内に L2 ループ検知未サポートの AX6700S, AX6300S 装置

(Ver.10.7 より前) を配置したとき、その装置でループ検知フレームを受信するとフレームを廃棄します。そのため、その装置を含む経路でループ障害が発生しても検知できません。

(7) inactive 状態にしたポートを自動的に active 状態にする機能 (自動復旧機能) について

スタティックリンクアグリゲーション上で自動復旧機能を使用する場合は、次の点に注意してください。

- 回線速度を変更 (ネットワーク構成の変更) する場合は、該当チャネルグループに異速度混在モードを設定してください。異速度混在モードを設定しないで回線速度を変更中にループを検知した場合、該当チャネルグループで自動復旧機能が動作しないおそれがあります。
- オートネゴシエーションで接続する場合は回線速度を指定してください。指定しないと、回線品質の劣化などによって一時的に回線速度が異なる状態になり、低速回線が該当チャネルグループから離脱することがあります。この状態でループを検知した場合、該当チャネルグループで自動復旧機能が動作しないおそれがあります。

自動復旧機能が動作しない場合は、ループ原因を解消したあと、運用コマンド `activate` でポートを active 状態にしてください。

26.2 コンフィグレーション

26.2.1 コンフィグレーションコマンド一覧

L2 ループ検知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 26-2 コンフィグレーションコマンド一覧

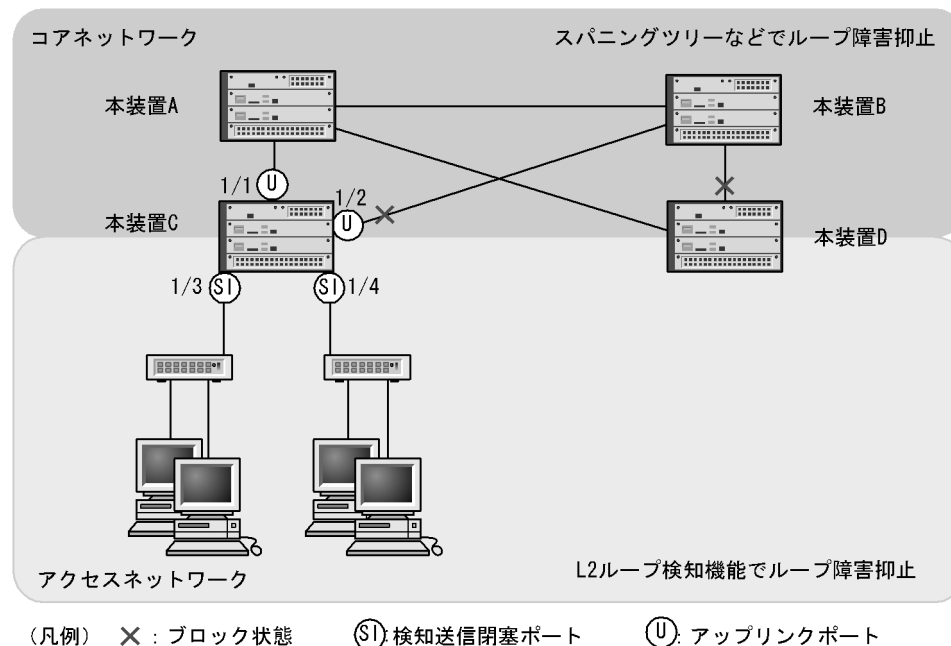
コマンド名	説明
loop-detection	L2 ループ検知機能でのポート種別を設定します。
loop-detection auto-restore-time	inactive 状態にしたポートを自動的に active 状態にするまでの時間を秒単位で指定します。
loop-detection enable	L2 ループ検知機能を有効にします。
loop-detection hold-time	inactive 状態にするまでの L2 ループ検知フレーム受信数の保持時間を秒単位で指定します。
loop-detection interval-time	L2 ループ検知フレームの送信間隔を設定します。
loop-detection threshold	ポートを inactive 状態にするまでの L2 ループ検知フレーム受信数を設定します。

26.2.2 L2 ループ検知の設定

L2 ループ検知機能を設定する手順を次に示します。ここでは、次の図に示す本装置 C の設定例を示します。

ポート 1/1 および 1/2 はコアネットワークと接続しているため、アップリンクポートを設定します。ポート 1/3 および 1/4 は下位装置と接続しているため、検知送信閉塞ポートを設定します。

図 26-5 L2 ループ検知の設定例



(1) L2 ループ検知機能の設定

[設定のポイント]

L2 ループ検知機能のコンフィギュレーションでは、装置全体で機能を有効にする設定と、実際に L2 ループ障害を検知したいポートを設定する必要があります。

[コマンドによる設定]

1. (config)# loop-detection enable id 64

本装置で L2 ループ検知機能を有効にします。

2. (config)# interface range gigabitethernet 1/1-2

```
(config-if-range)# loop-detection uplink-port
```

```
(config-if-range)# exit
```

ポート 1/1 および 1/2 をアップリンクポートに設定します。この設定によって、ポート 1/1 および 1/2 で L2 ループ検知フレームを受信した場合、送信元ポートに対して送信元のポート種別に従った動作をします。

3. (config)# interface range gigabitethernet 1/3-4

```
(config-if-range)# loop-detection send-inact-port
```

```
(config-if-range)# exit
```

ポート 1/3 および 1/4 を検知送信閉塞ポートに設定します。この設定によって、ポート 1/3 および 1/4 で L2 ループ検知フレームを送信し、また、本ポートでループ障害検知時は、本ポートを inactive 状態にします。

(2) L2 ループ検知フレームの送信間隔の設定

[設定のポイント]

L2 ループ検知フレームの最大送信レートを超えたフレームは送信しません。フレームを送信できなかったポートや VLAN では、ループ障害を検知できなくなります。L2 ループ検知フレームの最大送信レートを超える場合は、送信間隔を長く設定し最大送信レートに収まるようにする必要があります。

[コマンドによる設定]

1. (config)# loop-detection interval-time 60

L2 ループ検知フレームの送信間隔を 60 秒に設定します。

(3) inactive 状態にする条件の設定

[設定のポイント]

通常は、1 回のループ障害の検知で inactive 状態にします。この場合、初期値 (1 回) のままで運用できます。しかし、瞬間的なループで inactive 状態にしたくない場合には、inactive 状態にするまでの L2 ループ検知フレーム受信数を設定できます。

[コマンドによる設定]

1. (config)# loop-detection threshold 100

L2 ループ検知フレームを 100 回受信することで inactive 状態にするように設定します。

2. (config)# loop-detection hold-time 60

L2 ループ検知フレームを最後に受信してからの受信数を 60 秒保持するように設定します。

(4) 自動復旧時間の設定

[設定のポイント]

inactive 状態にしたポートを自動的に active 状態にしたい場合に設定します。

[コマンドによる設定]

1. (config)# loop-detection auto-restore-time 300

300 秒後に、inactive 状態にしたポートを自動的に active 状態に戻す設定をします。

26.3 オペレーション

26.3.1 運用コマンド一覧

L2 ループ検知の運用コマンド一覧を次の表に示します。

表 26-3 運用コマンド一覧

コマンド名	説明
show loop-detection	L2 ループ検知情報を表示します。
show loop-detection statistics	L2 ループ検知の統計情報を表示します。
show loop-detection logging	L2 ループ検知のログ情報を表示します。
clear loop-detection statistics	L2 ループ検知の統計情報をクリアします。
clear loop-detection logging	L2 ループ検知のログ情報をクリアします。
restart loop-detection	L2 ループ検知プログラムを再起動します。
dump protocols loop-detection	L2 ループ検知のダンプ情報をファイルへ出力します。

26.3.2 L2 ループ状態の確認

show loop-detection コマンドで L2 ループ検知の設定と運用状態を確認できます。

L2 ループ検知フレームの送信レートが最大値を超えて、フレームを送信できないポートがないかを確認できます。VLAN Port Counts の Configuration が Capacity を超えていない場合は問題ありません。

ループ障害によって inactive 状態となっているポートは Port Information の Status で確認できます。

図 26-6 L2 ループ検知の情報

```
> show loop-detection
Date 2008/04/21 12:10:10 UTC
Loop Detection ID      :64
Interval Time         :10
Output Rate           :30pps
Threshold              :1
Hold Time              :infinity
Auto Restore Time     :-
VLAN Port Counts
  Configuration       :103          Capacity      :300
Port Information
  Port  Status      Type      DetectCnt  RestoringTimer  SourcePort  Vlan
  1/1   Up             send-inact 0           -              -           -
  1/2   Down           send-inact 0           -              -           -
  1/3   Up             send      0           -              -           -
  1/4   Up             exception 0           -              -           -
  1/5   Down(loop)    send-inact 1           -              CH:32 (U)   100
CH:1   Up             trap      0           -              -           -
CH:32  Up             uplink    -           -              1/5         100
>
```


27 CFM

CFM (Connectivity Fault Management) は、レイヤ 2 レベルでのブリッジ間の接続性の検証とルート確認を行う、広域イーサネット網の保守管理機能です。

この章では、CFM の解説と操作方法について説明します。

27.1 解説

27.2 コンフィグレーション

27.3 オペレーション

27.1 解説

27.1.1 概要

イーサネットは企業内 LAN だけでなく広域網でも使われるようになってきました。これに伴い、イーサネットに SONET や ATM と同等の保守管理機能が求められています。

CFM では、次の三つの機能を使って、レイヤ 2 ネットワークの保守管理を行います。

1. Continuity Check

管理ポイント間で、情報が正しく相手に届くか（到達性・接続性）を常時監視します。

2. Loopback

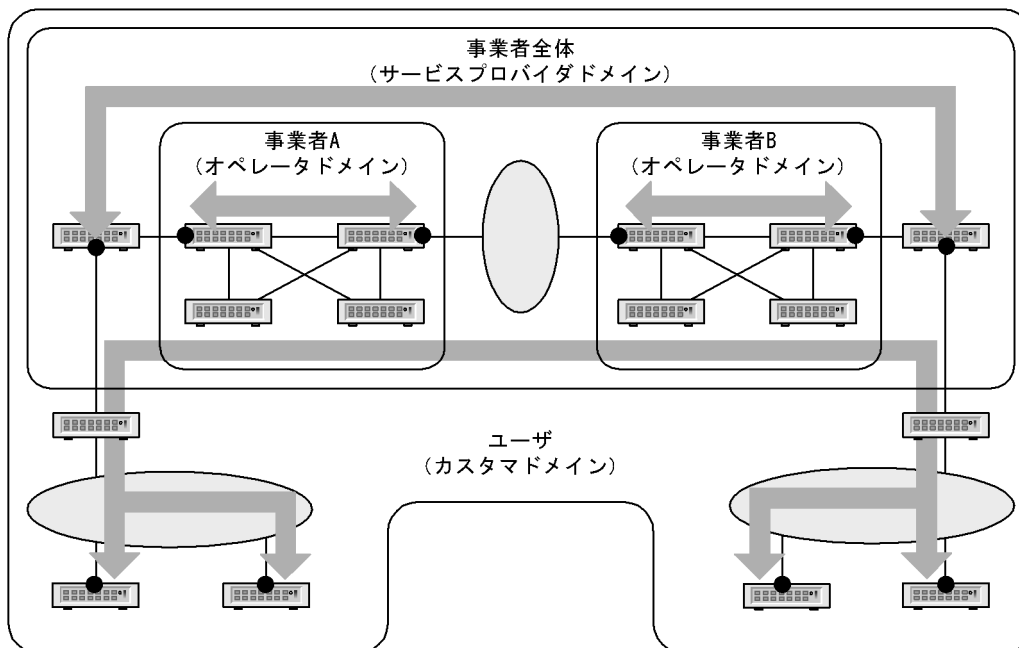
障害を検出したあと、Loopback でルート上のどこまで到達するのかを特定します（ループバック試験）。

3. Linktrace

障害を検出したあと、Linktrace で管理ポイントまでのルートを確認します（レイヤ 2 ネットワーク内のルート探索）。

CFM の構成例を次の図に示します。

図 27-1 CFM の構成例



(凡例) ● : 管理ポイント

← : 接続性の確認

(1) CFM の機能

CFM は IEEE802.1ag で規定されていて、次の表に示す機能があります。本装置は、これらの機能をサポートしています。

表 27-1 CFM の機能

名称	説明
Continuity Check (CC)	管理ポイント間の到達性の常時監視
Loopback	ループバック試験 ping 相当の機能をレイヤ 2 で実行します。
Linktrace	ルート探索 traceroute 相当の機能をレイヤ 2 で実行します。

(2) CFM の構成

CFM を構成する要素を次の表に示します。CFM はドメイン、MA、MEP および MIP から構成された保守管理範囲内で動作します。

表 27-2 CFM を構成する要素

名称	説明
ドメイン (Maintenance Domain)	CFM を適用するネットワーク上の管理用のグループのこと。
MA (Maintenance Association)	ドメインを細分化して管理する VLAN のグループのこと。
MEP (Maintenance association End Point)	管理終端ポイントのこと。 ドメインの境界上のポートで、MA 単位に設定します。 また、CFM の各機能を実行するポートです。
MIP (Maintenance domain Intermediate Point)	管理中間ポイントのこと。 ドメインの内部に位置する管理ポイントです。
MP (Maintenance Point)	管理ポイントのことで、MEP と MIP の総称です。

27.1.2 CFM の構成要素

(1) ドメイン

CFM ではドメインという単位でネットワークを階層的に管理し、ドメイン内で CFM PDU を送受信することで保守管理を行います。ドメインには 0 ~ 7 のレベル (ドメインレベル) があり、レベルの値が大きいかいほうが高いレベルとなります。

高いドメインレベルでは、低いドメインレベルの CFM PDU を廃棄します。低いドメインレベルでは、高いドメインレベルの CFM PDU を処理しないで転送します。したがって、低いドメインレベルの CFM PDU が高いドメインレベルのドメインに渡ることはなく、ドメインで独立した保守管理ができます。

ドメインレベルは区分に応じて使用するように、規格で規定されています。区分に割り当てられたドメインレベルを次の表に示します。

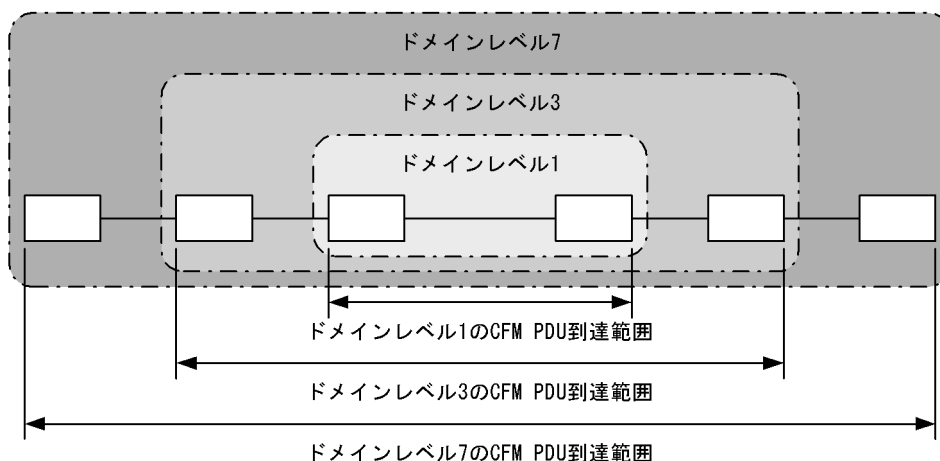
表 27-3 区分に割り当てられたドメインレベル

ドメインレベル	区分
7	カスタマ (ユーザ)
6	
5	
4	サービスプロバイダ (事業者全体)

ドメインレベル	区分
3	オペレータ（事業者）
2	
1	
0	

ドメインは階層的に設定できます。ドメインを階層構造にする場合は低いドメインレベルを内側に、高いドメインレベルを外側に設定します。階層的なドメインの構成例を次の図に示します。

図 27-2 階層的なドメインの構成例



(2) MA

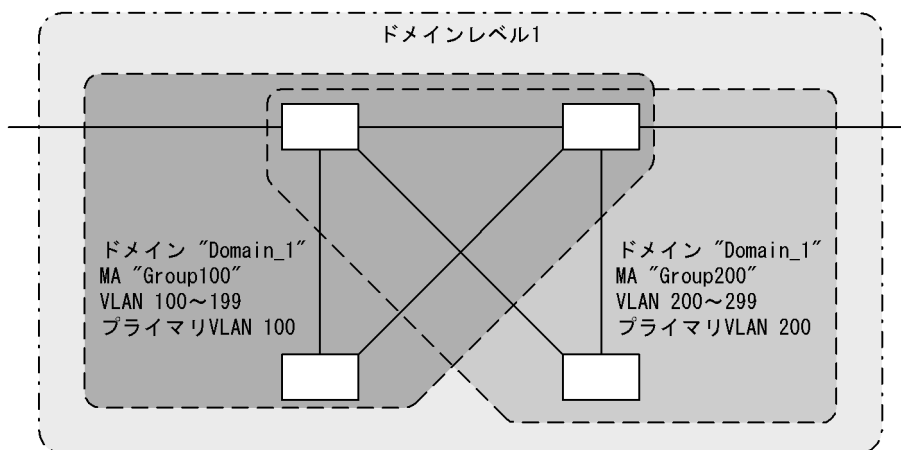
MA はドメイン内を VLAN グループで分割して管理する場合に使います。ドメインには最低一つの MA が必要です。

CFM は MA 内で動作するため、MA を設定することで管理範囲を細かく制御できます。

MA はドメイン名称および MA 名称で識別されます。そのため、同じ MA 内で運用する各装置では、設定時にドメインと MA の名称を合わせておく必要があります。

MA の管理範囲の例を次の図に示します。

図 27-3 MA の管理範囲の例



また、CFM PDU を送受信する VLAN (プライマリ VLAN) を同一 MA 内で合わせておく必要があります。

初期状態では、MA 内で VLAN ID の値がいちばん小さい VLAN がプライマリ VLAN になります。コンフィギュレーションコマンド `ma vlan-group` を使えば、任意の VLAN を明示的にプライマリ VLAN に設定できます。

プライマリ VLAN をデータ転送用の VLAN と同じ VLAN に設定することで、実際の到達性を監視できます。

(3) MEP

MEP はドメインの境界上の管理ポイントで、MA に対して設定します。MEP には MEP ID という MA 内でユニークな ID を設定して各 MEP を識別します。

CFM の機能は MEP で実行されます。CFM は MEP 間 (ドメインの境界から境界までの間) で CFM PDU を送受信することで、該当ネットワークの接続性を確認します。

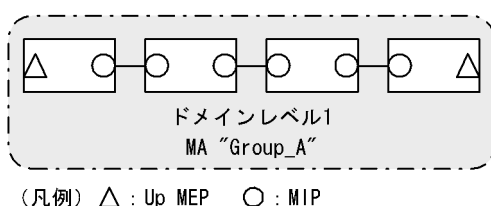
MEP には次の二つの種類があります。

Up MEP

リレー側に設定する MEP です。Up MEP 自身は CFM PDU を送受信しないで、同一 MA 内の MIP またはポートを介して送受信します。

Up MEP の設定例を次の図に示します。

図 27-4 Up MEP の設定例

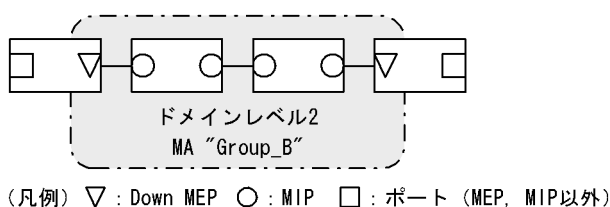


Down MEP

回線側に設定する MEP です。Down MEP 自身が CFM PDU を送受信します。

Down MEP の設定例を次の図に示します。

図 27-5 Down MEP の設定例



Down MEP, Up MEP からの送信例, および Down MEP, Up MEP での受信例を次の図に示します。

図 27-6 Down MEP , Up MEP からの送信

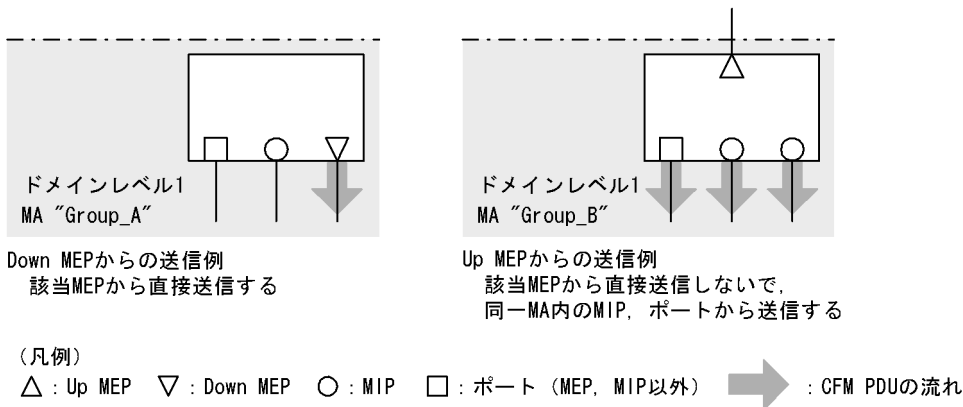
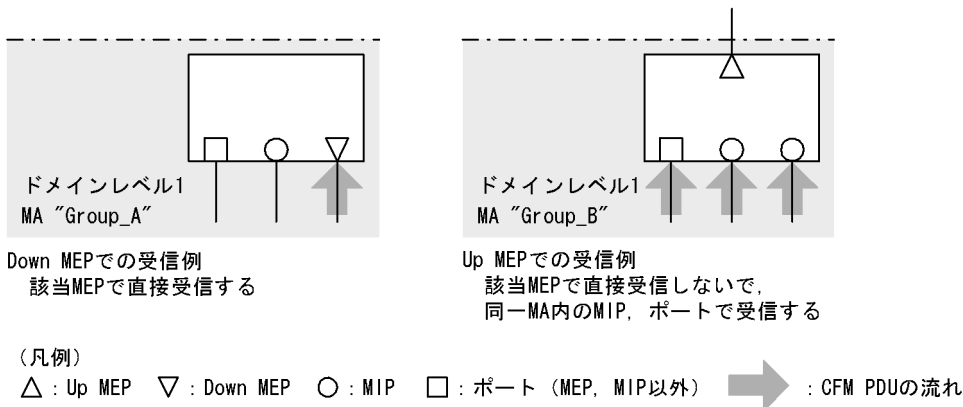
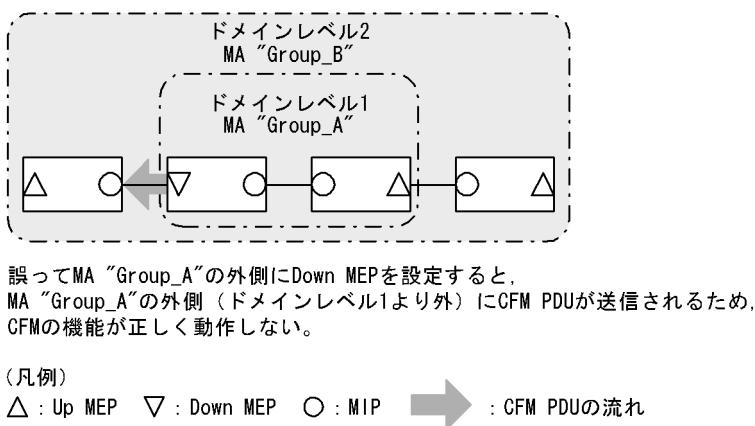


図 27-7 Down MEP , Up MEP での受信



Down MEP および Up MEP は正しい位置に設定してください。例えば、Down MEP は回線側 (MA の内側) に設定する必要があります。リレー側 (MA の外側) に対して設定した場合、CFM PDU が MA の外側に送信されるため、CFM の機能が正しく動作しません。誤って Down MEP を設定した例を次の図に示します。

図 27-8 誤って Down MEP を設定した例



(4) MIP

MIP はドメインの内部に設定する管理ポイントで、ドメインに対して設定します (同一ドメイン内の全

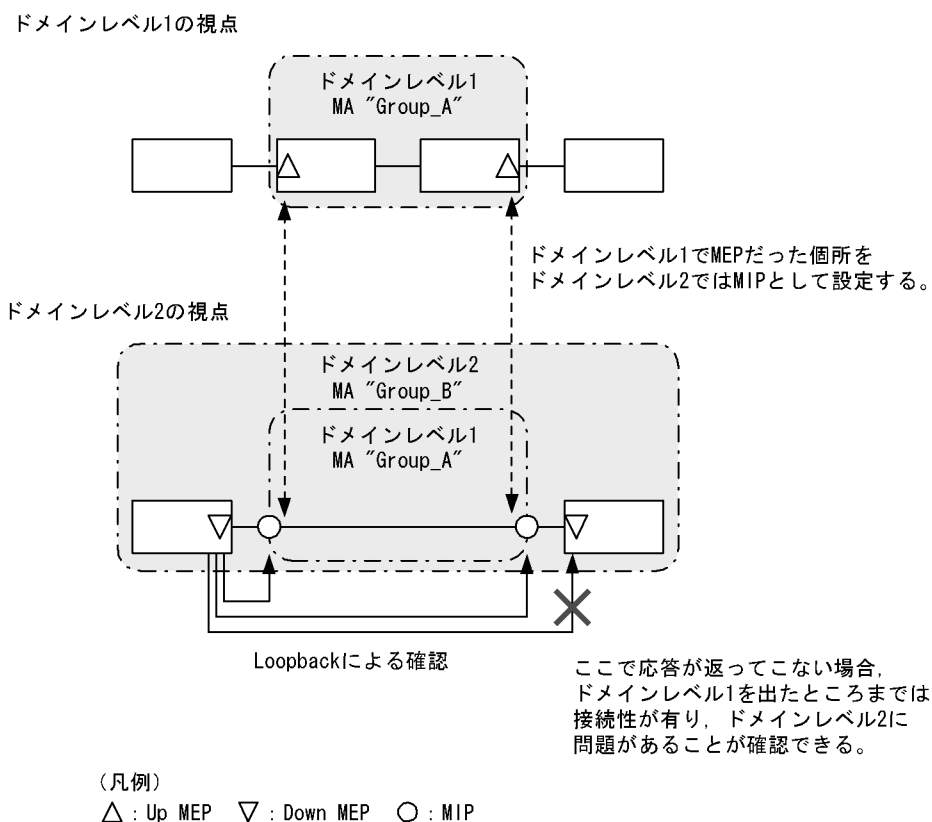
MA で共通)。階層構造の場合、MIP は高いドメインレベルのドメインが低いドメインレベルのドメインと重なる個所に設定します。また、MIP は Loopback および Linktrace に応答するので、ドメイン内の保守管理したい個所に設定します。

(a) ドメインが重なる個所に設定する場合

ドメインが重なる個所に MIP を設定すると、上位ドメインでは、低いドメインを認識しながらも、低いドメインの構成を意識しない状態で管理できます。

ドメインレベル 1 とドメインレベル 2 を使った階層構造の例を次の図に示します。

図 27-9 ドメインレベル 1 とドメインレベル 2 の階層構造の例



ドメインレベル 2 を設計する際、ドメインレベル 1 の MA で MEP に設定しているポートをドメインレベル 2 の MIP として設定します。これによって、ドメインレベル 2 ではドメインレベル 1 の範囲を認識しながらも、運用上は意識しない状態で管理できます。

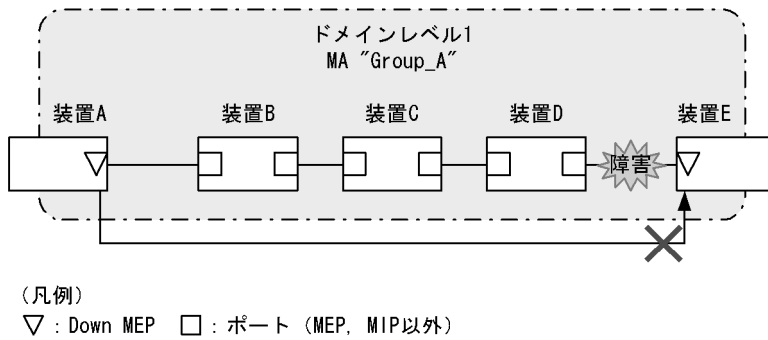
障害発生時は、ドメインレベル 2 の問題か、ドメインレベル 1 のどこかの問題かを切り分けられるため、調査範囲を特定できます。

(b) 保守管理したい個所に設定する場合

ドメイン内で細かく MIP を設定すれば、より細かな保守管理ができるようになります。

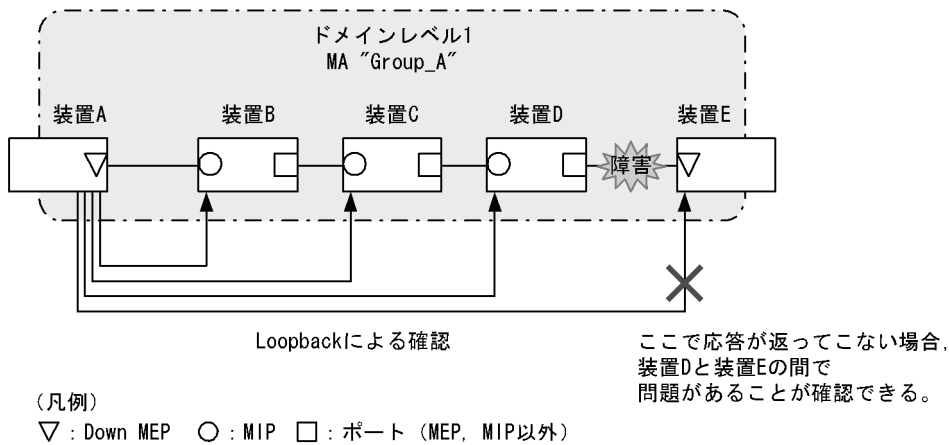
ドメイン内に MIP が設定されていない構成の例を次の図に示します。この例では、ネットワークに障害が発生した場合、装置 A、装置 E の MEP 間で通信できないことは確認できますが、どこで障害が発生したのか特定できません。

図 27-10 ドメイン内に MIP が設定されていない構成の例



ドメイン内に MIP を設定した構成の例を次の図に示します。この例では、ドメイン内に MIP を設定することで、Loopback や Linktrace の応答が各装置から返ってくるため、障害発生箇所を特定できるようになります。

図 27-11 ドメイン内に MIP を設定した構成の例



27.1.3 ドメインの設計

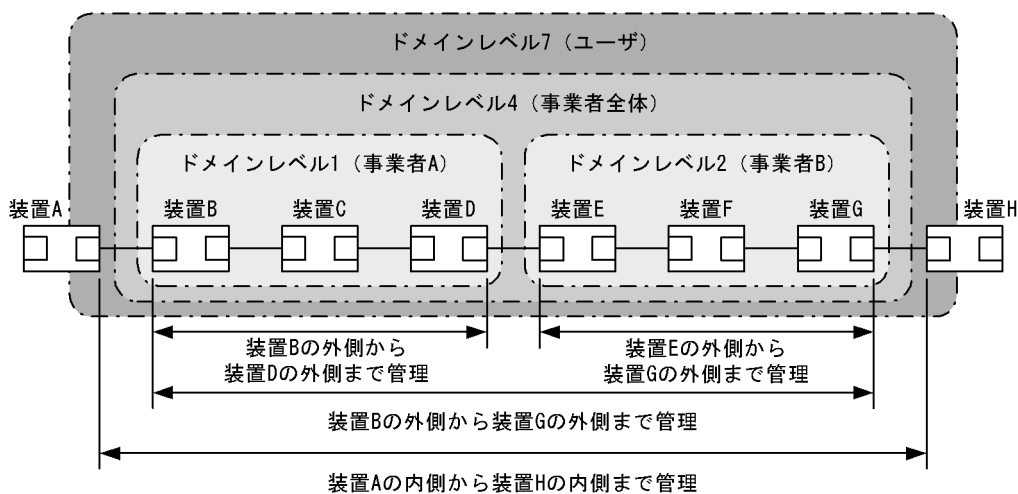
CFM を使用する際には、まずドメインを設計します。ドメインの構成と階層構造を設計し、次に個々のドメインの詳細設計をします。

ドメインの設計には、ドメインレベル、MA、MEP および MIP の設定が必要です。

(1) ドメインの構成と階層構造の設計

ドメインの境界となる MA のポートを MEP に設定し、低いドメインと重なるポートを MIP に設定します。次に示す図の構成例を基に、ドメインの構成および階層構造の設計手順を示します。

図 27-12 構成例



(凡例) □ : ポート

事業者 A, 事業者 B, 事業者全体, ユーザという単位でドメインを設計し, 区分に応じたドメインレベルを設定します。また, 次の項目を想定しています。

- 事業者 A, 事業者 B, 事業者全体は, ユーザに提供する回線が利用できることを保障するために, ユーザに提供するポートを含めた接続性を管理
- ユーザは, 事業者の提供する回線が使用できるかどうかを監視するために, 事業者から提供される回線の接続性を管理

ドメインの設計は, 次に示すように低いレベルから順に設定します。

- ドメインレベル 1, 2 の設定

1. ドメインレベル 1 で MA “Group_A” を設定します。

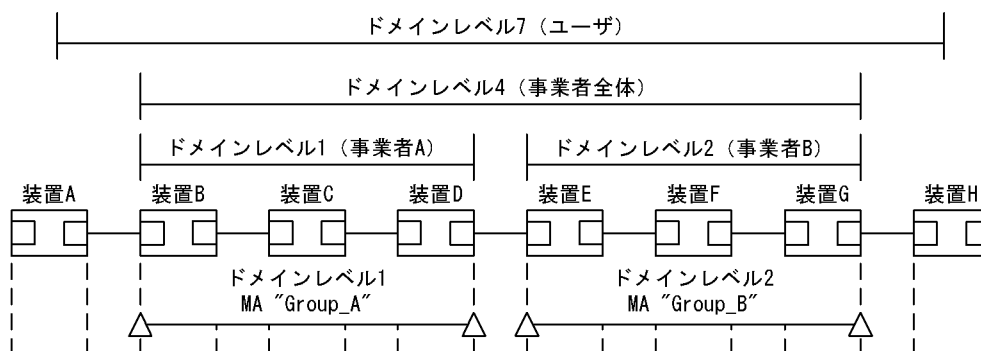
この例では, 一つのドメインを一つの MA で管理していますが, ドメイン内を VLAN グループ単位に分けて詳細に管理したい場合は, 管理する単位で MA を設定します。

2. ドメインの境界に当たる装置 B, D で, MA のポートに MEP を設定します。

事業者はユーザに提供するポートを含めた接続性を管理するため, Up MEP を設定します。

3. ドメインレベル 2 も同様に, MA を設定し, 装置 E, G に Up MEP を設定します。

図 27-13 ドメインレベル 1, 2 の設定



(凡例)

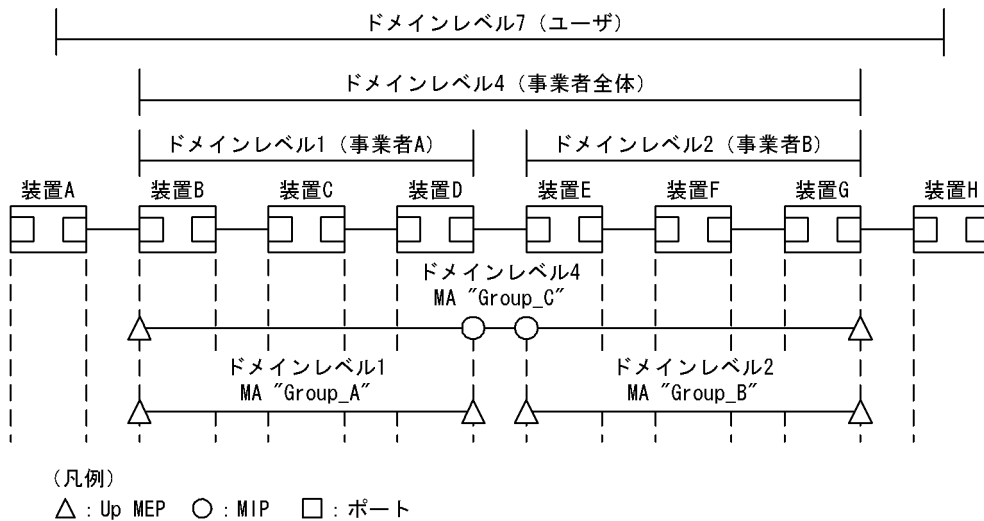
△ : Up MEP □ : ポート

- ドメインレベル4の設定

- ドメインレベル4でMA "Group_C"を設定します。
- ドメインレベル4の境界に当たる装置B, Gで, MAのポートにMEPを設定します。
事業者はユーザに提供するポートを含めた接続性を管理するため, Up MEPを設定します。
- ドメインレベル4はドメインレベル1と2を包含しているため, それぞれの中継点である装置D, EにMIPを設定します。

低いドメインのMEPを高いドメインでMIPに設定すると, LoopbackやLinktraceを使って自分で管理するドメインでの問題か, 低いレベルで管理するドメインでの問題かを切り分けられるため, 調査範囲を特定しやすくなります。

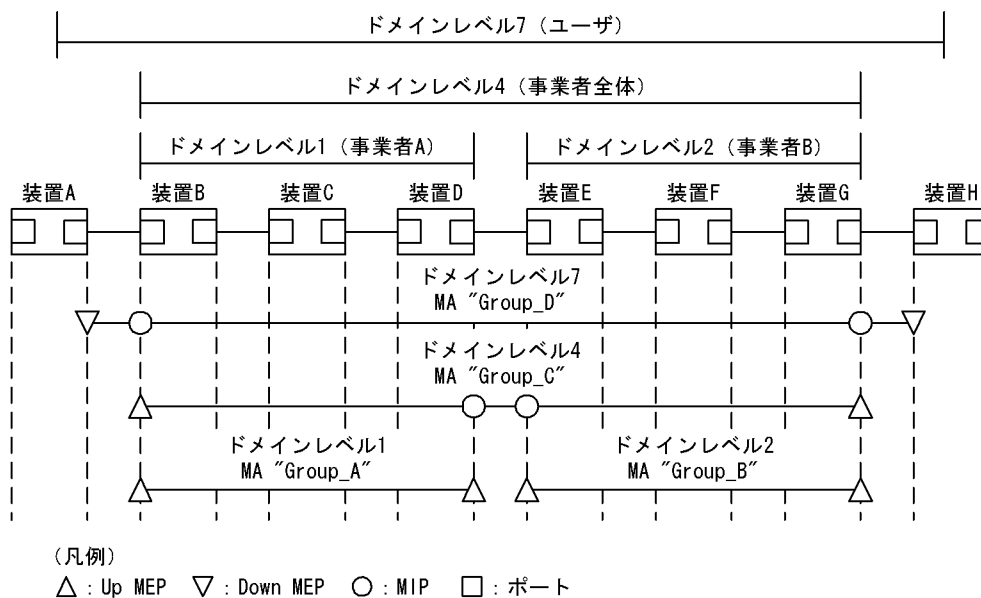
図 27-14 ドメインレベル4の設定



- ドメインレベル7の設定

- ドメインレベル7でMA "Group_D"を設定します。
- ドメインレベル7の境界に当たるA, Hで, MAのポートにMEPを設定します。
ユーザは事業者から提供される回線の接続性を管理するため, Down MEPを設定します。
- ドメインレベル7はドメインレベル4を包含しているため, 中継点である装置B, GにMIPを設定します。
ドメインレベル1と2は, ドメインレベル4の中継点として設定しているため, ドメインレベル7では設定する必要はありません。

図 27-15 ドメインレベル7の設定



(2) 個々のドメインの詳細設計

個々の詳細設計では、Loopback、Linktrace を適用したい個所に MIP を設定します。

MIP 設定前の構成および MIP 設定後の構成の例を次の図に示します。

図 27-16 MIP 設定前の構成例

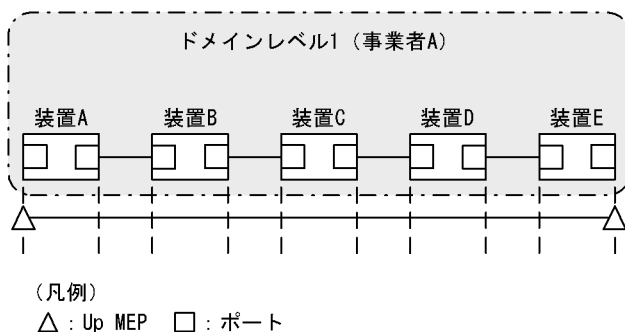
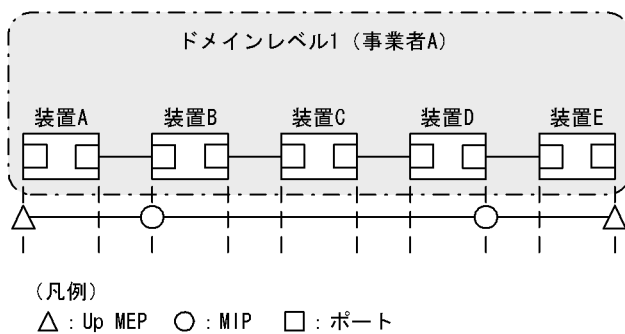


図 27-17 MIP 設定後の構成例



ドメインの内側で Loopback、Linktrace の宛先にしたいポートを MIP に設定します。この例では、装置

B, D に MIP を設定しています。この設定によって装置 B, D の MIP に対し、Loopback, Linktrace を実行できます。また、Linktrace のルート情報として応答を返すようになります。

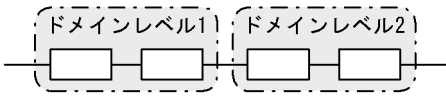
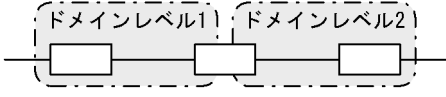
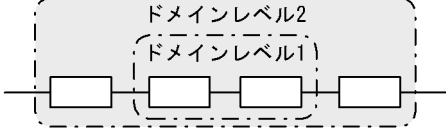
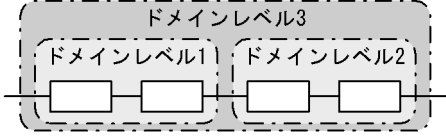
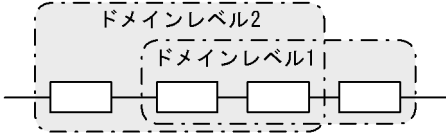
MIP を設定していない装置 C は Loopback, Linktrace の宛先として指定できません。また、Linktrace に応答しないためルート情報に装置 C の情報は含まれません。

(3) ドメインの構成例

ドメインは階層的に設定できますが、階層構造の内側が低いレベル、外側が高いレベルとなるように設定する必要があります。

ドメインの構成例と構成の可否を次の表に示します。

表 27-4 ドメインの構成例と構成の可否

構成状態	構成例	構成の可否
ドメインの隣接		可
ドメインの接触		可
ドメインのネスト		可
ドメインの隣接とネストの組み合わせ		可
ドメインの交差		不可

27.1.4 Continuity Check

Continuity Check (CC) は MEP 間の接続性を常時監視する機能です。MA 内の全 MEP が CCM (Continuity Check Message。CFM PDU の一種) を送受信し合い、MA 内の MEP を学習します。MEP の学習内容は Loopback, Linktrace でも使用します。

CC を動作させている装置で CCM を受信しなくなったり、該当装置の MA 内のポートが通信できない状態になったりした場合に、障害が発生したと見なします。この際、障害検出フラグを立てた CCM を送信し、MA 内の MEP に通知します。

CC で検出する障害を次の表に示します。検出する障害には障害レベルがあります。本装置の初期状態では、障害レベル 2 以上を検出します。

表 27-5 CC で検出する障害

障害レベル	障害内容	初期状態
5	ドメイン、MA が異なる CCM を受信した。	検出する
4	MEP ID または送信間隔が誤っている CCM を受信した。	
3	CCM を受信しなくなった。	
2	該当装置のポートが通信できない状態になった。	
1	障害検出通知の CCM を受信した。 Remote Defect Indication	検出しない

障害回復契機から障害回復監視時間が経過したあと、障害が回復したと見なします。

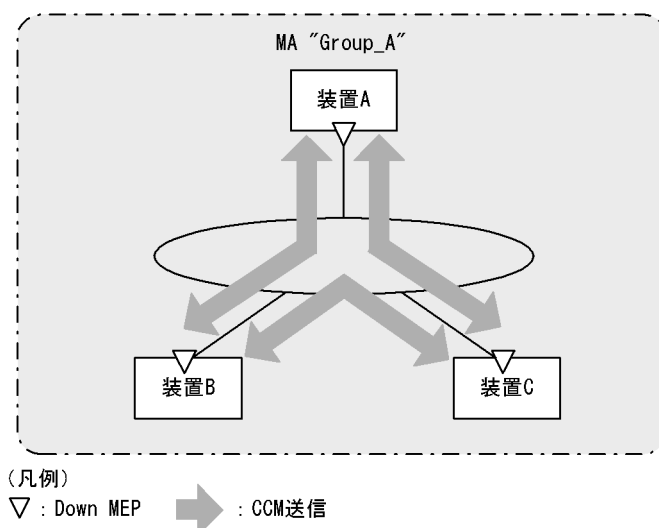
表 27-6 障害回復契機と障害回復監視時間

障害レベル	障害回復契機	障害回復監視時間
5	ドメイン、MA が異なる CCM を受信しなくなった。	受信していた CCM の送信間隔 × 3.5
4	MEP ID または送信間隔が誤っている CCM を受信しなくなった。	受信していた CCM の送信間隔 × 3.5
3	CCM を再び受信した。	受信した直後から
2	該当装置のポートが通信できる状態になった CCM を受信した。	受信した直後から
1	障害未検出の CCM を受信した。	受信した直後から

次の図の装置 B に着目して CC の動作例を示します。

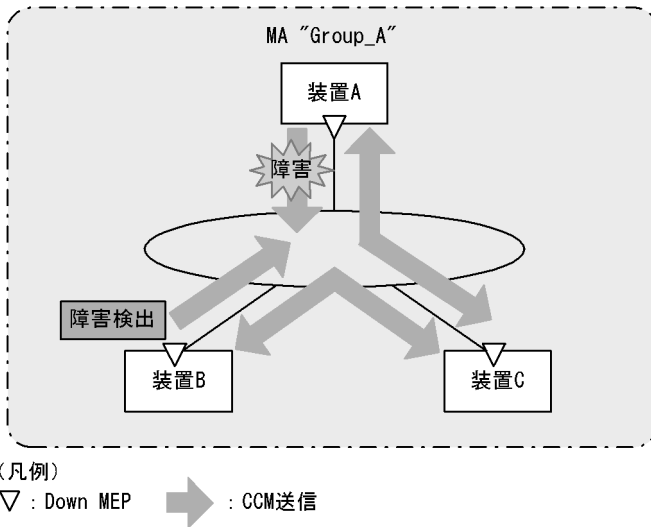
各 MEP はマルチキャストで MA 内に CCM を定期的を送信します。各 MEP の CCM を定期的受信することで常時接続性を監視します。

図 27-18 CC での常時接続性の監視



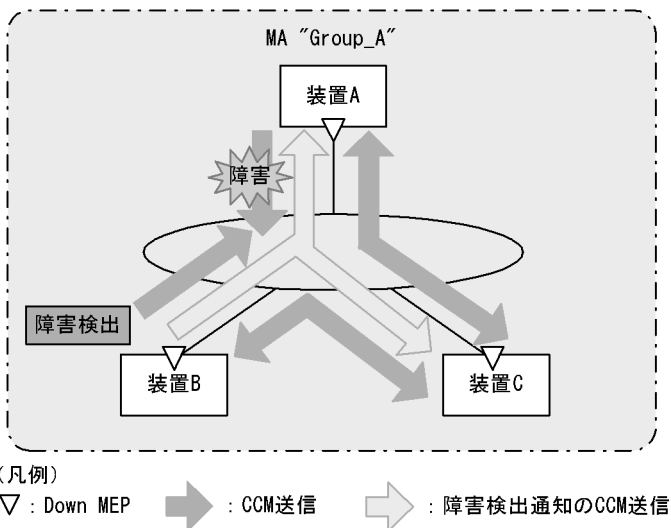
装置 A の CCM が装置の故障またはネットワーク上の障害によって、装置 B に届かなくなると、装置 B は装置 A とのネットワーク上の障害として検出します。

図 27-19 CC で障害を検出



障害を検出した装置 B は、MA 内の全 MEP に対して、障害を検出したことを通知します。

図 27-20 障害を全 MEP に通知



障害検出通知の CCM を受信した各 MEP は、MA 内のどこかで障害が発生したことを認識します。各装置で Loopback、Linktrace を実行することによって、MA 内のどのルートで障害が発生したのかを確認できます。

27.1.5 Loopback

Loopback はレイヤ 2 レベルで動作する、ping 相当の機能です。同一 MA 内の MEP-MEP 間または MEP-MIP 間の接続性を確認します。

CC が MEP-MEP 間の接続性の確認であるのに対し、Loopback では MEP-MIP 間の確認もできるため、MA 内の接続性を詳細に確認できます。

MEP から宛先ヘループバックメッセージ (CFM PDU の一種) を送信し、宛先から応答が返ってくることを確認することで接続性を確認します。

Loopback には MIP または MEP が直接応答するため、例えば、装置内に複数の MIP を設定した場合、MIP ごとに接続性を確認できます。

MIP および MEP に対する Loopback の実行例を次の図に示します。

図 27-21 MIP に対して Loopback を実行

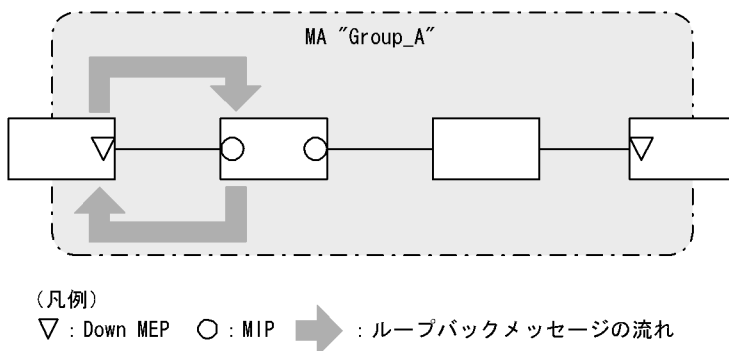
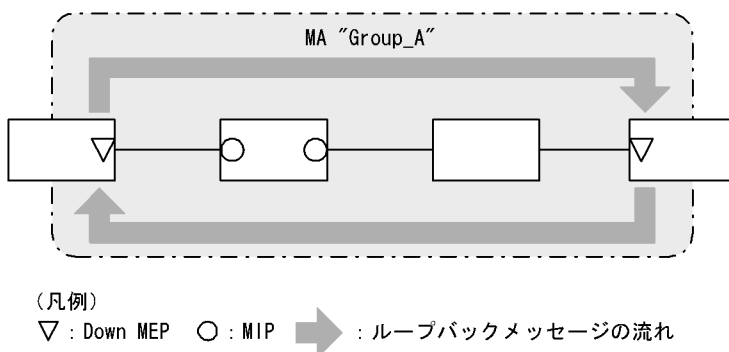


図 27-22 MEP に対して Loopback を実行



Loopback は CC の学習内容を使用するため、事前に CC を動作させておく必要があります。また、宛先に MIP を指定する場合は、事前に MIP のポートの MAC アドレスを調べておく必要があります。

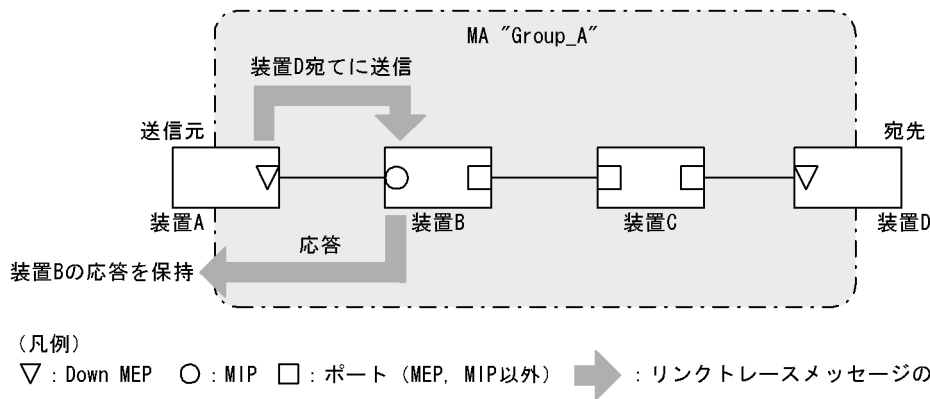
27.1.6 Linktrace

Linktrace はレイヤ 2 レベルで動作する traceroute 相当の機能です。同一 MA 内の MEP-MEP 間または MEP-MIP 間を経由する装置の情報を収集し、ルート情報を出力します。

リンクトレースメッセージ (CFM PDU の一種) を送信し、返ってきた応答をルート情報として収集します。

宛先にリンクトレースメッセージを送信した例を次の図に示します。

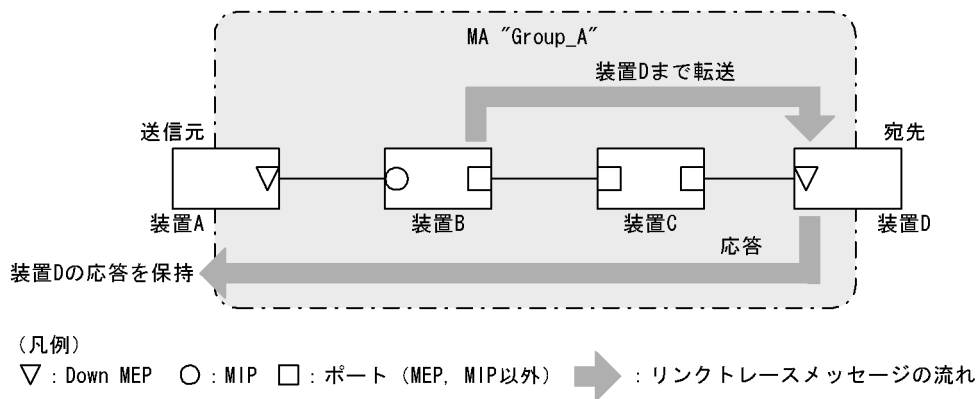
図 27-23 宛先にリンクトレースメッセージを送信



リンクトレースメッセージは宛先まで MIP を介して転送されます。MIP は転送する際に、自装置のどのポートで受信し、どのポートで転送したのかを応答します。送信元装置はルート情報として応答メッセージを保持します。

宛先にリンクトレースメッセージを転送した例を次の図に示します。

図 27-24 宛先にリンクトレースメッセージを転送



応答を返した MIP は宛先までリンクトレースメッセージを転送します。装置 C のように、MEP または MIP が設定されていない装置は応答を返しません（応答を返すには一つ以上の MIP が設定されている必要があります）。

宛先の MEP または MIP までリンクトレースメッセージが到達すると、宛先の MEP または MIP は到達したことで、どのポートで受信したのかを送信元に応答します。

送信元では、保持した応答をルート情報として出力し、宛先までのルートを確認します。

Linktrace は装置単位に応答します。例えば、装置内に設定された MIP が一つでも複数でも、どちらの場合も同じように、受信ポートと転送ポートの情報を応答します。

Linktrace は CC の学習内容を使用するため、事前に CC を動作させておく必要があります。また、宛先に MIP を指定する場合は、事前に MIP のポートの MAC アドレスを調べておく必要があります。

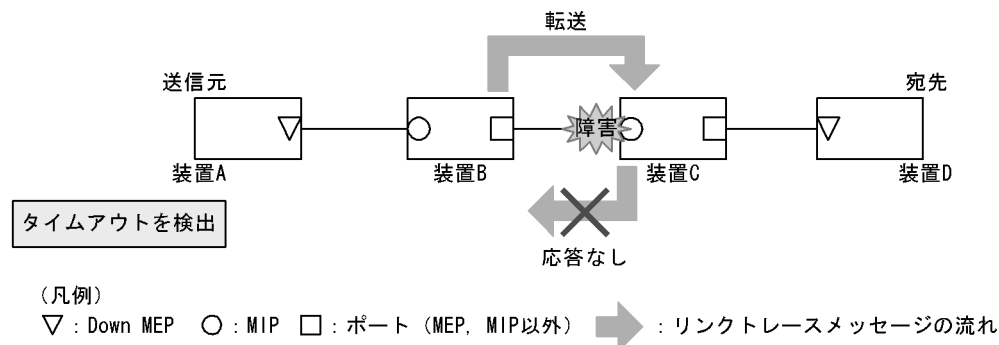
(a) Linktrace による障害の切り分け

Linktrace の実行結果によって、障害が発生した装置やポートなどを絞り込みます。

- タイムアウトを検出した場合

Linktrace でタイムアウトを検出した例を次の図に示します。

図 27-25 Linktrace でタイムアウトを検出した例

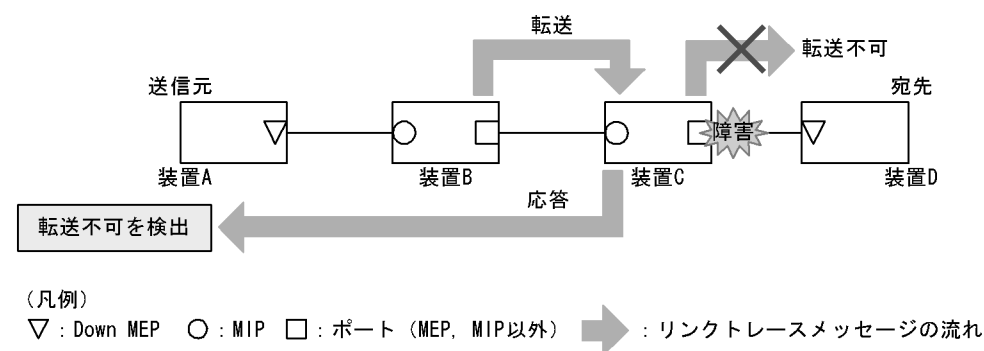


この例では、装置 A が Linktrace でタイムアウトを検出した場合、ネットワーク上の受信側のポートが通信できない状態が考えられます。リンクトレースメッセージが装置 B から装置 C に転送されていますが、装置 C が通信できない状態になっていて、応答を返さないため、タイムアウトになります。

- 転送不可を検出した場合

Linktrace で通信不可を検出した例を次の図に示します。

図 27-26 Linktrace で通信不可を検出した例



装置 A が Linktrace での転送不可を検出した場合、ネットワーク上の送信側のポートが通信できない状態が考えられます。これは、装置 C が装置 D (宛先) にリンクトレースメッセージを転送できなかった場合、装置 A に送信側ポートが通信できない旨の応答を返すためです。

(b) Linktrace の応答について

リンクトレースメッセージはマルチキャストフレームです。

CFM が動作している装置でリンクトレースメッセージを転送する際には、MIP CCM データベースと MAC アドレステーブルを参照して、どのポートで転送するか決定します。

CFM が動作していない装置ではリンクトレースメッセージをフラッディングします。このため、CFM が動作していない装置がネットワーク上にある場合、宛先のルート以外の装置からも応答が返ります。

27.1.7 共通動作仕様

(1) ブロック状態のポートでの動作

CFM の各機能について、ブロック状態のポートでの動作を次の表に示します。

表 27-7 Up MEP がブロック状態の場合

機能	動作
CC	<ul style="list-style-type: none"> • CCM を送受信する。送信する CCM のポート状態には Blocked を設定する
Loopback	<ul style="list-style-type: none"> • 運用コマンド l2ping は実行できない • 自宛のループバックメッセージに回答する
Linktrace	<ul style="list-style-type: none"> • 運用コマンド l2traceroute は実行できない • リンクトレースメッセージに回答する。回答するリンクトレースメッセージの Egress Port の状態には Blocked を設定する

表 27-8 Down MEP がブロック状態の場合

機能	動作
CC	<ul style="list-style-type: none"> • CCM を送受信しない
Loopback	<ul style="list-style-type: none"> • 運用コマンド l2ping は実行できない • 自宛のループバックメッセージに回答しない
Linktrace	<ul style="list-style-type: none"> • 運用コマンド l2traceroute は実行できない • リンクトレースメッセージに回答しない

表 27-9 MIP がブロック状態の場合

機能	動作
CC	<ul style="list-style-type: none"> • CCM を透過しない
Loopback	<ul style="list-style-type: none"> • 回線側から受信した自宛のループバックメッセージに回答しない • リレー側から受信した自宛のループバックメッセージに回答する • ループバックメッセージを透過しない
Linktrace	<ul style="list-style-type: none"> • 回線側から受信したリンクトレースメッセージに回答しない • リレー側から受信したリンクトレースメッセージに回答する。回答するリンクトレースメッセージの Egress Port の状態には Blocked を設定する • リンクトレースメッセージを透過しない

表 27-10 MEP, MIP 以外のポートがブロック状態の場合

機能	動作
CC	<ul style="list-style-type: none"> • CCM を透過しない
Loopback	<ul style="list-style-type: none"> • ループバックメッセージを透過しない
Linktrace	<ul style="list-style-type: none"> • リンクトレースメッセージを透過しない

(2) VLAN トンネル構成での設定について

VLAN トンネリング網で CFM を使用する場合、VLAN トンネリング網内と VLAN トンネリング網外でドメインを分け、それぞれで管理します。なお、ドメインの設定個所によっては、CFM の機能の使用に一部制限があります。ドメインの設定個所別の機能の使用制限について次の表に示します。

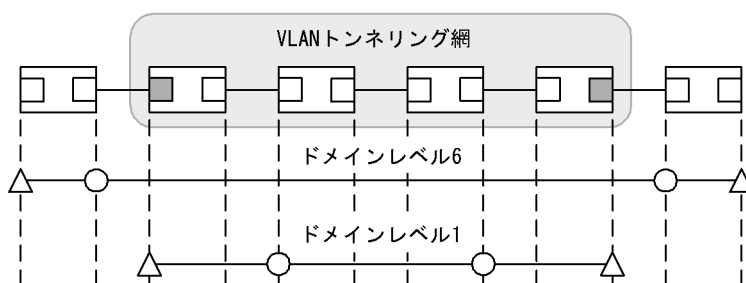
表 27-11 ドメインの設定個所別の機能の使用制限

ドメインの設定個所	機能		
	CC	Loopback	Linktrace
VLAN トネリング網内と VLAN トネリング網外	使用可	使用可	<ul style="list-style-type: none"> VLAN トネリング網内は使用可 VLAN トネリング網外は VLAN トネリング網外を越える場合は使用不可
VLAN トネリング網内だけ	使用可	使用可	使用可
VLAN トネリング網外だけ	使用可	使用可	使用可

(a) VLAN トネリング網内と VLAN トネリング網外で CFM を使用する場合

VLAN トネリング網内と VLAN トネリング網外で CFM を使用する例を次の図に示します。

図 27-27 VLAN トネリング網内と VLAN トネリング網外で CFM を使用する例



(凡例)

△ : Up MEP ○ : MIP ■ : VLAN トネリング設定ポート □ : ポート

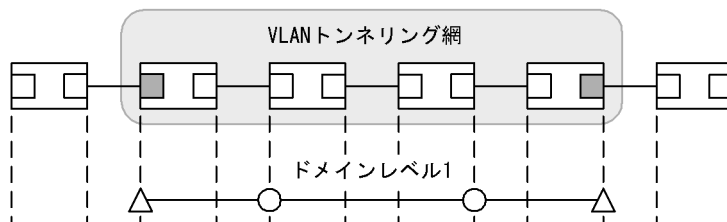
VLAN トネリング網内のドメインレベル 1 は、VLAN トネリング網内で任意の個所に管理ポイントを設定できます。VLAN トネリング網外のドメインレベル 6 は、VLAN トネリング網外の装置だけに管理ポイントを設定できます。VLAN トネリング網内にはドメインレベル 6 の管理ポイントは設定できません。VLAN トネリング網内の管理はドメインレベル 1 でします。

また、VLAN トネリング網外のドメインレベル 6 では VLAN トネリング網外を越えては Linktrace を使用できません。

(b) VLAN トネリング網内だけで CFM を使用する場合

VLAN トネリング網内だけで CFM を使用する例を次の図に示します。

図 27-28 VLAN トネリング網内だけで CFM を使用する例



(凡例)

△ : Up MEP ○ : MIP ■ : VLAN トネリング設定ポート □ : ポート

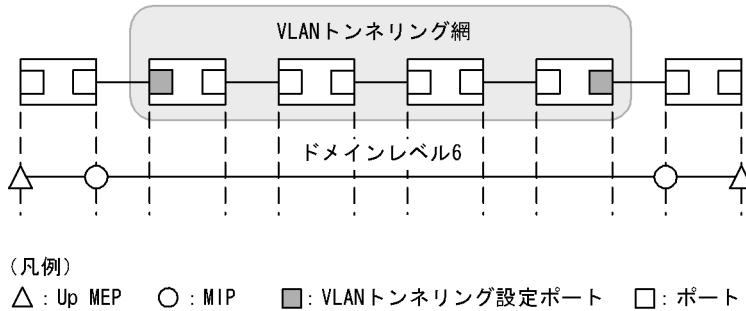
VLAN トネリング網内のドメインレベル 1 は、VLAN トネリング網内で任意の個所に管理ポイントを設定

設定できます。該当ドメインでは CFM の各機能が使用できます。

(c) VLAN トネリング網外だけで CFM を使用する場合

VLAN トネリング網外だけで CFM を使用する例を次の図に示します。

図 27-29 VLAN トネリング網外だけで CFM を使用する例



VLAN トネリング網外のドメインレベル6は、VLAN トネリング網外の装置だけに管理ポイントを設定できます。VLAN トネリング網内にはドメインレベル6の管理ポイントは設定できません。該当ドメインでは CFM の各機能が使用できます。

27.1.8 CFM で使用するデータベース

CFM で使用するデータベースを次の表に示します。

表 27-12 CFM で使用するデータベース

データベース	内容	内容確認コマンド
MEP CCM データベース	各 MEP が保持しているデータベース。同一 MA 内の MEP の情報。CC で常時接続性の監視をする際に使用。保持する内容は次のとおりです。 <ul style="list-style-type: none"> MEP ID MEP ID に対応する MAC アドレス 該当 MEP で発生した障害情報 	show cfm remote-mep
MIP CCM データベース	装置で保持しているデータベース。同一ドメイン内の MEP の情報。リンクトレースメッセージを転送する際、どのポートで転送するかを決定する際に使用。保持する内容は次のとおりです。 <ul style="list-style-type: none"> MEP の MAC アドレス 該当 MEP の CCM を受信した VLAN とポート 	なし
リンクトレースデータベース	Linktrace の実行結果を保持しているデータベース。保持する内容は次のとおりです。 <ul style="list-style-type: none"> Linktrace を実行した MEP と宛先 TTL 応答を返した装置の情報 リンクトレースメッセージを受信したポートの情報 リンクトレースメッセージを転送したポートの情報 	show cfm l2traceroute-db

(1) MEP CCM データベース

MEP CCM データベースは、同一 MA 内にどのような MEP があるかを保持しています。また、該当する MEP で発生した障害情報も保持しています。

Loopback, Linktrace では宛先を MEP ID で指定できますが、MEP CCM データベースに登録されていない MEP ID は指定できません。MEP ID がデータベース内に登録されているかどうかは運用コマンド `show cfm remote-mep` で確認できます。

本データベースのエントリは CC 実行時に MEP が CCM を受信したときに作成します。

(2) MIP CCM データベース

MIP CCM データベースは、リンクトレースメッセージを転送する際にどのポートから転送すればよいかを決定する際に使用します。

転送時、MIP CCM データベースに宛先 MEP の MAC アドレスが登録されていない場合は、MAC アドレステーブルを参照して転送するポートを決定します。

MAC アドレステーブルにもない場合はリンクトレースメッセージは転送しないで、転送できなかった旨の応答を転送元に返します。

本データベースのエントリは CC 実行時に MIP が CCM を転送したときに作成します。

(3) リンクトレースデータベース

リンクトレースデータベースは、Linktrace の実行結果を保持しています。

運用コマンド `show cfm l2traceroute-db` で、過去に実行した Linktrace の結果を参照できます。

(a) 保持できるルート数について

装置全体で 1024 装置分の応答を保持します。

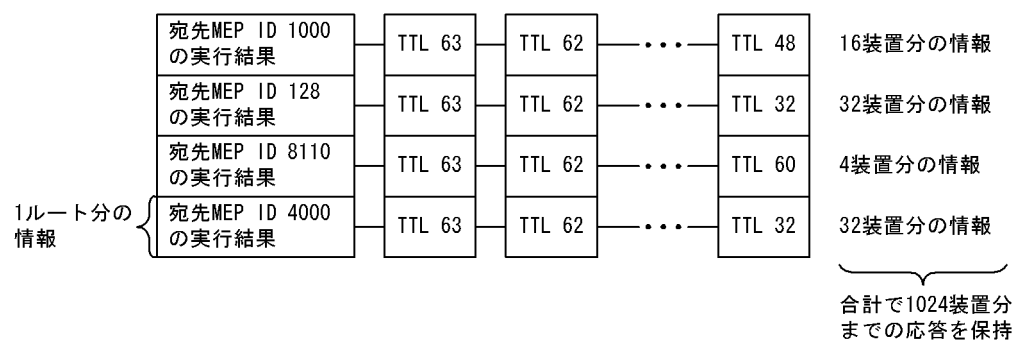
1 ルート当たり何装置分の応答を保持するかで何ルート分保持できるかが決ります。1 ルート当たり 256 装置分の応答を保持した場合は 4 ルート、1 ルート当たり 16 装置分の応答を保持している場合は 64 ルート保持できます。

応答が 1024 装置分を超えた場合、古いルートの情報が消去され、新しいルートの情報を保持します。

リンクトレースデータベースに登録されている宛先に対して Linktrace を実行した場合、リンクトレースデータベース上から該当宛先までのルート情報を削除したあとに新しい Linktrace の応答を保持します。

リンクトレースデータベースを次の図に示します。

図 27-30 リンクトレースデータベース



本データベースのエントリは Linktrace 実行時に MEP が応答を受信したときに作成します。

27.1.9 CFM 使用時の注意事項

(1) CFM を動作させない装置について

CFM を適用する際、ドメイン内の全装置で CFM を動作させる必要はありませんが、CFM を動作させない装置では CFM PDU を透過させる必要があります。

本装置を除き、CFM を動作させない装置は、次の表に示すフレームを透過するように設定してください。

表 27-13 透過させるフレーム

フレーム種別	宛先 MAC アドレス
マルチキャスト	0180.c200.0030 ~ 0180.c200.003f

本装置は、CFM が動作していない場合はすべての CFM PDU を透過します。

(2) 他機能との共存について

次に示すポートでは同時に使用できません。

- レイヤ 2 認証設定ポート

(3) CFM PDU のバースト受信について

CC で常時監視するリモート MEP 数が 1024 以上あると、リモート MEP からの CFM PDU 送信タイミングが偶然一致した場合に、本装置で CFM PDU をバースト受信することがあります。その場合、本装置で CFM PDU を廃棄することがあり、障害を誤検出するおそれがあります。

本現象が頻発する場合は、各装置での CFM PDU の送信タイミングが重ならないように調整してください。

(4) 同ドメインで同一プライマリ VLAN を設定している MA での MEP 設定について

同ドメインで同一プライマリ VLAN を設定している MA (同一 MA も含む) で、同一ポートに対して 2 個以上の MEP を設定できません。設定した場合は、該当する MEP で CFM が正常に動作しません。

(5) Linktrace でのルート情報の収集について

Linktrace ではリンクトレースメッセージの転送先ポートは、MIP CCM データベースまたは MAC アドレステーブルを参照して決定します。そのため、リンクアップ時 (リンクダウン後の再アップ含む) やスパニングツリーなどによる経路変更後は、CC で CCM を送受信するまで転送先ポートが決定できないため、正しいルート情報の収集ができません。

(6) Up MEP および MIP で CFM が動作しないタイミング

次のイベント発生後に、一度もリンクアップしていない Up MEP および MIP のポートでは CFM の各機能が動作しません。一度リンクアップさせることで動作します。

- 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 (BCU, CSU, MSU)
- 1 枚目の BSU アップ
- 運用コマンド `restart vlan` の実行
- 運用コマンド `restart cfm` の実行

(7) ブロック状態のポートで MIP が Loopback , Linktrace に応答しない場合について

ブロック状態のポートに MIP を設定し、該当ポートで次に示す運用をした場合、MIP は Loopback , Linktrace に応答しないことがあります。

- スパニングツリー (PVST+, シングル) でループガード機能を運用
- スパニングツリー (MSTP) の運用時に、アクセス VLAN またはネイティブ VLAN をプライマリ VLAN として設定
- LLDP を運用
- OADP を運用

(8) 冗長構成での CC の動作について

スパニングツリーなどの冗長構成を組んだネットワーク上で CC を運用している場合、通信経路の切り替えが発生したときに、まれに自装置の MEP が送信した CCM を受信して ErrorCCM を検出することがあります。本障害は通信経路が安定すると回復します。

(9) 二重化構成で CFM を使用する場合について

系切替時、CFM の各情報は引き継ぎません。系切替で待機系から運用系に変わった際には次の表に示す情報を初期化します。

表 27-14 系切替で運用系に変わったときに初期化される CFM の情報

系切替時に初期化する情報	初期化による影響
MEP CCM データベース	運用コマンド <code>show cfm remote-mep</code> で系切替前のリモート MEP 情報が見れない。
MIP CCM データベース	CC を実行するまで、Linktrace , Loopback の宛先に MEP ID を使用できない。
Linktrace データベース	運用コマンド <code>l2tracert</code> を実行するまで、運用コマンド <code>show cfm l2tracert-db</code> でルート情報が見れない。
障害情報	運用コマンド <code>show cfm fault</code> で系切替前の障害が見れない。
統計情報	運用コマンド <code>show cfm statistics</code> で系切替前の統計情報が見れない。

27.2 コンフィグレーション

27.2.1 コンフィグレーションコマンド一覧

CFM 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。

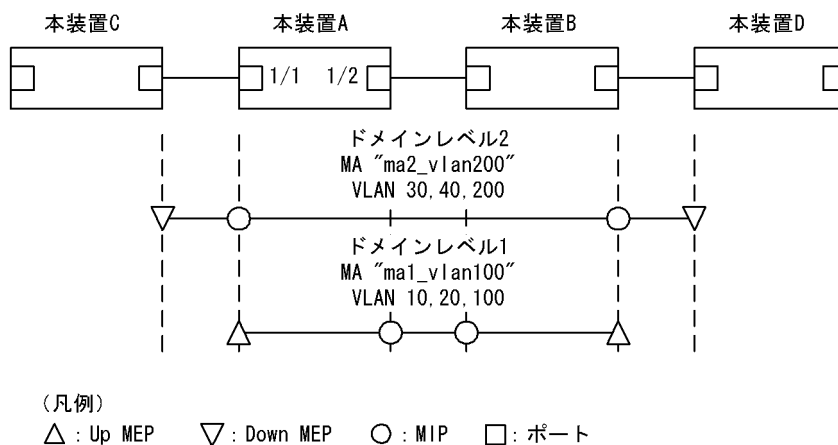
表 27-15 コンフィグレーションコマンド一覧

コマンド名	説明
domain name	該当ドメインで使用する名称を設定します。
ethernet cfm cc alarm-priority	CC で検知する障害レベルを設定します。
ethernet cfm cc alarm-reset-time	CC で障害を再検知と見なすまでの時間を設定します。
ethernet cfm cc alarm-start-time	CC で障害を検知してからトラップを通知するまでの時間を設定します。
ethernet cfm cc enable	ドメインで CC を使用する MA を設定します。
ethernet cfm cc interval	CCM の送信間隔を設定します。
ethernet cfm domain	ドメインを設定します。
ethernet cfm enable (global)	CFM を開始します。
ethernet cfm enable (interface)	no ethernet cfm enable 設定時に CFM を停止します。
ethernet cfm mep	CFM で使用する MEP を設定します。
ethernet cfm mip	CFM で使用する MIP を設定します。
ma name	該当ドメインで使用する MA の名称を設定します。
ma vlan-group	該当ドメインで使用する MA に所属する VLAN を設定します。

27.2.2 CFM の設定 (複数ドメイン)

複数ドメインを設定する手順を説明します。ここでは、次の図に示す本装置 A の設定例を示します。

図 27-31 CFM の設定例 (複数ドメイン)



(1) 複数ドメインおよびドメインごとの MA の設定

[設定のポイント]

複数のドメインがある場合、低いドメインレベルのドメインから設定します。MA の設定はドメイン

レベルと MA 識別番号，ドメイン名称，および MA 名称を対向装置と一致させる必要があります。設定が異なる場合，本装置と対向装置は同一 MA と判断されません。

MA のプライマリ VLAN には，本装置の MEP から CFM PDU を送信する VLAN を設定します。

primary-vlan パラメータが設定されていない場合は，vlan-group パラメータで設定された VLAN の中から，最も小さな VLAN ID を持つ VLAN がプライマリ VLAN になります。

[コマンドによる設定]

1. (config)# ethernet cfm domain level 1 direction-up
(config-ether-cfm)# domain name str operator_1
ドメインレベル 1 と MEP の初期状態を Up MEP にすることを設定します。コンフィグレーションイーサネット CFM モードに移行し，ドメイン名称を設定します。
2. (config-ether-cfm)# ma 1 name str ma1_vlan100
(config-ether-cfm)# ma 1 vlan-group 10,20,100 primary-vlan 100
(config-ether-cfm)# exit
MA1 で MA 名称，MA に所属する VLAN，プライマリ VLAN を設定します。
3. (config)# ethernet cfm domain level 2
(config-ether-cfm)# domain name str operator_2
(config-ether-cfm)# ma 2 name str ma2_vlan200
(config-ether-cfm)# ma 2 vlan-group 30,40,200 primary-vlan 200
(config-ether-cfm)# exit
ドメインレベル 2 と MEP の初期状態を Down MEP にすることを設定します。
MA2 で MA 名称，MA に所属する VLAN，プライマリ VLAN を設定します。

(2) MEP および MIP の設定

[設定のポイント]

MEP および MIP の設定数は，収容条件数以内に収まるように設定してください。

設定した MEP および MIP の運用を開始するには，装置の CFM を有効にする設定が必要になります。

[コマンドによる設定]

1. (config)# interface gigabitethernet 1/1
(config-if)# ethernet cfm mep level 1 ma 1 mep-id 101
(config-if)# ethernet cfm mip level 2
(config-if)# exit
(config)# interface gigabitethernet 1/2
(config-if)# ethernet cfm mip level 1
(config-if)# exit
ポート 1/1 に，ドメインレベル 1，MA1 に所属する MEP を設定します。また，ドメインレベル 2 の MIP を設定します。ポート 1/2 にドメインレベル 1 の MIP を設定します。
2. (config)# ethernet cfm enable
本装置の CFM の運用を開始します。

(3) ポートの CFM の停止

[設定のポイント]

一時的にポートの CFM を停止したい場合に設定します。

[コマンドによる設定]

1. (config)# interface gigabitethernet 1/1
(config-if)# no ethernet cfm enable
(config-if)# exit
ポート 1/1 の CFM を停止します。

(4) CC の設定

[設定のポイント]

ethernet cfm cc enable コマンドの設定直後から、CC が動作します。

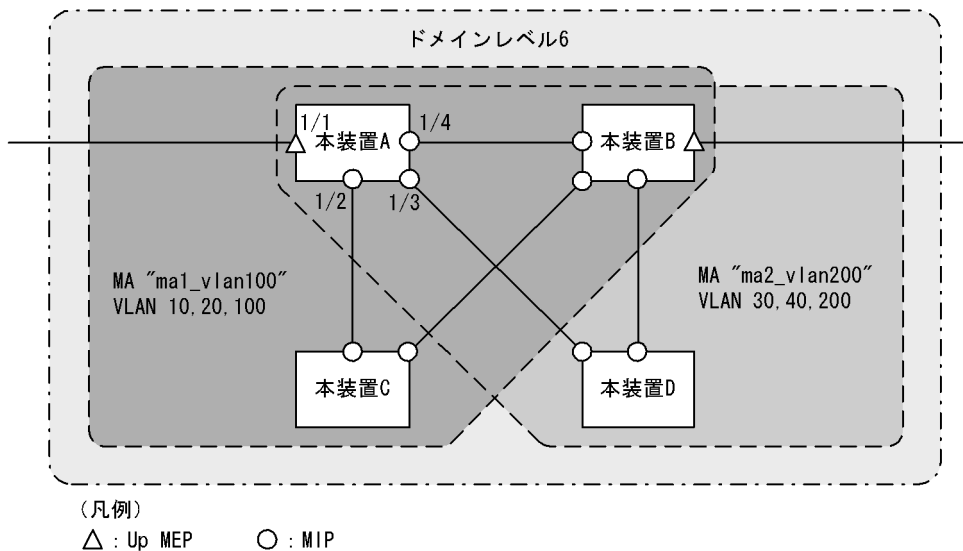
[コマンドによる設定]

1. (config)# ethernet cfm cc level 1 ma 1 interval 10s
(config)# ethernet cfm cc level 1 ma 1 enable
ドメインレベル 1, MA1 で、CCM の送信間隔を 10 秒に設定したあとに CC の動作を開始します。

27.2.3 CFM の設定 (同一ドメイン, 複数 MA)

同一ドメインで複数の MA を設定する手順を説明します。ここでは、次の図に示す本装置 A の設定例を示します。

図 27-32 CFM の設定例 (同一ドメイン, 複数 MA)



(1) 同一ドメインでの複数 MA の設定

[設定のポイント]

同一ドメインで複数の MA を設定する場合は、MA 識別番号および MA 名称が重複しないように設定します。ドメインおよび MA の基本的な設定のポイントは、「27.2.2 CFM の設定 (複数ドメイン)」

を参照してください。

[コマンドによる設定]

1. (config)# ethernet cfm domain level 6 direction-up
 (config-ether-cfm)# domain name str customer_6
 ドメインレベルと MEP の初期状態を Up MEP にすることを設定します。コンフィグレーションインターサネット CFM モードに移行し、ドメイン名称を設定します。

2. (config-ether-cfm)# ma 1 name str ma1_vlan100
 (config-ether-cfm)# ma 1 vlan-group 10,20,100 primary-vlan 100
 (config-ether-cfm)# ma 2 name str ma2_vlan200
 (config-ether-cfm)# ma 2 vlan-group 30,40,200 primary-vlan 200
 (config-ether-cfm)# exit
 MA 識別番号と MA 名称、MA に所属する VLAN、プライマリ VLAN を設定します。

(2) MEP および MIP の設定

[設定のポイント]

MEP は MA ごとに設定する必要があります。MIP は複数の MA で共通で、ポート単位に一つ設定します。MEP および MIP の基本的な設定のポイントは、「27.2.2 CFM の設定 (複数ドメイン)」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)# ethernet cfm mep level 6 ma 1 mep-id 101
 (config-if)# ethernet cfm mep level 6 ma 2 mep-id 201
 (config-if)# exit
 (config)# interface range gigabitethernet 1/2-4
 (config-if-range)# ethernet cfm mip level 6
 (config-if-range)# exit
 ポート 1/1 に、ドメインレベル 6、MA1 に所属する MEP を設定します。また、MA2 に所属する MEP を設定します。ポート 1/2 ~ 1/4 にドメインレベル 6 の MIP を設定します。

2. (config)# ethernet cfm enable
 本装置の CFM の運用を開始します。

27.3 オペレーション

27.3.1 運用コマンド一覧

CFM の運用コマンド一覧を次の表に示します。

表 27-16 運用コマンド一覧

コマンド名	説明
l2ping	CFM の Loopback 機能を実行します。指定 MP 間の接続を確認します。
l2traceroute	CFM の Linktrace 機能を実行します。指定 MP 間のルートを確認します。
show cfm	CFM のドメイン情報を表示します。
show cfm remote-mep	CFM のリモート MEP の情報を表示します。
show cfm fault	CFM の障害情報を表示します。
show cfm l2traceroute-db	l2traceroute コマンドで取得したルート情報を表示します。
show cfm statistics	CFM の統計情報を表示します。
clear cfm remote-mep	CFM のリモート MEP 情報をクリアします。
clear cfm fault	CFM の障害情報をクリアします。
clear cfm l2traceroute-db	l2traceroute コマンドで取得したルート情報をクリアします。
clear cfm statistics	CFM の統計情報をクリアします。
restart cfm	CFM プログラムを再起動します。
dump protocols cfm	CFM のダンプ情報をファイルへ出力します。

27.3.2 MP 間の接続確認

l2ping コマンドで、指定した MP 間の疎通を確認して、結果を表示します。コマンドには確認回数および応答待ち時間を指定できます。指定しない場合、確認回数は 5 回、応答待ち時間は 5 秒です。疎通確認の応答受信または応答待ち時間経過を契機に、次の確認を繰り返します。

図 27-33 l2ping コマンドの実行結果

```
>l2ping remote-mep 1010 domain-level 7 ma 1000 mep 1020 count 3 timeout 1
L2ping to MP:1010(0012.e220.00a3) on Level:7 MA:1000 MEP:1020 VLAN:20
Time:2009/03/14 19:10:24
1: L2ping Reply from 0012.e220.00a3 64bytes Time= 751 ms
2: L2ping Reply from 0012.e220.00a3 64bytes Time= 752 ms
3: L2ping Reply from 0012.e220.00a3 64bytes Time= 744 ms

--- L2ping Statistics ---
Tx L2ping Request : 3 Rx L2ping Reply : 3 Lost Frame : 0%
Round-trip Min/Avg/Max : 744/749/752 ms

>
```

27.3.3 MP 間のルート確認

l2traceroute コマンドで、指定した MP 間のルート情報を収集し、結果を表示します。コマンドには応答待ち時間と TTL 値を指定できます。指定しない場合、応答待ち時間は 5 秒、TTL 値は 64 です。

宛先に指定した MP から応答を受信したことを「Hit」で確認できます。

図 27-34 l2traceroute コマンドの実行結果

```
>l2traceroute remote-mep 2010 domain-level 7 ma 1000 mep 2020 timeout 10 ttl 64
Date 2009/03/15 14:05:30 UTC
L2traceroute to MP:0012.e220.00a3 on Level:7 MA:1000 MEP:1020 VLAN:1000
Time:2009/03/15 14:05:30
63 0012.e220.00c0 Forwarded
62 0012.e210.000d Forwarded
61 0012.e242.00a3 NotForwarded Hit
```

27.3.4 ルート上の MP の状態確認

show cfm l2traceroute-db detail コマンドで、宛先の MP までのルートとルート上の MP の詳細情報を確認できます。「NotForwarded」が表示された場合、Ingress Port および Egress Port の「Action」で、リンクトレースメッセージが中継されなかった理由を確認できます。

図 27-35 show cfm l2traceroute-db detail コマンドの実行結果

```
> show cfm l2traceroute-db remote-mac 0012.e220.1040 detail
Date 2009/03/16 10:21:42 UTC
L2traceroute to MP:2010(0012.e220.1040) on Level:7 MA:2000 MEP:2020 VLAN:20
Time:2009/03/16 10:21:42
63 0012.e220.10a9 Forwarded
  Last Egress : 0012.f110.2400 Next Egress : 0012.e220.10a0
  Relay Action: MacAdrTbl
  Chassis ID   Type: MAC           Info: 0012.e228.10a0
  Ingress Port MP Address: 0012.e220.10a9 Action: OK
  Egress Port  MP Address: 0012.e220.10aa Action: OK
62 0012.e228.aa3b NotForwarded
  Last Egress : 0012.e220.10a0 Next Egress : 0012.e228.aa30
  Relay Action: MacAdrTbl
  Chassis ID   Type: MAC           Info: 0012.e228.aa30
  Ingress Port MP Address: 0012.e228.aa2c Action: -
  Egress Port  MP Address: 0012.e228.aa3b Action: Down
>
```

27.3.5 CFM の状態の確認

show cfm コマンドで、CFM の設定状態と障害検知状態を表示します。CC で障害を検知した場合、検知した障害の中で、最も障害レベルの高い障害種別を「Status」で確認できます。

図 27-36 show cfm コマンドの実行結果

```
>show cfm
Date 2009/03/15 18:32:10 UTC
Domain Level 3 Name(str): ProviderDomain_3
  MA 300 Name(str) : Tokyo_to_Osaka
    Primary VLAN:300 VLAN:10-20,300
    CC:Enable Interval:1min
    Alarm Priority:3 Start Time:2500ms Reset Time:10000ms
    MEP Information
      ID:8012 UpMEP CH12(Up) Enable MAC:0012.e200.00b2 Status:Timeout
  MA 400 Name(str) : Tokyo_to_Nagoya
    Primary VLAN:400 VLAN:30-40,400
    CC:Enable Interval:1min
    Alarm Priority:3 Start Time:2500ms Reset Time:10000ms
    MEP Information
      ID:8014 DownMEP 1/21(Up) Disable MAC:0012.e220.0040 Status:-
  MIP Information
    1/12(Up) Enable MAC:0012.e200.0012
    1/22(Down) Disable MAC:-
Domain Level 4 Name(str): ProviderDomain_4
  MIP Information
    CH12(Up) Enable MAC:0012.e220.00b2
>
```

27.3.6 障害の詳細情報の確認

show cfm fault detail コマンドで、障害種別ごとに、障害検知状態と障害検知のきっかけとなった CCM 情報を表示します。CCM を送信したリモート MEP は「RMEP」、「MAC」および「VLAN」で確認できます。

図 27-37 show cfm fault detail コマンドの実行結果

```
>show cfm fault detail
Date 2009/03/21 12:23:41 UTC
MD:7 MA:1000 MEP:1000 Fault
  OtherCCM : - RMEP:1020 MAC:0012.e220.1e22 VLAN:1000 Time:2009/03/20 11:22:17
  ErrorCCM : -
  Timeout : -
  PortState: -
  RDI      : On RMEP:1011 MAC:0012.e220.11a2 VLAN:1000 Time:2009/03/21 11:42:10
>
```

show cfm fault detail コマンドで表示されるリモート MEP 情報は障害検知のきっかけとなった情報であり、実際には複数のリモート MEP で障害が発生しているおそれがあります。

現在どのリモート MEP で障害が発生しているかは、show cfm remote-mep コマンドで表示されるリモート MEP 情報の「ID」および「Status」で確認できます。

図 27-38 show cfm remote-mep コマンドの実行結果

```
>show cfm remote-mep
Date 2009/03/21 12:25:30 UTC
Total RMEP Counts: 5
Domain Level 7 Name(str): ProviderDomain_7
  MA 1000 Name(str) : Tokyo_to_Osaka
    MEP ID:1000 0/20(Up) Enable Status:RDI
    RMEP Information Counts: 3
      ID:1011 Status:- MAC:0012.e200.005a Time:2009/03/21 12:25:29
      ID:1020 Status:RDI MAC:0012.e220.1e22 Time:2009/03/21 12:25:29
      ID:1030 Status:RDI MAC:0012.e220.1e09 Time:2009/03/21 12:25:29
    MA 2000 Name(str) : Tokyo_to_Nagoya
      MEP ID:8012 CH1 (Up) Enable Status:-
      RMEP Information Counts: 2
        ID:8003 Status:- MAC:0012.e20a.1241 Time:2009/03/21 12:25:28
        ID:8004 Status:- MAC:0012.e20d.12a1 Time:2009/03/21 12:25:29
>
```

28 SNMP を使用したネットワーク管理

この章では本装置の SNMP エージェント機能についてサポート仕様を中心に説明します。

28.1 解説

28.2 コンフィグレーション

28.3 オペレーション

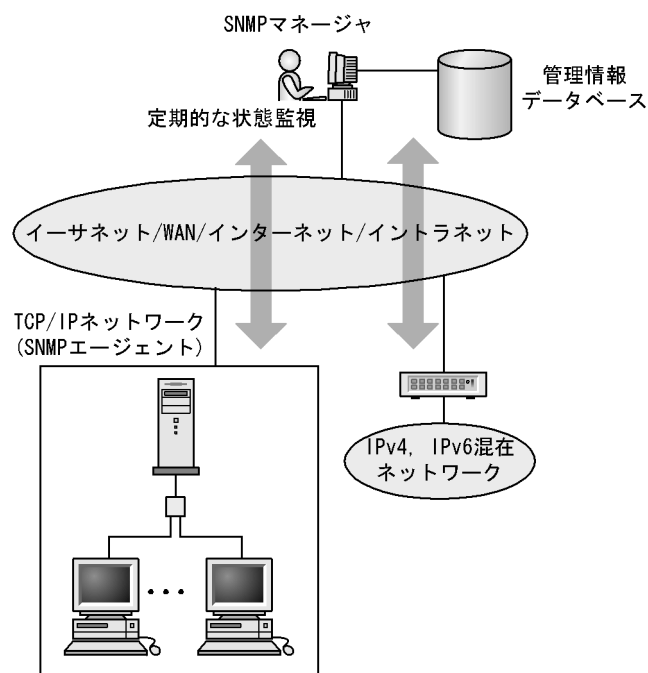
28.1 解説

28.1.1 SNMP 概説

(1) ネットワーク管理

ネットワークシステムの稼働環境や性能を維持するためには、高度なネットワーク管理が必要です。SNMP (simple network management protocol) は業界標準のネットワーク管理プロトコルです。SNMPをサポートしているネットワーク機器で構成されたマルチベンダーネットワークを管理できます。管理情報を収集して管理するサーバを SNMP マネージャ、管理される側のネットワーク機器を SNMP エージェントといいます。ネットワーク管理の概要を次の図に示します。

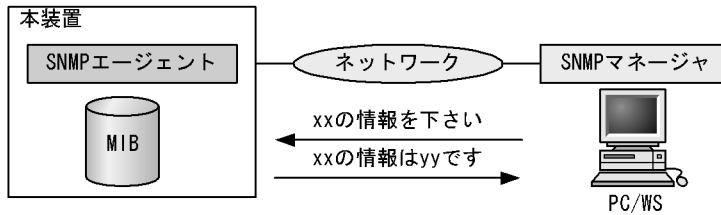
図 28-1 ネットワーク管理の概要



(2) SNMP エージェント機能

本装置の SNMP エージェントは、ネットワーク上の装置内部に組み込まれたプログラムです。装置内の情報を SNMP マネージャに提供する機能があります。装置内にある各種情報を MIB (Management Information Base) と呼びます。SNMP マネージャは、装置の情報を取り出して編集・加工し、ネットワーク管理を行うための各種情報をネットワーク管理者に提供するソフトウェアです。MIB 取得の例を次の図に示します。

図 28-2 MIB 取得の例

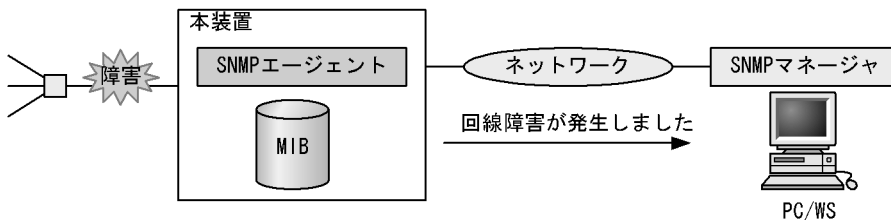


本装置の運用コマンドには MIB 情報を表示するための SNMP コマンドがあります。このコマンドは、自装置およびリモート装置の SNMP エージェントの MIB を表示します。

本装置では、SNMPv1 (RFC1157)、SNMPv2C (RFC1901)、および SNMPv3 (RFC3410) をサポートしています。SNMP マネージャを使用してネットワーク管理を行う場合は、SNMPv1、SNMPv2C、または SNMPv3 プロトコルで使用してください。なお、SNMPv1、SNMPv2C、SNMPv3 をそれぞれ同時に使用することもできます。

また、SNMP エージェントはトラップ (Trap) やインフォーム (Inform) と呼ばれるイベント通知 (主に障害発生の情報など) 機能があります。SNMP マネージャは、トラップまたはインフォームを受信することで定期的に装置の状態変化を監視しなくても変化を知ることができます。ただし、トラップは UDP を使用しているため、装置から SNMP マネージャに対するトラップの到達確認ができません。そのため、ネットワークの輻輳などによって、トラップがマネージャに到達しない場合があります。トラップの例を次の図に示します。

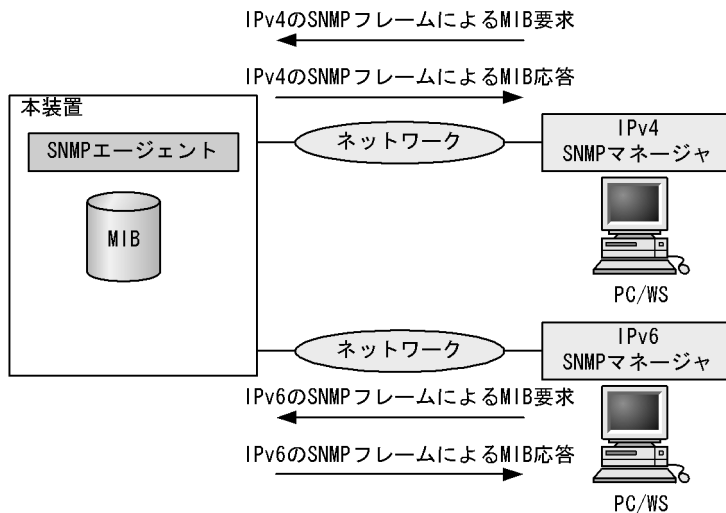
図 28-3 トラップの例



インフォームもトラップと同じ UDP によるイベント通知ですが、トラップとは異なって SNMP マネージャからの応答を要求します。そのため、応答の有無でインフォームの到達を確認できます。これによって、ネットワークの輻輳などに対してもインフォームの再送で対応できます。

本装置の SNMP プロトコルは IPv6 に対応しています。コンフィグレーションに設定した SNMP マネージャの IP アドレスによって、IPv4 または IPv6 アドレスが設定されている SNMP マネージャからの MIB 要求や、SNMP マネージャへのトラップまたはインフォーム送信ができます。IPv4/IPv6 SNMP マネージャからの MIB 要求と応答の例を次の図に示します。

図 28-4 IPv4/IPv6 SNMP マネージャからの MIB 要求と応答の例



(3) SNMPv3

SNMPv3 は SNMPv2C までの全機能に加えて、管理セキュリティ機能が大幅に強化されています。ネットワーク上を流れる SNMP パケットを認証・暗号化することによって、SNMPv2C でのコミュニティ名と SNMP マネージャの IP アドレスの組み合わせによるセキュリティ機能では実現できなかった、盗聴、なりすまし、改ざん、再送などのネットワーク上の危険から SNMP パケットを守ることができます。

(a) SNMP エンティティ

SNMPv3 では、SNMP マネージャおよび SNMP エージェントを「SNMP エンティティ」と総称します。本装置の SNMPv3 は、SNMP エージェントに相当する SNMP エンティティをサポートしています。

(b) SNMP エンジン

SNMP エンジンとは認証、および暗号化したメッセージ送受信と管理オブジェクトへのアクセス制御のためのサービスを提供します。SNMP エンティティとは 1 対 1 の関係です。SNMP エンジンとは、同一管理ドメイン内でユニークな SNMP エンジン ID により識別されます。

(c) ユーザ認証とプライバシー機能

SNMPv1, SNMPv2C でのコミュニティ名による認証に対して、SNMPv3 ではユーザ認証を行います。また、SNMPv1, SNMPv2C にはなかったプライバシー機能（暗号化、復号化）も SNMPv3 でサポートされています。ユーザ認証とプライバシー機能は、ユーザ単位に設定できます。

本装置では、ユーザ認証プロトコルとして次の二つプロトコルをサポートしています。

- HMAC-MD5-96 (メッセージダイジェストアルゴリズムを使用した認証プロトコル。128 ビットのダイジェストのうち、最初の 96 ビットを使用する。秘密鍵は 16 オクテット)
- HMAC-SHA-96 (SHA メッセージダイジェストアルゴリズムを使用した認証プロトコル。160 ビットの SHA ダイジェストのうち、最初の 96 ビットを使用する。秘密鍵は 20 オクテット)

プライバシープロトコルとして次のプロトコルをサポートしています。

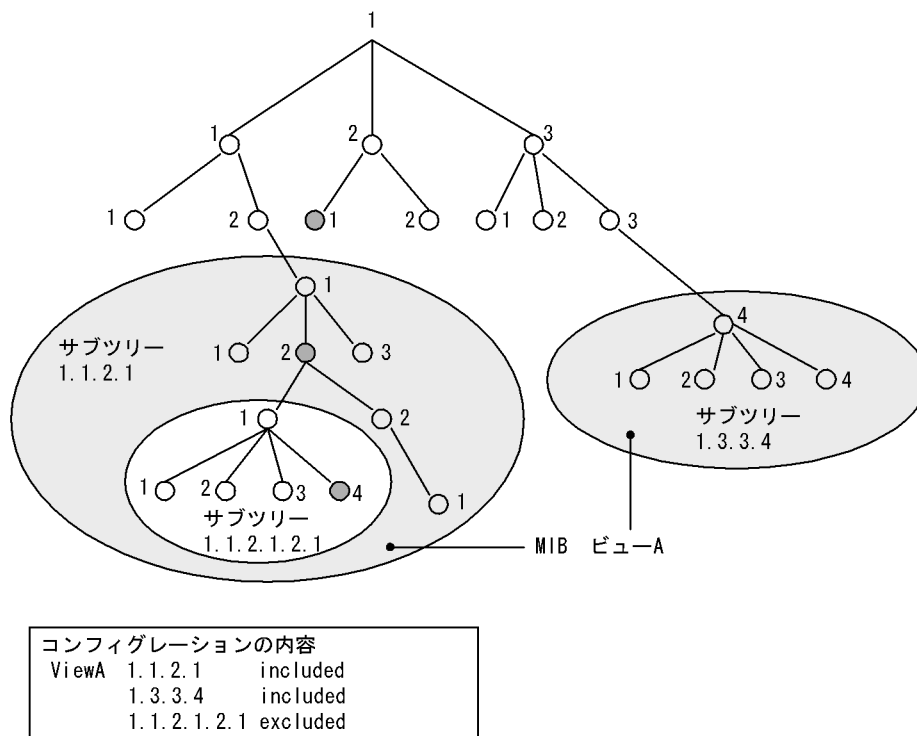
- CBC-DES (Cipher Block Chaining - Data Encryption Standard。共通鍵暗号アルゴリズムである DES (56 ビット鍵) を、CBC モードで強力にした暗号化プロトコル)

(d) MIB ビューによるアクセス制御

SNMPv3 では、ユーザ単位に、アクセスできる MIB オブジェクトの集合を設定できます。この MIB オブジェクトの集合を MIB ビューと呼びます。MIB ビューは、MIB のオブジェクト ID のツリーを表すビューサブツリーを集約することによって表現されます。集約するには、ビューサブツリーごとに included (MIB ビューに含む)、または excluded (MIB ビューから除外する) を選択できます。MIB ビューは、ユーザ単位に、Read ビュー、Write ビュー、Notify ビューとして設定できます。

次に、MIB ビューの例を示します。MIB ビューは、「図 28-5 MIB ビューの例」に示すような MIB ツリーの一部である MIB サブツリーをまとめて設定します。オブジェクト ID 1.1.2.1.2 は、サブツリー 1.1.2.1 に含まれるので、MIB ビュー A でアクセスできます。しかし、オブジェクト ID 1.2.1 は、どちらのサブツリーにも含まれないので、アクセスできません。また、オブジェクト ID 1.1.2.1.2.1.4 は、サブツリー 1.1.2.1.2.1 がビュー A から除外されているためアクセスできません。

図 28-5 MIB ビューの例



28.1.2 MIB 概説

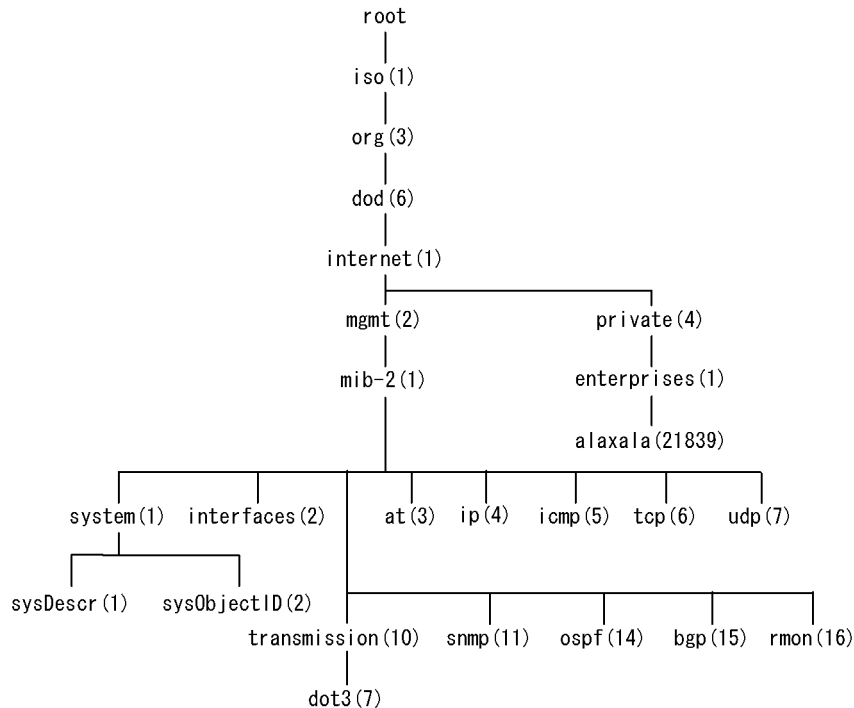
装置が管理し、SNMP マネージャに提供する MIB は、RFC で規定されたものと、装置の開発ベンダーが独自に用意する情報の 2 種類があります。

RFC で規定された MIB を標準 MIB と呼びます。標準 MIB は規格化されているため提供情報の内容の差はあまりありません。装置の開発ベンダーが独自に用意する MIB をプライベート MIB と呼び、装置によって内容が異なります。ただし、MIB のオペレーション (情報の採取・設定など) は、標準 MIB、プライベート MIB で共通です。オペレーションは、装置と目的の MIB 情報を指定するだけです。装置は IP アドレスで、MIB 情報はオブジェクト ID で指定します。

(1) MIB 構造

MIB の構造はツリー構造になっています。MIB はツリー構造のため、各ノードを識別するために番号を付けて表す決まりになっています。root から各ノードの数字を順番にたどって番号を付けることで個々の MIB 情報を一意に識別できます。この番号列をオブジェクト ID と呼びます。オブジェクト ID は root から下位のオブジェクトグループ番号をドットで区切って表現します。例えば、sysDescr という MIB をオブジェクト ID で示すと 1.3.6.1.2.1.1.1 になります。MIB ツリーの構造例を次の図に示します。

図 28-6 MIB ツリーの構造例



(2) MIB オブジェクトの表し方

オブジェクト ID は数字と . (ドット) (例: 1.3.6.1.2.1.1.1) で表現します。しかし、数字の羅列ではわかりにくいいため、マネージャによっては、sysDescr というニーモニックで指定できるものもあります。ニーモニックで指定する場合、SNMP マネージャがどの MIB のニーモニックを使えるか確認してから使用してください。また、本装置の SNMP コマンドで使用できるニーモニックについては、snmp lookup コマンドを実行することで確認できます。

(3) インデックス

MIB を指定するときのオブジェクト ID を使用しますが、一つの MIB に一つの意味だけある場合と一つの MIB に複数の情報がある場合があります。MIB を特定するためにはインデックス (INDEX) を使用します。インデックスは、オブジェクト ID の後ろに数字を付加して表し、何番目の情報かなどを示すために使用します。

一つの MIB に一つの意味だけがある場合、MIB のオブジェクト ID に ".0" を付加して表します。一つの MIB に複数の情報がある場合、MIB のオブジェクト ID の後ろに数字を付加して何番目の情報であるか表します。例えば、インタフェースのタイプを示す MIB に ifType (1.3.6.1.2.1.2.2.1.2) があります。本装置には複数のインタフェースがあります。特定のインタフェースのタイプを調べるには、"2 番目のインタフェースのタイプ" というように具体的に指定する必要があります。MIB で指定するときは、2 番目を示

すインデックス .2 を MIB の最後に付加して ifType.2 (1.3.6.1.2.1.2.2.1.2.2) と表します。

インデックスの表し方は、各 MIB によって異なります。RFC などの MIB の定義で、INDEX{ xxxxx,yyyyy,zzzzz } となっている MIB のエントリは、xxxxx と yyyyy と zzzzz をインデックスに持ちます。それぞれの MIB について、どのようなインデックスを取るか確認して MIB のオペレーションを行ってください。

(4) 本装置のサポート MIB

本装置では、装置の状態、インタフェースの統計情報、装置の機器情報など、管理に必要な MIB を提供しています。なお、プライベート MIB の定義 (ASN.1) ファイルは、ソフトウェアとともに提供します。

各 MIB の詳細については、マニュアル「MIB レファレンス」を参照してください。

28.1.3 SNMPv1, SNMPv2C オペレーション

管理データ (MIB:management information base) の収集や設定を行うため、SNMP では次に示す 4 種類のオペレーションがあります。

- GetRequest : 指定した MIB の情報を取り出します。
- GetNextRequest : 指定した次の MIB の情報を取り出します。
- GetBulkRequest : GetNextRequest の拡張版です。
- SetRequest : 指定した MIB に値を設定します。

各オペレーションは SNMP マネージャから装置 (SNMP エージェント) に対して行われます。各オペレーションについて説明します。

(1) GetRequest オペレーション

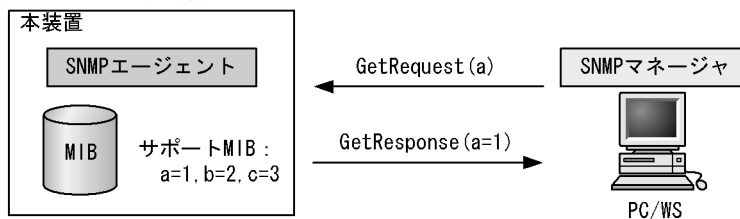
GetRequest オペレーションは、SNMP マネージャから装置 (エージェント機能) に対して MIB の情報を取り出すときに使用します。このオペレーションでは、一つまたは複数 MIB を指定できます。

装置が該当する MIB を保持している場合、GetResponse オペレーションで MIB 情報を応答します。該当する MIB を保持していない場合は、GetResponse オペレーションで noSuchName を応答します。

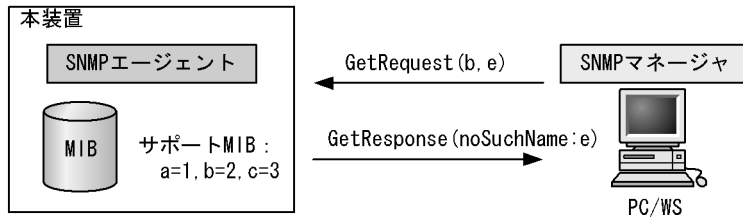
GetRequest オペレーションを次の図に示します。

図 28-7 GetRequest オペレーション

- 該当する MIB がある場合

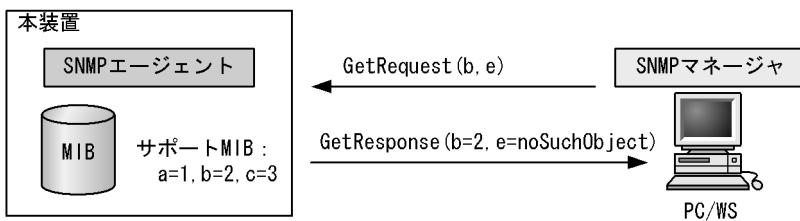


●該当するMIBがない場合



SNMPv2C では、装置が該当する MIB を保持していない場合は、GetResponse オペレーションで MIB 値に noSuchObject を応答します。SNMPv2C の場合の GetRequest オペレーションを次の図に示します。

図 28-8 GetRequest オペレーション (SNMPv2C)



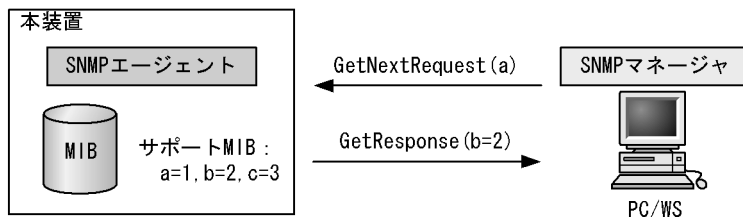
(2) GetNextRequest オペレーション

GetNextRequest オペレーションは、GetRequest オペレーションに似たオペレーションです。GetRequest オペレーションは、指定した MIB の読み出しに使用しますが、GetNextRequest オペレーションは、指定した MIB の次の MIB を取り出すときに使用します。このオペレーションも一つまたは複数の MIB を指定できます。

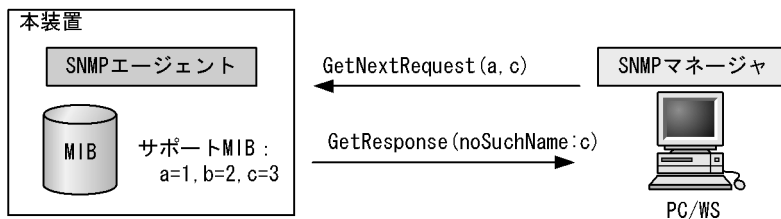
装置が指定した次の MIB を保持している場合は、GetResponse オペレーションで MIB を応答します。指定した MIB が最後の場合は、GetResponse で noSuchName を応答します。GetNextRequest オペレーションを次の図に示します。

図 28-9 GetNextRequest オペレーション

●指定したMIBの次のMIBがある場合

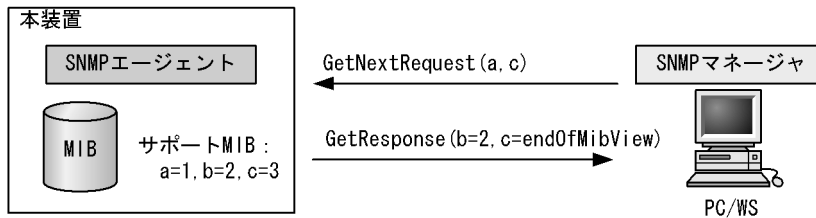


●指定したMIBが最後の場合



SNMPv2C の場合、指定した MIB が最後の場合は GetResponse で MIB 値に endOfMibView を応答します。SNMPv2C の場合の GetNextRequest オペレーションを次の図に示します。

図 28-10 GetNextRequest オペレーション (SNMPv2C)

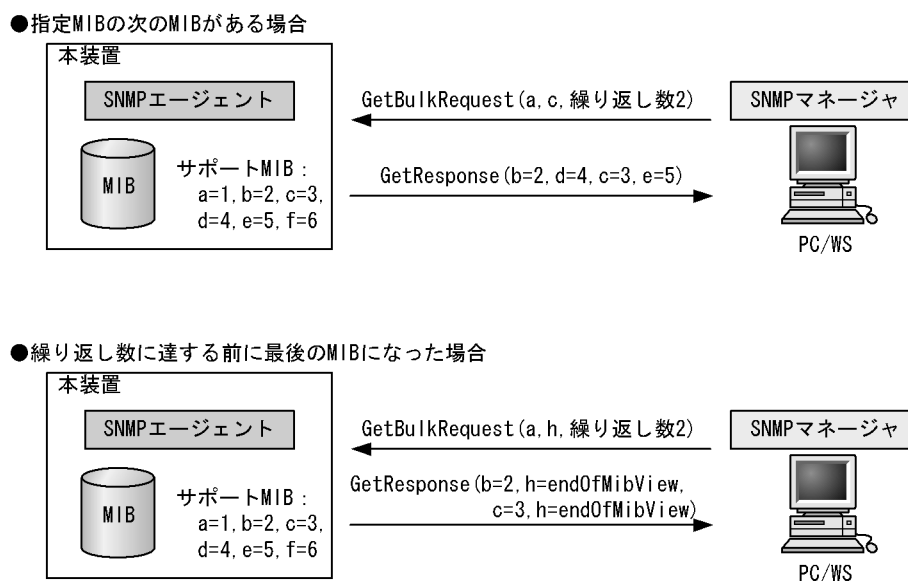


(3) GetBulkRequest オペレーション

GetBulkRequest オペレーションは、GetNextRequest オペレーションを拡張したオペレーションです。このオペレーションでは繰り返し回数を設定し、指定した MIB の次の項目から指定した繰り返し回数個分の MIB を取得できます。このオペレーションも、一つまたは複数の MIB を指定できます。

装置が、指定した MIB の次の項目から指定した繰り返し回数個分の MIB を保持している場合は、GetResponse オペレーションで MIB を応答します。指定した MIB が最後の場合、または繰り返し数に達する前に最後の MIB になった場合、GetResponse オペレーションで MIB 値に endOfMibView を応答します。GetBulkRequest オペレーションを次の図に示します。

図 28-11 GetBulkRequest オペレーション

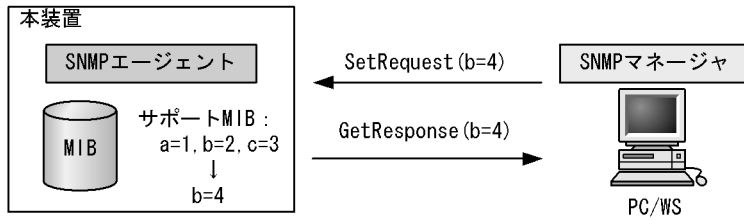


(4) SetRequest オペレーション

SetRequest オペレーションは、SNMP マネージャから装置 (エージェント機能) に対して行うオペレーションという点で GetRequest, GetNextRequest, GetBulkRequest オペレーションと似ていますが、値の設定方法が異なります。

SetRequest オペレーションでは、設定する値と MIB を指定します。値を設定すると、GetResponse オペレーションで MIB と設定値を応答します。SetRequest オペレーションを次の図に示します。

図 28-12 SetRequest オペレーション



(a) MIB を設定できない場合の応答

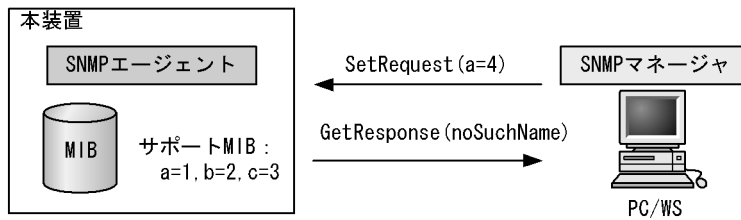
MIB を設定できないケースは、次に示す 3 とおりです。

- MIB が読み出し専用の場合 (読み出し専用コミュニティに属するマネージャの場合も含む)
- 設定値が正しくない場合
- 装置の状態によって設定できない場合

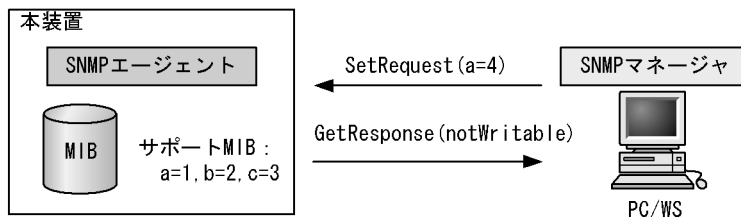
各ケースによって、応答が異なります。MIB が読み出し専用の場合、noSuchName の GetResponse 応答をします。SNMPv2C の場合、MIB が読み出し専用のときは notWritable の GetResponse 応答をします。MIB が読み出し専用の場合の SetRequest オペレーションを次の図に示します。

図 28-13 MIB 変数が読み出し専用の場合の SetRequest オペレーション

●SNMP

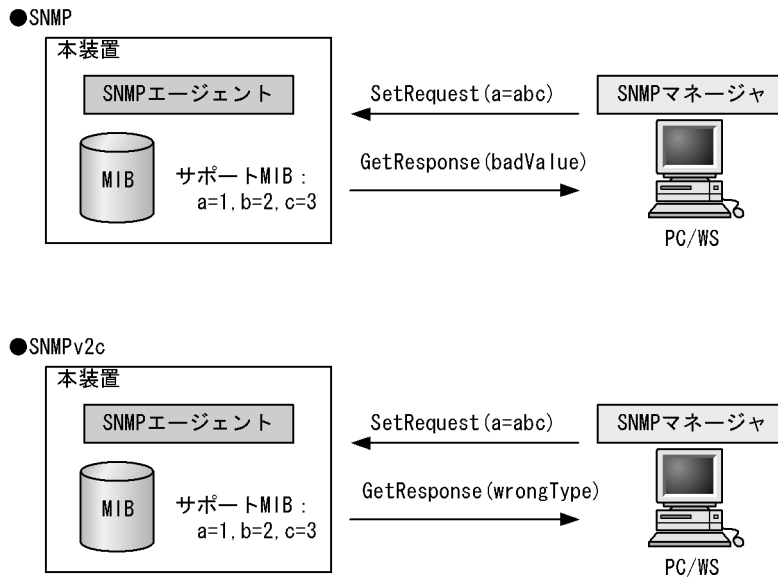


●SNMPv2c



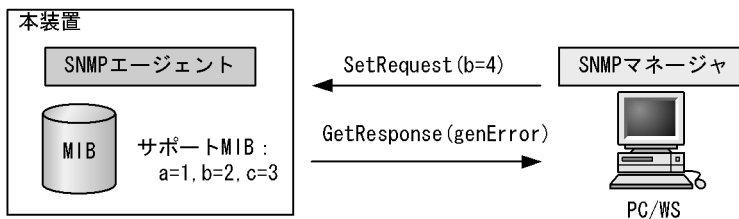
設定値のタイプが正しくない場合、badValue の GetResponse 応答をします。SNMPv2C の場合、設定値のタイプが正しくないときは wrongType の GetResponse 応答をします。設定値のタイプが正しくない場合の SetRequest オペレーションを次の図に示します。

図 28-14 設定値のタイプが正しくない場合の SetRequest オペレーション例



装置の状態によって設定できない場合、genError を応答します。例えば、装置内で値を設定しようとしたときに、装置内部で設定タイムアウトを検出した場合などがこれに当てはまります。装置の状態によって設定できない場合の SetRequest オペレーションを次の図に示します。

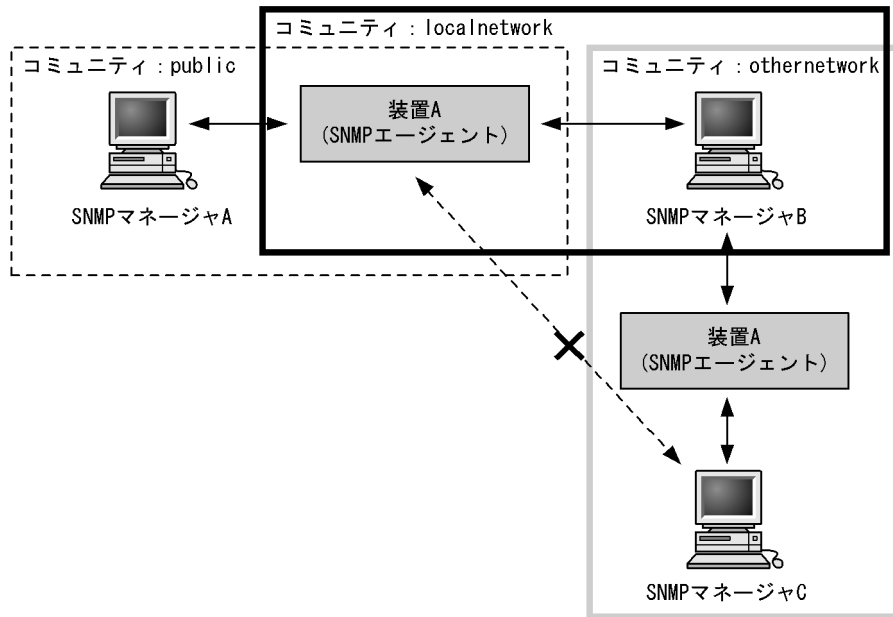
図 28-15 装置の状態によって設定できない場合の SetRequest オペレーション



(5) コミュニティによるオペレーション制限

SNMPv1 および SNMPv2C では、オペレーションを実行する SNMP マネージャを限定するため、コミュニティという概念があります。コミュニティはオペレーションを実行する SNMP マネージャと SNMP エージェントを一つのグループとして割り当てる名称です。MIB に対してオペレーションする場合は、SNMP マネージャと SNMP エージェントは、同一のグループ（コミュニティ）に属する必要があります。コミュニティによるオペレーションを次の図に示します。

図 28-16 コミュニティによるオペレーション



装置 A はコミュニティ (public) およびコミュニティ (localnetwork) に属しています。コミュニティ (othernetwork) には属していません。この場合、装置 A はコミュニティ (public) およびコミュニティ (localnetwork) の SNMP マネージャ A, B から MIB のオペレーションを受け付けますが、コミュニティ (othernetwork) の SNMP マネージャ C からのオペレーションは受け付けません。

(6) IP アドレスによるオペレーション制限

本装置では、セキュリティを考慮し、アクセスリストを使用することでコミュニティと SNMP マネージャの IP アドレスの組み合わせが合わないときは MIB のオペレーションを受け付けないようにできます。本装置で SNMPv1 および SNMPv2C を使用するときは、コミュニティをコンフィグレーションコマンドで登録する必要があります。なお、コミュニティは文字列で設定します。また、一般的にコミュニティ名称は、public を使用している場合が多いです。

(7) SNMP オペレーションのエラーステータスコード

オペレーションでエラーが発生した場合、SNMP エージェントはエラーステータスにエラーコードを設定し、何番目の MIB 情報でエラーが発生したかをエラー位置番号に設定した GetResponse オペレーションの応答を返します。オペレーションの結果が正常なら、エラーステータスにエラーなしのコードを設定し、MIB 情報内にオペレーションした MIB 情報を設定した GetResponse オペレーションの応答を返します。エラーステータスコードを次の表に示します。

表 28-1 エラーステータスコード

エラーステータス	コード	内容
noError	0	エラーはありません。
tooBig	1	データサイズが大きく PDU に値を設定できません。
noSuchName	2	指定 MIB がない、または書き込みできませんでした。
badValue	3	設定値が不正です。
readOnly	4	書き込みできませんでした (本装置では、応答することはありません)。
genError	5	その他のエラーが発生しました。

エラーステータス	コード	内容
noAccess	6	アクセスできない MIB に対して set を行おうとしました。
wrongType	7	MIB で必要なタイプと異なるタイプが指定されました。
wrongLength	8	MIB で必要なデータ長と異なる長さが指定されました。
wrongEncoding	9	ASN.1 符号が不正でした。
wrongValue	10	MIB 値が不正でした。
noCreation	11	該当する MIB が存在しません。
inconsistentValue	12	現在何か理由があって値が設定できません。
resourceUnavailable	13	値の設定のためにリソースが必要ですが、リソースが利用できません。
commitFailed	14	値の更新に失敗しました。
undoFailed	15	値の更新に失敗したときに、更新された値を元に戻すのに失敗しました。
notWritable	17	セットできません。
inconsistentName	18	該当する MIB が存在しないため、現在は作成できません。

28.1.4 SNMPv3 オペレーション

管理データ (MIB:management information base) の収集や設定を行うため、SNMP では次に示す四種類のオペレーションがあります。

- GetRequest : 指定した MIB の情報を取り出します。
- GetNextRequest : 指定した次の MIB の情報を取り出します。
- GetBulkRequest : GetNextRequest の拡張版です。
- SetRequest : 指定した MIB に値を設定します。

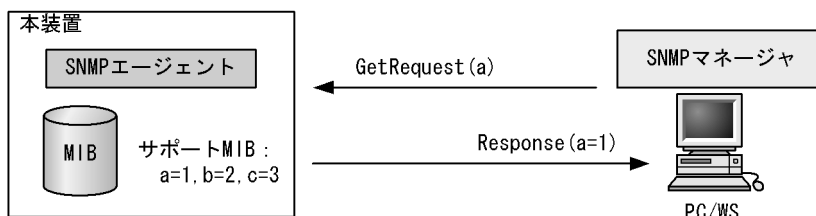
各オペレーションは SNMP マネージャから装置 (SNMP エージェント) に対して行われます。各オペレーションについて説明します。

(1) GetRequest オペレーション

GetRequest オペレーションは、SNMP マネージャから装置 (エージェント機能) に対して MIB の情報を取り出すときに使用します。このオペレーションでは、一つまたは複数の MIB を指定できます。装置が該当する MIB を保持している場合、Response オペレーションで MIB 情報を応答します。

GetRequest オペレーションを次の図に示します。

図 28-17 GetRequest オペレーション



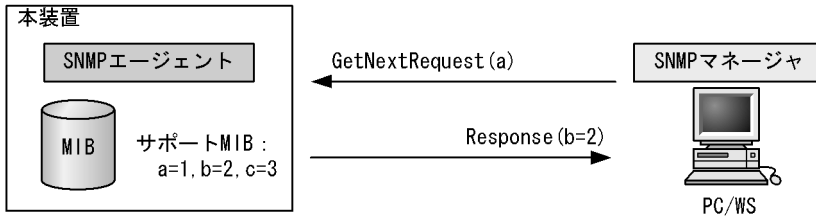
(2) GetNextRequest オペレーション

GetNextRequest オペレーションは、GetRequest オペレーションに似たオペレーションです。

GetRequest オペレーションが指定した MIB の読み出しに使用するのに対し，GetNextRequest オペレーションは指定した MIB の次の MIB を取り出すときに使用します。このオペレーションも一つまたは複数の MIB を指定できます。

GetNextRequest オペレーションを次の図に示します。

図 28-18 GetNextRequest オペレーション

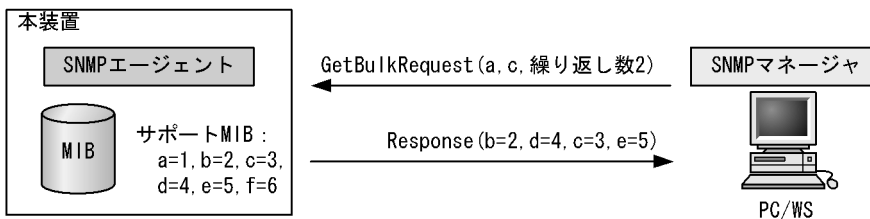


(3) GetBulkRequest オペレーション

GetBulkRequest オペレーションは，GetNextRequest オペレーションを拡張したオペレーションです。このオペレーションでは繰り返し回数を設定し，指定した MIB の次の項目から指定した繰り返し回数個分の MIB を取得できます。このオペレーションも，一つまたは複数の MIB を指定できます。

GetBulkRequest オペレーションを次の図に示します。

図 28-19 GetBulkRequest オペレーション



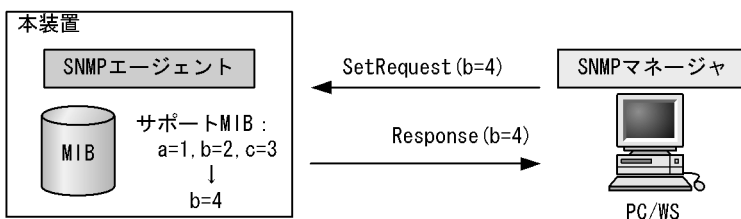
(4) SetRequest オペレーション

SetRequest オペレーションは，SNMP マネージャから装置（エージェント機能）に対して行うオペレーションという点で GetRequest，GetNextRequest，GetBulkRequest オペレーションと似ていますが，値の設定方法が異なります。

SetRequest オペレーションでは，設定する値と MIB を指定します。値を設定すると，Response オペレーションで MIB と設定値を応答します。

SetRequest オペレーションを次の図に示します。

図 28-20 SetRequest オペレーション



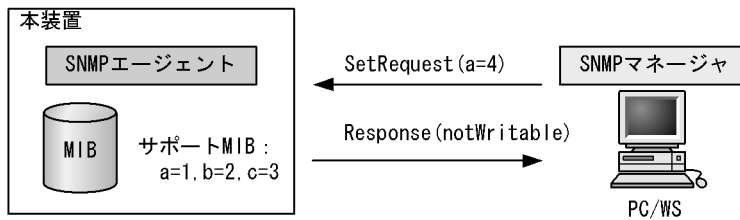
(a) MIB を設定できない場合の応答

MIB を設定できないケースは、次に示す 3 とおりです。

- MIB が読み出し専用の場合
- 設定値が正しくない場合
- 装置の状態によって設定できない場合

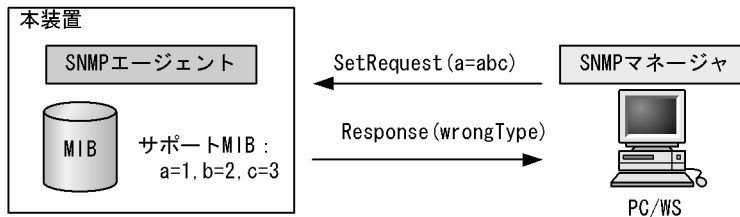
各ケースによって、応答が異なります。MIB が読み出し専用ときは notWritable の Response 応答をします。MIB が読み出し専用の場合の SetRequest オペレーションを次の図に示します。

図 28-21 MIB 変数が読み出し専用の場合の SetRequest オペレーション



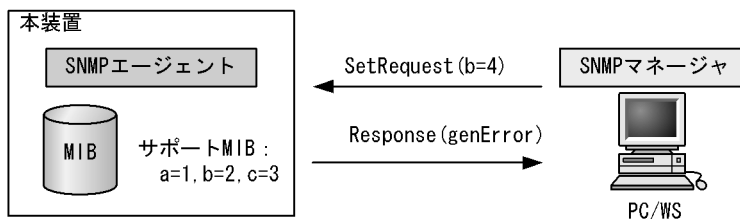
設定値のタイプが正しくないときは wrongType の Response 応答をします。設定値のタイプが正しくない場合の SetRequest オペレーションを次の図に示します。

図 28-22 設定値のタイプが正しくない場合の SetRequest オペレーション例



装置の状態によって設定できない場合、genError を応答します。例えば、装置内で値を設定しようとしたときに、装置内部で設定タイムアウトを検出した場合などがこれに当てはまります。装置の状態によって設定できない場合の SetRequest オペレーションを次の図に示します。

図 28-23 装置の状態によって設定できない場合の SetRequest オペレーション



(5) SNMPv3 でのオペレーション制限

SNMPv1 および SNMPv2C ではコミュニティと SNMP マネージャの IP アドレスの組み合わせによって確認が行われるのに対し、SNMPv3 ではユーザ認証と MIB ビューによって MIB のオペレーションを制限します。本装置で SNMPv3 を使用するときには、SNMP セキュリティユーザ、MIB ビューおよびセキュリティグループをコンフィグレーションコマンドで登録する必要があります。また、トラップを送信するに

は、SNMP セキュリティユーザ、MIB ビュー、セキュリティグループ、およびトラップ送信 SNMP マネージャをコンフィギュレーションコマンドで登録する必要があります。

(6) SNMPv3 オペレーションのエラーステータスコード

オペレーションの結果エラーが発生した場合、SNMP エージェントはエラーステータスにエラーコードを設定し、何番目の MIB 情報でエラーが発生したかをエラー位置番号に設定した Response オペレーションの応答を返します。オペレーションの結果が正常であれば、エラーステータスにエラーなしのコードを設定し、MIB 情報内にオペレーションした MIB 情報を設定した Response オペレーションの応答を返します。エラーステータスコードを次の表に示します。

表 28-2 エラーステータスコード

エラーステータス	コード	内容
noError	0	エラーはありません。
tooBig	1	データサイズが大きすぎて PDU に値を設定できません。
noSuchName	2	指定 MIB がない、または書き込みできませんでした。
badValue	3	設定値が不正です。
readOnly	4	書き込みできませんでした (本装置では、応答することはありません)。
genError	5	その他のエラーが発生しました。
noAccess	6	アクセスできない MIB に対して set を行おうとしました。
wrongType	7	MIB で必要なタイプと異なるタイプが指定されました。
wrongLength	8	MIB で必要なデータ長と異なる長さが指定されました。
wrongEncoding	9	ASN.1 符号が不正でした。
wrongValue	10	MIB 値が不正でした。
noCreation	11	該当する MIB が存在しません。
inconsistentValue	12	現在何か理由があって値が設定できません。
resourceUnavailable	13	値の設定のためにリソースが必要ですが、リソースが利用できません。
commitFailed	14	値の更新に失敗しました。
undoFailed	15	値の更新に失敗したときに、更新された値を元に戻すのに失敗しました。
authorizationError	16	認証に失敗しました。
notWritable	17	セットできません。
inconsistentName	18	該当する MIB が存在しないため、現在は作成できません。

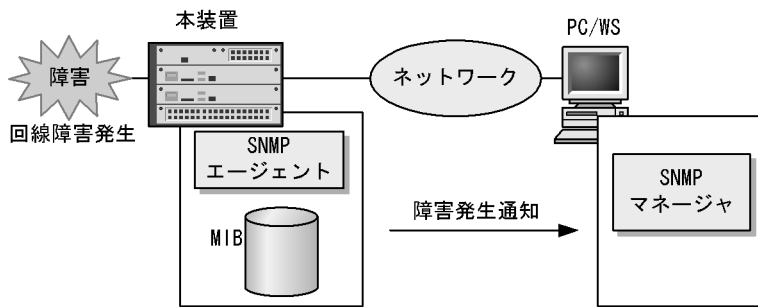
28.1.5 トラップ

(1) トラップ概説

SNMP エージェントはトラップ (Trap) と呼ばれるイベント通知 (主に障害発生の情報やログ情報など) 機能があります。トラップは重要なイベントを SNMP エージェントから SNMP マネージャに非同期に通知する機能です。SNMP マネージャは、トラップを受信することで装置の状態変化を検知できます。この通知を基に、装置内の MIB を取得して、さらに詳細な情報を得ることができます。

なお、トラップは UDP を使用しているため、装置から SNMP マネージャに対するトラップの到達が確認できません。そのため、ネットワークの輻輳などによってトラップがマネージャに到達しない場合があります。トラップの例を次の図に示します。

図 28-24 トラップの例



(2) トラップフォーマット (SNMPv1)

トラップフレームには、どの IP アドレスの装置で、いつ、何が発生したかを示す情報を含みます。トラップフォーマット (SNMPv1) を次の図に示します。

図 28-25 トラップフォーマット (SNMPv1)

SNMPバージョン		Community名		Trap PDU			
TRAP	装置ID	エージェントアドレス	トラップ番号	拡張トラップ番号	発生時刻	関連MIB情報	

装置ID : 装置の識別ID (通常MIB-IIのsysObjectIDの値が設定される)
 エージェントアドレス : トラップが発生した装置のIPアドレス
 トラップ番号 : トラップの種類を示す識別番号
 拡張トラップ番号 : トラップ番号の補足をするための番号
 発生時刻 : トラップが発生した時間 (装置が起動してからの経過時間)
 関連MIB情報 : このトラップに関連するMIB情報

(3) トラップフォーマット (SNMPv2C, SNMPv3)

トラップフレームには、いつ、何が発生したかを示す情報を含みます。トラップフォーマット (SNMPv2C, SNMPv3) を次の図に示します。

図 28-26 トラップフォーマット (SNMPv2C, SNMPv3)

SNMPバージョン		Community名		Trap PDU		
TRAP	リクエストID	エラーステータス	エラーインデックス	関連MIB情報		

リクエストID : メッセージ識別子。リクエストごとに異なる。
 エラーステータス : 発生したエラーを示す値
 エラーインデックス : 関連MIB情報でのエラー位置
 関連MIB情報 : このトラップに関連するMIB情報

28.1.6 インフォーム

(1) インフォーム概説

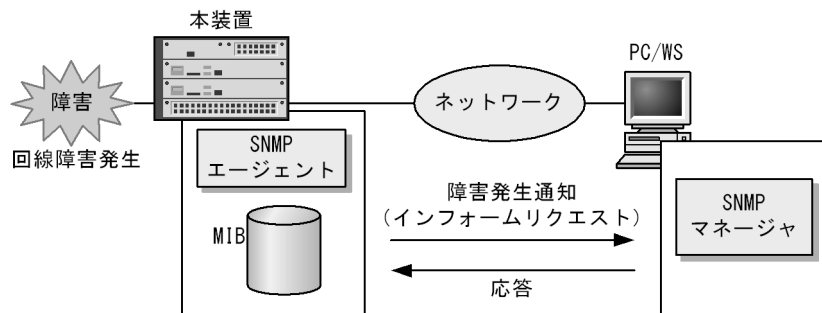
SNMP エージェントはインフォーム (Inform) と呼ばれるイベント通知 (主に障害発生の情報やログ情報など) 機能があります。インフォームはインフォームリクエストを発行して、重要なイベントを SNMP

エージェントから SNMP マネージャに通知する機能です。SNMP マネージャは、インフォームリクエストを受信することで装置の状態変化を検知できます。この通知を基に、装置内の MIB を取得して、さらに詳細な情報を得ることができます。

インフォームは SNMPv2c だけのサポートとなります。また、SNMP マネージャもインフォームに対応している必要があります。

なお、インフォームもトラップと同じ UDP によるイベント通知ですが、トラップとは異なって SNMP マネージャからの応答を要求します。そのため、応答の有無でインフォームリクエストの到達を確認できます。これによって、ネットワークの輻輳などに対してもインフォームリクエストの再送で対応できます。インフォームの例を次の図に示します。

図 28-27 インフォームの例



(2) インフォームリクエストフォーマット

インフォームリクエストフレームには、いつ、何が発生したかを示す情報を含みます。インフォームリクエストフォーマットを次の図に示します。

図 28-28 インフォームリクエストフォーマット

SNMPバージョン	Community名	InformRequest PDU			
INFORM	リクエストID	エラーステータス	エラーインデックス	関連MIB情報	

- リクエストID : メッセージ識別子。リクエストごとに異なる。
- エラーステータス : 発生したエラーを示す値
- エラーインデックス : 関連MIB情報でのエラー位置
- 関連MIB情報 : このインフォームリクエストに関連するMIB情報

28.1.7 RMON MIB

RMON (Remote Network Monitoring) とは、イーサネット統計情報を提供する機能、収集した統計情報の閾値チェックを行ってイベントを発生させる機能、パケットをキャプチャする機能などをもちます。この RMON は RFC1757 で規定されています。

RMON MIB のうち、statistics, history, alarm, event の各グループについて概要を説明します。

(1) statistics グループ

監視対象のサブネットワークについての、基本的な統計情報を収集します。例えば、サブネットワーク中の総パケット数、ブロードキャストパケットのような各種類ごとのパケット数、CRC エラー、コリジョン

エラーなどのエラー数などです。statistics グループを使うと、サブネットワークのトラフィック状況や回線状態などの統計情報を取得できます。

(2) history グループ

statistics グループで収集する情報とほぼ同じ統計情報をサンプリングし、来歴情報として保持できます。

history グループには historyControlTable という制御テーブルと、etherHistoryTable というデータテーブルがあります。historyControlTable はサンプリング間隔や来歴記録数の設定を行うための MIB です。

etherHistoryTable は、サンプリングした統計情報の来歴記録の MIB です。history グループは、一定期間の統計情報を装置内で保持しています。このため、SNMP マネージャなどが定期的にポーリングして統計情報を収集するのと比較して、ネットワークに負荷をかけることが少なく、連続した一定期間の統計情報を取得できます。

(3) alarm グループ

監視対象とする MIB のチェック間隔、閾値などを設定して、その MIB が閾値に達したときにログを記録したり、SNMP マネージャにトラップまたはインフォームを発行したりすることを指定する MIB です。この alarm グループを使用するときは、event グループも設定する必要があります。

alarm グループによる MIB 監視には、MIB 値の差分（変動）と閾値を比較する delta 方式と、MIB 値と閾値を直接比較する absolute 方式があります。

delta 方式による閾値チェックでは、例えば、CPU 使用率の変動が 50% 以上あったときに、ログを収集したり、SNMP マネージャにトラップまたはインフォームを発行したりできます。absolute 方式による閾値チェックでは、例えば、CPU の使用率が 80% に達したときに、ログを収集したり、SNMP マネージャにトラップまたはインフォームを発行したりできます。

本装置では、閾値をチェックするタイミングによる検出漏れをできるだけ防止するために、alarmInterval (MIB 値を監視する時間間隔 (秒) を表す MIB) の間に複数回チェックします。alarmInterval ごとの閾値チェック回数を次の表に示します。

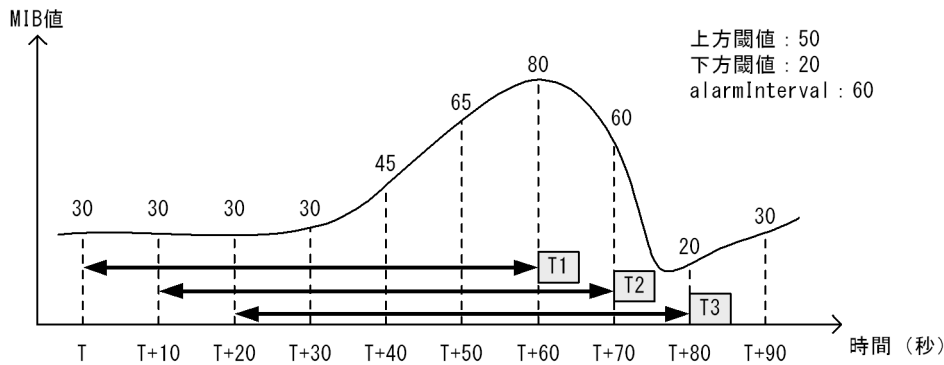
表 28-3 alarmInterval ごとの閾値チェック回数

alarmInterval (秒)	閾値チェック回数
1	1
2 ~ 5	2
6 ~ 10	3
11 ~ 20	4
21 ~ 50	5
51 ~ 100	6
101 ~ 200	7
201 ~ 400	8
401 ~ 800	9
801 ~ 1300	10
1301 ~ 2000	11
2001 ~ 4294967295	12

閾値のチェックは、およそ alarmInterval を閾値チェック回数で割った秒数ごとに行います。例えば、alarmInterval が 60 (秒) の場合、閾値チェック回数は 6 回になるため、10 秒に 1 回のタイミングで閾値をチェックします。

上方閾値を 50、下方閾値を 20、alarmInterval を 60 とし、CPU 使用率の MIB 値を delta 方式で監視した場合の例を次の図に示します。

図 28-29 delta 方式による MIB 監視例



T1

閾値と比較する値が 50 (T+60 (秒) の MIB 値 80 - T (秒) の MIB 値 30) のため、上方閾値以上を検出

T2

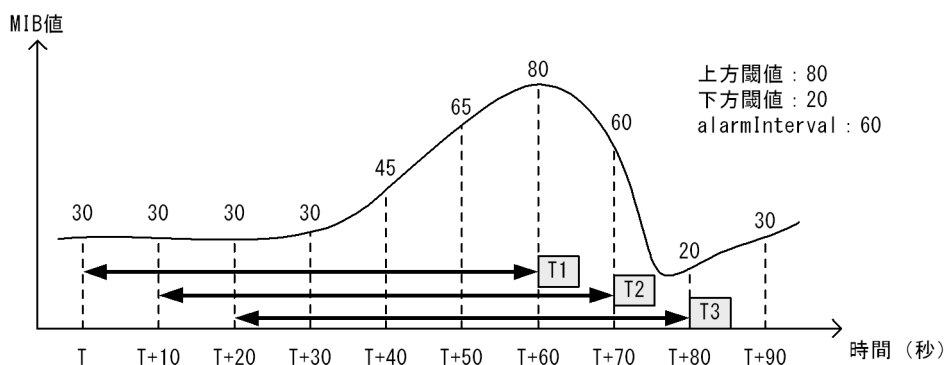
閾値と比較する値が 30 (T+70 (秒) の MIB 値 60 - T+10 (秒) の MIB 値 30) のため、閾値検出なし

T3

閾値と比較する値が -10 (T+80 (秒) の MIB 値 20 - T+20 (秒) の MIB 値 30) のため、下方閾値以下を検出

上方閾値を 80、下方閾値を 20、alarmInterval を 60 とし、CPU 使用率の MIB 値を absolute 方式で監視した場合の例を次の図に示します。

図 28-30 absolute 方式による MIB 監視例



T1

閾値と比較する値が 80 (T+60 (秒) の MIB 値) のため、上方閾値以上を検出

T2

閾値と比較する値が 60 (T+70 (秒) の MIB 値) のため、閾値検出なし

T3

閾値と比較する値が 20 (T+80 (秒) の MIB 値) のため、下方閾値以下を検出

(4) event グループ

event グループには alarm グループで設定した MIB の閾値を超えたときの動作を指定する eventTable グループ MIB と閾値を超えたときにログを記録する logTable グループ MIB があります。

eventTable グループ MIB は、閾値に達したときにログを記録するのか、SNMP マネージャにトラップまたはインフォームを発行するのか、またはその両方するか何もしないかを設定するための MIB です。

logTable グループ MIB は、eventTable グループ MIB でログの記録を指定したときに、装置内にログを記録します。装置内のログのエントリ数は決まっているので、エントリをオーバーした場合、新しいログ情報の追加によって、古いログ情報が消去されていきます。定期的に SNMP マネージャに記録を退避しないと、前のログが消されてしまう可能性がありますので注意してください。

28.1.8 SNMP マネージャとの接続時の注意事項

(1) MIB 情報収集周期のチューニング

SNMP マネージャは、ネットワーク上の新しい装置を検出したり、トラフィック状況を監視したりするため、SNMP エージェントサポート機器から定期的に MIB を取得します。この定期的な MIB 取得の間隔が短いと、ネットワーク機器やネットワークに負荷が掛かります。また、装置の状態や構成などによって、MIB 取得時にマネージャ側でタイムアウトが発生するおそれがあります。特に、次に示すケースでは応答タイムアウトの発生するおそれが高まります。

- 接続 SNMP マネージャ数が多い場合
本装置に SNMP マネージャが多数接続され、MIB 情報の収集が集中した場合。
- SNMP イベントが同時に多数発生している場合
本装置から大量にトラップまたはインフォームが発行されるような状態のときに、MIB を取得した場合や、本装置から発行されたトラップまたはインフォームに基づいて、並行して MIB を取得した場合。

応答タイムアウトが頻発する場合は、SNMP マネージャのポーリング周期や応答監視タイマ値をチューニングしてください。代表的な SNMP マネージャのチューニングパラメータには、次の三つがあります。

- ポーリング周期
- 応答監視タイマ
- 応答監視タイムアウト時のリトライ回数

28.2 コンフィグレーション

28.2.1 コンフィグレーションコマンド一覧

SNMP/RMON 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 28-4 コンフィグレーションコマンド一覧

コマンド名	説明
hostname	本装置のホスト名称を設定します。本設定は RFC1213 の sysName に対応します。
rmon alarm	RMON (RFC1757) アラームグループの制御情報を設定します。
rmon collection history	RMON (RFC1757) イーサネットの統計来歴の制御情報を設定します。
rmon event	RMON (RFC1757) イベントグループの制御情報を設定します。
snmp-server community	SNMP コミュニティに対するアクセスリストを設定します。
snmp-server contact	本装置の連絡先などを設定します。本設定は RFC1213 の sysContact に対応します。
snmp-server engineID local	SNMP エンジン ID 情報を設定します。
snmp-server group	SNMP セキュリティグループ情報を設定します。
snmp-server host	トラップまたはインフォームを送信するネットワーク管理装置 (SNMP マネージャ) を登録します。
snmp-server informs	インフォームの再送条件を設定します。
snmp-server location	本装置を設置する場所の名称を設定します。本設定は RFC1213 の sysLocation に対応します。
snmp-server traps	トラップまたはインフォームの発行契機を設定します。
snmp-server user	SNMP セキュリティユーザ情報を設定します。
snmp-server view	MIB ビュー情報を設定します。
snmp trap link-status	回線がリンクアップまたはダウンした場合に、トラップまたはインフォーム (SNMP link down および up Trap) の送信を抑制します。

28.2.2 SNMPv1 , SNMPv2C による MIB アクセス許可の設定

[設定のポイント]

SNMP マネージャから本装置の MIB へのアクセスを許可するための設定をします。

[コマンドによる設定]

1. (config)# access-list 1 permit 10.1.1.1 0.0.0.0
IP アドレス 10.1.1.1 からのアクセスを許可するアクセスリストの設定を行います。
2. (config)# snmp-server community "NETWORK" ro 1
SNMP マネージャのコミュニティに対する MIB アクセスモードおよび適用するアクセスリストを設定します。
 - コミュニティ名 : NETWORK
 - アクセスリスト : 1
 - アクセスモード : read only

28.2.3 SNMPv3 による MIB アクセス許可の設定

[設定のポイント]

SNMPv3 で MIB にアクセスするために、アクセスを許可する MIB オブジェクトの集合を MIB ビューとして設定し、ユーザ認証とプライバシー機能の情報を SNMP セキュリティユーザとして設定します。また、MIB ビューと SNMP セキュリティユーザを関連づけるために、SNMP セキュリティグループを設定します。

[コマンドによる設定]

- ```
(config)# snmp-server view "READ_VIEW" 1.3.6.1 included
(config)# snmp-server view "READ_VIEW" 1.3.6.1.6.3 excluded
(config)# snmp-server view "WRITE_VIEW" 1.3.6.1.2.1.1 included
```

 MIB ビューを設定します。
  - ビュー名 READ\_VIEW に internet グループ MIB (サブツリー : 1.3.6.1) を登録します。
  - ビュー名 READ\_VIEW から snmpModules グループ MIB (サブツリー : 1.3.6.1.6.3) を対象外にします。
  - ビュー名 WRITE\_VIEW に system グループ MIB (サブツリー : 1.3.6.1.2.1.1) を登録します。
- ```
(config)# snmp-server user "ADMIN" "ADMIN_GROUP" v3 auth md5 "ABC*_1234" priv
des "XYZ/+6789"
```

 SNMP セキュリティユーザを設定します。
 - SNMP セキュリティユーザ名 : ADMIN
 - SNMP セキュリティグループ名 : ADMIN_GROUP
 - 認証プロトコル : HMAC-MD5
 - 認証パスワード : ABC*_1234
 - 暗号化プロトコル : CBC-DES
 - 暗号化パスワード : XYZ/+6789
- ```
(config)# snmp-server group "ADMIN_GROUP" v3 priv read "READ_VIEW" write
"WRITE_VIEW"
```

 SNMP セキュリティグループを設定します。
  - SNMP セキュリティグループ名 : ADMIN\_GROUP
  - セキュリティレベル : 認証あり, 暗号化あり
  - Read ビュー名 : READ\_VIEW
  - Write ビュー名 : WRITE\_VIEW

### 28.2.4 SNMPv1 , SNMPv2C によるトラップ送信の設定

#### [ 設定のポイント ]

トラップを発行する SNMP マネージャを登録します。

#### [ コマンドによる設定 ]

1. (config)# snmp-server host 10.1.1.1 traps "NETWORK" version 1 snmp  
SNMP マネージャに標準トラップを発行する設定をします。
  - コミュニティ名：NETWORK
  - SNMP マネージャの IP アドレス：10.1.1.1
  - 発行するトラップ：coldStart , warmStart , linkDown , linkUp , authenticationFailure

## 28.2.5 SNMPv3 によるトラップ送信の設定

### [ 設定のポイント ]

MIB ビューと SNMP セキュリティユーザを設定の上、SNMP セキュリティグループを設定し、さらに SNMP トラップモードを設定します。

### [ コマンドによる設定 ]

1. (config)# snmp-server view "ALL\_TRAP\_VIEW" \* included  
MIB ビューを設定します。
  - ビュー名 ALL\_TRAP\_VIEW に全サブツリーを登録します。
2. (config)# snmp-server user "ADMIN" "ADMIN\_GROUP" v3 auth md5 "ABC\*\_1234" priv des "XYZ/+6789"  
SNMP セキュリティユーザを設定します。
  - SNMP セキュリティユーザ名：ADMIN
  - SNMP セキュリティグループ名：ADMIN\_GROUP
  - 認証プロトコル：HMAC-MD5
  - 認証パスワード：ABC\*\_1234
  - 暗号化プロトコル：DES
  - 暗号化パスワード：XYZ/+6789
3. (config)# snmp-server group "ADMIN\_GROUP" v3 priv notify "ALL\_TRAP\_VIEW"  
SNMP セキュリティグループを設定します。
  - SNMP セキュリティグループ名：ADMIN\_GROUP
  - セキュリティレベル：認証あり、暗号化あり
  - Notify ビュー名：ALL\_TRAP\_VIEW
4. (config)# snmp-server host 10.1.1.1 traps "ADMIN" version 3 priv snmp  
SNMPv3 によって SNMP マネージャに標準トラップを発行する設定をします。
  - SNMP マネージャの IP アドレス：10.1.1.1
  - SNMP セキュリティユーザ名：ADMIN
  - セキュリティレベル：認証あり、暗号化あり
  - 発行するトラップ：coldStart , warmStart , linkDown , linkUp , authenticationFailure

## 28.2.6 SNMPv2C によるインフォーム送信の設定

### [ 設定のポイント ]

インフォームを発行する SNMP マネージャを登録します。

[ コマンドによる設定 ]

1. (config)# snmp-server host 10.1.1.1 informs "NETWORK" version 2c snmp

SNMP マネージャに標準のインフォームを発行する設定をします。

- コミュニティ名 : NETWORK
- SNMP マネージャの IP アドレス : 10.1.1.1
- 発行するインフォーム : coldStart , warmStart , linkDown , linkUp , authenticationFailure

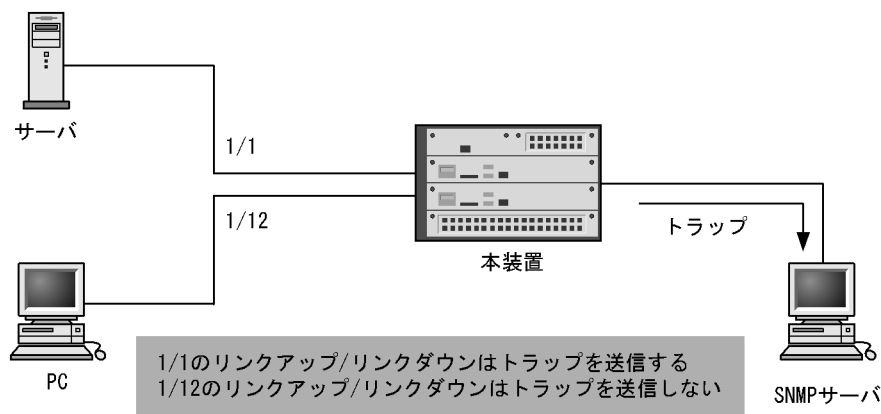
## 28.2.7 リンクトラップの抑止

本装置は、デフォルト動作としてイーサネットインタフェースがリンクアップまたはリンクダウンしたときに、SNMP トラップまたはインフォームを発行します。また、コンフィグレーションによって、イーサネットインタフェースごとに、リンクトラップの送信抑止を設定できます。例えば、サーバと接続する回線のように重要度の高い回線だけトラップまたはインフォームを送信し、そのほかの回線のリンクトラップの送信を抑止することで、本装置、ネットワーク、および SNMP マネージャの不要な処理を削減できます。

[ 設定のポイント ]

リンクトラップの設定内容はネットワーク全体の運用方針に従って決定します。

図 28-31 リンクトラップの構成図



ここでは、ポート 1/1 については、トラップまたはインフォームを送信するので、コンフィグレーションの設定は必要ありません。ポート 1/12 については、トラップまたはインフォームを送信しないように設定します。

[ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/12

(config-if)# no snmp trap link-status

リンクアップ/リンクダウン時にトラップまたはインフォームを送信しません。

2. (config-if)# exit

## 28.2.8 RMON イーサネットヒストリグループの制御情報の設定

### [ 設定のポイント ]

RMON (RFC1757) イーサネットの統計来歴の制御情報を設定します。本コマンドでは最大 32 エントリの設定ができます。あらかじめ SNMP マネージャを登録しておく必要があります。

### [ コマンドによる設定 ]

1. (config)# interface gigabitethernet 1/5

ギガビット・イーサネットインタフェース 1/5 のインタフェースモードに遷移します。

2. (config-if)# rmon collection history controlEntry 33 owner "NET-MANAGER"  
buckets 10

統計来歴の制御情報の情報識別番号、設定者の識別情報、および統計情報を格納する来歴エントリ数を設定します。

- 情報識別番号：33
- 来歴情報の取得エントリ：10 エントリ
- 設定者の識別情報："NET-MANAGER"

## 28.2.9 RMON による特定 MIB 値の閾値チェック

### [ 設定のポイント ]

特定の MIB の値に対して定期的に閾値チェックを行い、閾値を超えたら SNMP マネージャにイベントを通知するように設定します。

イベント実行方法に trap を指定する場合は、あらかじめ SNMP トラップモードの設定が必要です。

### [ コマンドによる設定 ]

1. (config)# rmon event 3 log trap public

アラームが発生したときに実行するイベントを設定します。

- 情報識別番号：3
- イベント実行方法：log, trap
- Trap 送信コミュニティ名：public

2. (config)# rmon alarm 12 "ifOutDiscards.3" 256111 delta rising-threshold 400000  
rising-event-index 3 falling-threshold 100 falling-event-index 3 owner  
"NET-MANAGER"

RMON アラームグループの制御情報を次の条件で設定します。

- RMON アラームグループの制御情報識別番号：12
- 閾値チェックを行う MIB のオブジェクト識別子：ifOutDiscards.3
- 閾値チェックを行う時間間隔：256111 秒
- 閾値チェック方式：差分値チェック (delta)
- 上方閾値の値：400000
- 上方閾値を超えたときのイベント方法の識別番号：3
- 下方閾値の値：100
- 下方閾値を超えたときのイベント方法の識別番号：3
- コンフィグレーション設定者の識別情報：NET-MANAGER

## 28.2.10 SNMPv1 , SNMPv2C による VRF からの MIB アクセス許可の設定【OP-NPAR】

### [ 設定のポイント ]

VRF に存在する SNMP マネージャから本装置の MIB へのアクセスを許可するための設定をします。

### [ コマンドによる設定 ]

1. (config)# access-list 2 permit 10.1.1.1 0.0.0.0  
IP アドレス 10.1.1.1 からのアクセスを許可するアクセスリストを設定します。
2. (config)# snmp-server community "NETWORK" ro 2 vrf 2  
SNMP マネージャのコミュニティに対する MIB アクセスモードおよび適用するアクセスリストを設定します。
  - コミュニティ名 : NETWORK
  - アクセスリスト : 2
  - アクセスモード : read only
  - VRF ID : 2

## 28.2.11 SNMPv3 による VRF からの MIB アクセス許可の設定【OP-NPAR】

### [ 設定のポイント ]

SNMPv3 で MIB にアクセスするために、アクセスを許可する MIB オブジェクトの集合を MIB ビューとして設定し、ユーザ認証とプライバシー機能の情報、およびアクセスを許可する VRF ID を SNMP セキュリティユーザとして設定します。また、MIB ビューと SNMP セキュリティユーザを関連づけるために、SNMP セキュリティグループを設定します。

### [ コマンドによる設定 ]

1. (config)# snmp-server view "READ\_VIEW" 1.3.6.1 included  
(config)# snmp-server view "READ\_VIEW" 1.3.6.1.6.3 excluded  
(config)# snmp-server view "WRITE\_VIEW" 1.3.6.1.2.1.1 included  
MIB ビューを設定します。
  - ビュー名 READ\_VIEW に internet グループ MIB (サブツリー : 1.3.6.1) を登録します。
  - ビュー名 READ\_VIEW から snmpModules グループ MIB (サブツリー : 1.3.6.1.6.3) を対象外にします。
  - ビュー名 WRITE\_VIEW に system グループ MIB (サブツリー : 1.3.6.1.2.1.1) を登録します。
2. (config)# snmp-server user "ADMIN" "ADMIN\_GROUP" v3 auth md5 "ABC\*\_1234" priv des "XYZ/+6789" vrf 2  
SNMP セキュリティユーザを設定します。
  - SNMP セキュリティユーザ名 : ADMIN
  - SNMP セキュリティグループ名 : ADMIN\_GROUP
  - 認証プロトコル : HMAC-MD5
  - 認証パスワード : ABC\*\_1234
  - 暗号化プロトコル : CBC-DES

- 暗号化パスワード：XYZ/+6789
- VRF ID：2

3. (config)# snmp-server group "ADMIN\_GROUP" v3 priv read "READ\_VIEW" write "WRITE\_VIEW"

SNMP セキュリティグループを設定します。

- SNMP セキュリティグループ名：ADMIN\_GROUP
- セキュリティレベル：認証あり，暗号化あり
- Read ビュー名：READ\_VIEW
- Write ビュー名：WRITE\_VIEW

## 28.2.12 SNMPv1 , SNMPv2C による VRF へのトラップ送信の設定【OP-NPAR】

[ 設定のポイント ]

VRF に存在する SNMP マネージャに対して，トラップを発行する設定をします。

[ コマンドによる設定 ]

1. (config)# snmp-server host 10.1.1.1 vrf 2 traps "NETWORK" version 1 snmp

SNMP マネージャに標準トラップを発行する設定をします。

- コミュニティ名：NETWORK
- SNMP マネージャの IP アドレス：10.1.1.1
- 発行するトラップ：coldStart , warmStart , linkDown , linkUp , authenticationFailure
- VRF ID：2

## 28.2.13 SNMPv3 による VRF へのトラップ送信の設定【OP-NPAR】

[ 設定のポイント ]

MIB ビューと SNMP セキュリティユーザを設定の上，SNMP セキュリティグループを設定し，さらに SNMP トラップモードを設定します。SNMP セキュリティユーザで登録する VRF ID と SNMP トラップモードで設定する VRF ID は，同一である必要があります。

[ コマンドによる設定 ]

1. (config)# snmp-server view "ALL\_TRAP\_VIEW" \* included

MIB ビューを設定します。

- ビュー名 ALL\_TRAP\_VIEW に全サブツリーを登録します。

2. (config)# snmp-server user "ADMIN" "ADMIN\_GROUP" v3 auth md5 "ABC\*\_1234" priv des "XYZ/+6789" vrf 2

SNMP セキュリティユーザを設定します。

- SNMP セキュリティユーザ名：ADMIN
- SNMP セキュリティグループ名：ADMIN\_GROUP
- 認証プロトコル：HMAC-MD5

- 認証パスワード：ABC\*\_1234
  - 暗号化プロトコル：DES
  - 暗号化パスワード：XYZ/+6789
  - VRF ID：2
3. (config)# snmp-server group "ADMIN\_GROUP" v3 priv notify "ALL\_TRAP\_VIEW"  
SNMP セキュリティグループを設定します。
- SNMP セキュリティグループ名：ADMIN\_GROUP
  - セキュリティレベル：認証あり，暗号化あり
  - Notify ビュー名：ALL\_TRAP\_VIEW
4. (config)# snmp-server host 10.1.1.1 vrf 2 traps "ADMIN" version 3 priv snmp  
SNMPv3 によって SNMP マネージャに標準トラップを発行する設定をします。
- SNMP マネージャの IP アドレス：10.1.1.1
  - SNMP セキュリティユーザ名：ADMIN
  - セキュリティレベル：認証あり，暗号化あり
  - 発行するトラップ：coldStart , warmStart , linkDown , linkUp , authenticationFailure
  - VRF ID：2

## 28.2.14 SNMPv2C による VRF へのインフォーム送信の設定 【OP-NPAR】

### [ 設定のポイント ]

VRF に存在する SNMP マネージャに対して，インフォームを発行する設定をします。

### [ コマンドによる設定 ]

1. (config)# snmp-server host 10.1.1.1 vrf 2 informs "NETWORK" version 2c snmp  
SNMP マネージャに標準のインフォームを発行する設定をします。
- コミュニティ名：NETWORK
  - SNMP マネージャの IP アドレス：10.1.1.1
  - 発行するインフォーム：coldStart , warmStart , linkDown , linkUp , authenticationFailure
  - VRF ID：2

## 28.3 オペレーション

### 28.3.1 運用コマンド一覧

SNMP/RMON に関する運用コマンド一覧を次の表に示します。

表 28-5 運用コマンド一覧

| コマンド名             | 説明                                                    |
|-------------------|-------------------------------------------------------|
| show snmp         | SNMP 情報を表示します。                                        |
| show snmp pending | 送信を保留中のインフォームリクエストを表示します。                             |
| snmp lookup       | サポート MIB オブジェクト名称およびオブジェクト ID を表示します。                 |
| snmp get          | 指定した MIB の値を表示します。                                    |
| snmp getnext      | 指定した次の MIB の値を表示します。                                  |
| snmp walk         | 指定した MIB ツリーを表示します。                                   |
| snmp getif        | interface グループの MIB 情報を表示します。                         |
| snmp getroute     | ipRouteTable (IP ルーティングテーブル) を表示します。                  |
| snmp getarp       | ipNetToMediaTable (IP アドレス変換テーブル) を表示します。             |
| snmp getforward   | ipForwardTable (IP フォワーディングテーブル) を表示します。              |
| snmp rget         | 指定したリモート装置の MIB の値を表示します。                             |
| snmp rgetnext     | 指定したリモート装置の次の MIB の値を表示します。                           |
| snmp rwalk        | 指定したリモート装置の MIB ツリーを表示します。                            |
| snmp rgetroute    | 指定したリモート装置の ipRouteTable (IP ルーティングテーブル) を表示します。      |
| snmp rgetarp      | 指定したリモート装置の ipNetToMediaTable (IP アドレス変換テーブル) を表示します。 |

### 28.3.2 SNMP マネージャとの通信の確認

本装置に SNMP エージェント機能を設定して SNMP プロトコルによるネットワーク管理を行う場合、次のことを確認してください。

ネットワーク上の SNMP マネージャから本装置に対して MIB を取得できること

本装置からネットワーク上の SNMP マネージャへ SNMP のトラップまたはインフォームが送信されていること、さらに、インフォームの場合は応答を受信できること

show snmp コマンドで SNMP マネージャとの通信状態を確認できます。



図 28-32 show snmp コマンドの実行結果

```

> show snmp
Date 2011/12/27 15:06:08 UTC
Contact: Suzuki@example.com
Location: ServerRoom
SNMP packets input : 137 (get:417 set:2)
 Get-request PDUs : 18
 Get-next PDUs : 104
 Get-bulk PDUs : 0
 Set-request PDUs : 6
 Response PDUs : 3 (with error 0)
 Error PDUs : 7
 Bad SNMP version errors: 1
 Unknown community name : 5
 Illegal operation : 1
 Encoding errors : 0

SNMP packets output : 185
 Trap PDUs : 4
 Inform-request PDUs : 53
 Response PDUs : 128 (with error 4)
 No errors : 124
 Too big errors : 0
 No such name errors : 3
 Bad values errors : 1
 General errors : 0
 Timeouts : 49
 Drops : 0

[TRAP]
Host: 192.168.0.1, sent:1
Host: 192.168.0.2, sent:3

[INFORM]
Timeout(sec) : 10
Retry : 5
Pending informs : 1/25 (current/max)
Host: 192.168.0.3
 sent :8 retries:26
 response:2 pending:1 failed:5 dropped:0
Host: 192.168.0.4
 sent :3 retries:15
 response:0 pending:0 failed:3 dropped:0
Host: 2001:db8::10
 sent :1 retries:0
 response:1 pending:0 failed:0 dropped:0

```

SNMP マネージャから MIB が取得できない場合は、「SNMP packets input」の項目で、「Error PDUs」の値が増加していないこと、および PDU を受信できていることを確認してください。「Error PDUs」の値が増加しているときは、コンフィグレーションの内容を確認してください。PDU を受信できていないときは、ネットワークの設定が正しいか、また、SNMP マネージャまでの経路上で障害が発生していないかを確認してください。

SNMP マネージャでトラップまたはインフォームが受信できない場合は、「[TRAP]」と「[INFORM]」の項目で、SNMP マネージャの IP アドレスが「Host」として設定されていることを確認してください。設定されていないときは、コンフィグレーションコマンド snmp-server host を実行して、SNMP マネージャに関する情報を設定してください。

なお、これらの方法で解決できない場合はマニュアル「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、本装置から取得できる MIB、トラップおよびインフォームについてはマニュアル「MIB レファレンス」を参照してください。



# 29 ログ出力機能

この章では、本装置のログ出力機能について説明します。

---

29.1 解説

---

29.2 コンフィグレーション

---

## 29.1 解説

---

本装置では動作情報や障害情報などを運用メッセージとして通知します。同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います。装置管理者は、表示コマンドでこれらの情報を参照できます。

採取した本装置のログ情報は、syslog インタフェースを使用して syslog 機能を持つネットワーク上の他装置（UNIX ワークステーションなど）に送ることができます<sup>1</sup>、<sup>2</sup>。また、同様に、ログ情報を E-Mail を使用してネットワーク上の他装置に送ることもできます。これらのログ出力機能を使用することで、多数の装置を管理する場合にログの一元管理ができるようになります。また、ログ情報を E-Mail で送信することもできます。

### 注 1

他装置からの syslog メッセージを受信する機能はサポートしていません。

### 注 2

本装置で生成した syslog メッセージでは、RFC3164 で定義されている HEADER 部の HOSTNAME 欄は未設定です。

## 29.2 コンフィグレーション

### 29.2.1 コンフィグレーションコマンド一覧

ログ出力機能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 29-1 コンフィグレーションコマンド一覧 (syslog 出力に関する設定)

| コマンド名              | 説明                                        |
|--------------------|-------------------------------------------|
| logging event-kind | syslog サーバに送信対象とするログ情報のイベント種別を設定します。      |
| logging facility   | ログ情報を syslog インタフェースで出力するためのファシリティを設定します。 |
| logging host       | ログ情報の出力先を設定します。                           |
| logging trap       | syslog サーバに送信対象とするログ情報の重要度を設定します。         |

表 29-2 コンフィグレーションコマンド一覧 (E-Mail 出力に関する設定)

| コマンド名                    | 説明                                       |
|--------------------------|------------------------------------------|
| logging email            | ログ情報を E-Mail で出力するための E-Mail アドレスを設定します。 |
| logging email-event-kind | E-Mail で出力対象とするログ情報のイベント種別を設定します。        |
| logging email-from       | ログ情報を E-Mail で出力する E-Mail の送信元を設定します。    |
| logging email-interval   | ログ情報を E-Mail で出力するための送信間隔を設定します。         |
| logging email-server     | ログ情報を E-Mail で出力するため SMTP サーバの情報を設定します。  |

### 29.2.2 ログの syslog 出力の設定

#### [ 設定のポイント ]

syslog 出力機能を使用して、採取したログ情報を syslog サーバに送信するための設定をします。

#### [ コマンドによる設定 ]

1. (config)# logging host LOG\_HOST  
ログをホスト名 LOG\_HOST 宛てに出力するように設定します。

### 29.2.3 ログの VRF への syslog 出力の設定

#### [ 設定のポイント ]

syslog 出力機能を使用して、採取したログ情報を VRF に存在する syslog サーバに送信するための設定をします。

VRF を指定する場合には、ログ出力先を IPv4 アドレスまたは IPv6 アドレスで指定する必要があります。ホスト名で指定した場合は、VRF を指定できません。

#### [ コマンドによる設定 ]

1. (config)# logging host 128.1.1.2 vrf 2  
ログを IP アドレス 128.1.1.2、VRF ID 2 宛てに出力するように設定します。

## 29.2.4 ログの E-Mail 出力の設定

[ 設定のポイント ]

E-Mail 送信機能を使用して、採取したログ情報をリモートホスト、PC などに送信するための設定をします。

[ コマンドによる設定 ]

1. `(config)# logging email system@loghost`  
送信先のメールアドレスとして `system@loghost` を設定します。

# 30 sFlow 統計（フロー統計）機能

この章では、本装置を中継するパケットのトラフィック特性を分析する機能である sFlow 統計の解説と操作方法について説明します。

---

30.1 解説

---

30.2 コンフィグレーション

---

30.3 オペレーション

---

## 30.1 解説

### 30.1.1 sFlow 統計の概要

sFlow 統計はエンド - エンドのトラフィック (フロー) 特性や隣接するネットワーク単位のトラフィック特性を分析するため、ネットワークの上を流れるトラフィックを中継装置 (ルータやスイッチ) でモニターする機能です。sFlow 統計は国際的に公開されているフロー統計プロトコル (RFC3176) で、レイヤ 2 からレイヤ 7 までの統計情報をサポートしています。sFlow 統計情報 (以降, sFlow パケット) を受け取って表示する装置を sFlow コレクタ (以降, コレクタ) と呼び、コレクタに sFlow パケットを送付する装置を sFlow エージェント (以降, エージェント) と呼びます。sFlow 統計を使ったネットワーク構成例を次の図に示します。

図 30-1 sFlow 統計のネットワーク構成例

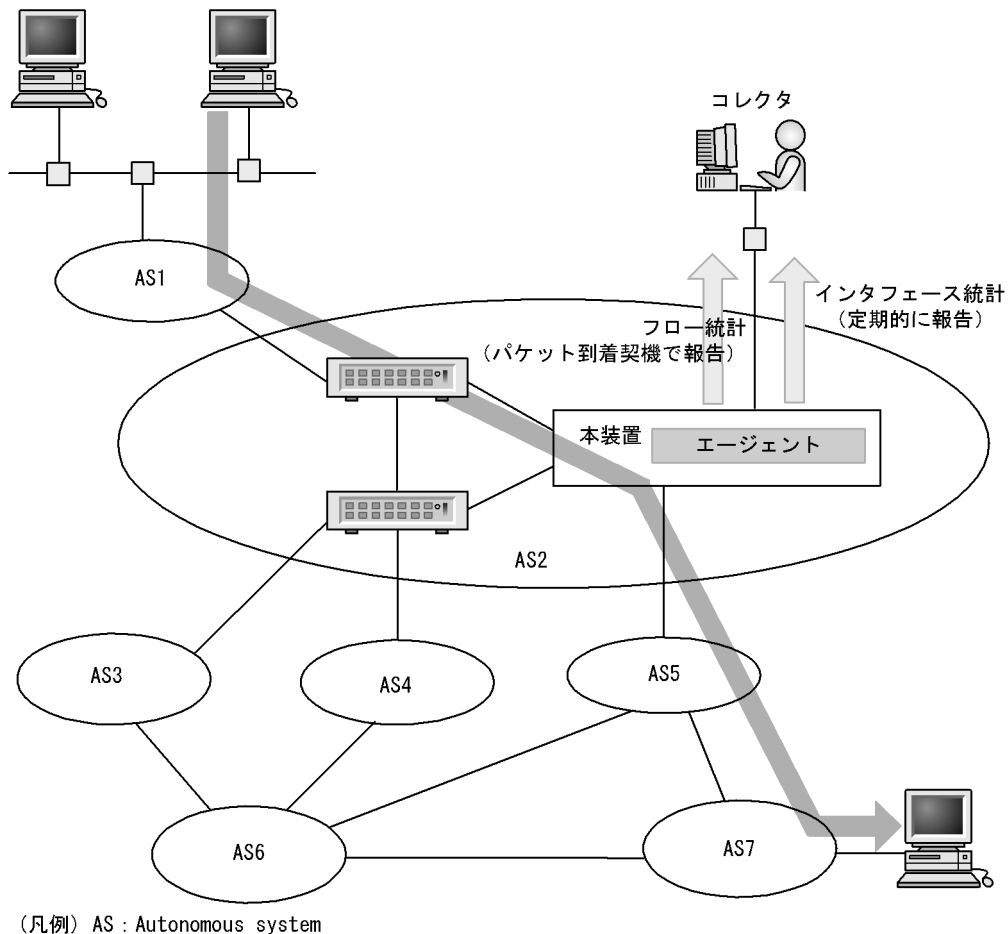
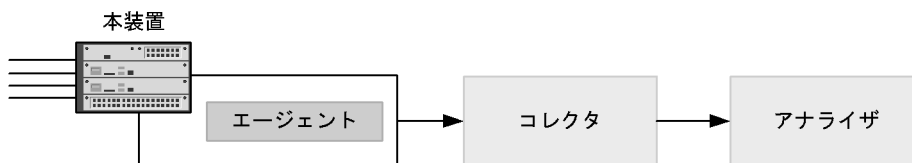


図 30-2 システム構成





本装置のエージェントでモニタされた情報はコレクタに集められ、統計結果をアナライザによってグラフィカルに表示できます。したがって、sFlow 統計機能を利用するにはコレクタとアナライザが必要です。

表 30-1 システム構成要素

| 構成要素        | 役割                                                   |
|-------------|------------------------------------------------------|
| エージェント（本装置） | 統計情報を収集してコレクタに送付します。                                 |
| コレクタ        | エージェントから送付される統計情報を集計・編集・表示します。さらに、編集データをアナライザに送付します。 |
| アナライザ       | コレクタから送付されるデータをグラフィカルに表示します。                         |

注 アナライザと一緒にしている場合もあります。

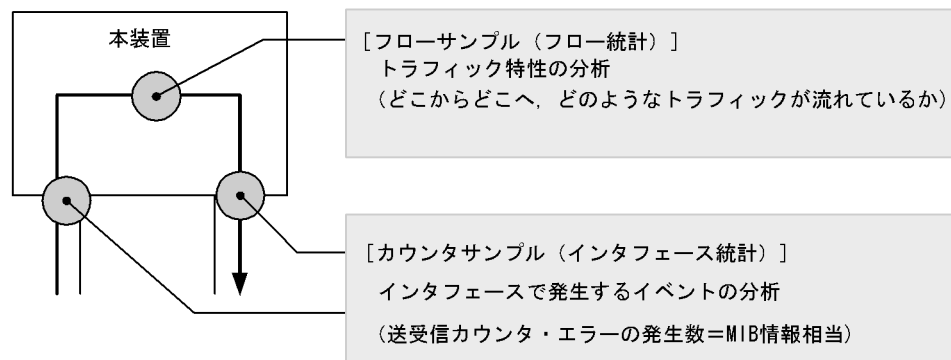
### 30.1.2 sFlow 統計エージェント機能

本装置のエージェントには、次の二つの機能があります。

- ・フロー統計（sFlow 統計ではフローサンプルと呼びます。以降、この名称で表記します。）作成機能
- ・インタフェース統計（sFlow 統計ではカウンタサンプルと呼びます。以降、この名称で表記します。）作成機能

フローサンプル作成機能は送受信パケット（フレーム）をユーザ指定の割合でサンプリングし、パケット情報を加工してフローサンプル形式でコレクタに送信する機能です。カウンタサンプル作成機能はインタフェース統計をカウンタサンプル形式でコレクタに送信する機能です。それぞれの収集個所と収集内容を次の図に示します。

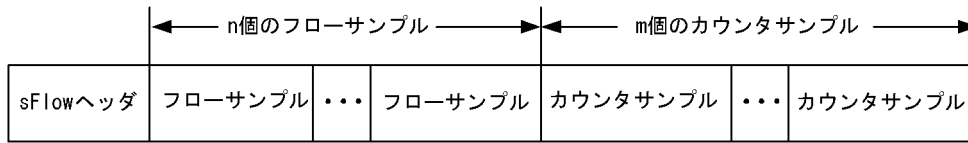
図 30-3 フローサンプルとカウンタサンプル



### 30.1.3 sFlow パケットフォーマット

本装置がコレクタに送信する sFlow パケット（フローサンプルパケットとカウンタサンプルパケット）について説明します。コレクタに送信するフォーマットは RFC3176 で規定されています。sFlow パケットのフォーマットを次の図に示します。

図 30-4 sFlow パケットフォーマット



(1) sFlow ヘッダ

sFlow ヘッダへ設定される内容を次の表に示します。

表 30-2 sFlow ヘッダのフォーマット

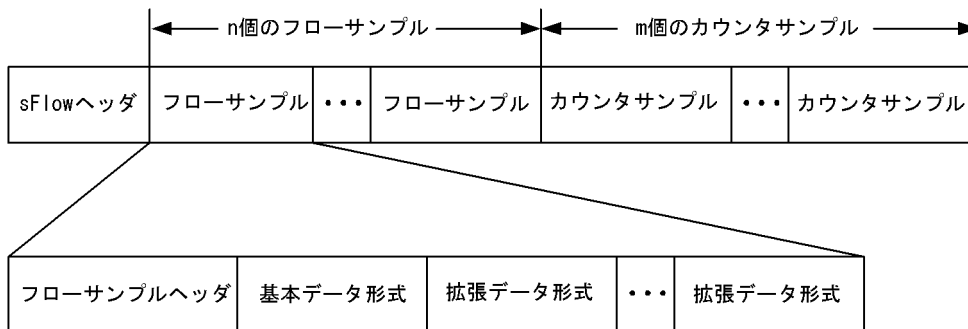
| 設定項目           | 説明                                                                                 | サポート |
|----------------|------------------------------------------------------------------------------------|------|
| バージョン番号        | sFlow パケットのバージョン (バージョン 2, 4 をサポート)                                                |      |
| アドレスタイプ        | エージェントの IP タイプ (IPv4=1, IPv6=2)                                                    |      |
| エージェント IP アドレス | エージェントの IP アドレス                                                                    |      |
| シーケンス番号        | sFlow パケットの生成ごとに増加する番号                                                             |      |
| 生成時刻           | 現在の時間 (装置の起動時からのミリセカンド)                                                            |      |
| サンプル数          | この信号に含まれるサンプリング (フロー・カウンタ) したパケット数 (「図 30-4 sFlow パケットフォーマット」の例では $n + m$ が設定されます) |      |

(凡例) : サポートする

(2) フローサンプル

フローサンプルとは、受信パケットのうち、他装置へ転送または本装置宛てと判定されるパケットの中から一定のサンプリング間隔でパケットを抽出し、コレクタに送信するためのフォーマットです。フローサンプルにはモニタしたパケットに加えて、パケットには含まれていない情報 (受信インタフェース, 送信インタフェース, AS 番号など) も収集するため、詳細なネットワーク監視ができます。フローサンプルのフォーマットを次の図に示します。

図 30-5 フローサンプルのフォーマット



(a) フローサンプルヘッダ

フローサンプルヘッダへ設定する内容を次の表に示します。

表 30-3 フローサンプルヘッダのフォーマット

| 設定項目            | 説明                                                                                                                                                        | サポート |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| sequence_number | フローサンプルの生成ごとに増加する番号                                                                                                                                       |      |
| source_id       | フローサンプルの装置内の発生源（受信インタフェース）を表す SNMP Interface Index                                                                                                        |      |
| sampling_rate   | フローサンプルのサンプリング間隔                                                                                                                                          |      |
| sample_pool     | インタフェースに到着したパケットの総数                                                                                                                                       |      |
| drops           | 廃棄したフローサンプルの総数                                                                                                                                            |      |
| input           | 受信インタフェースの SNMP Interface Index。<br>インタフェースが不明な場合 0 を設定                                                                                                   |      |
| output          | 送信インタフェースの SNMP Interface Index <sup>1 2</sup> 。<br>送信インタフェースが不明な場合は 0 を設定。<br>送信インタフェースが複数の場合（マルチキャストなど）は最上位ビットを立て、下位ビットが送信インタフェースの数を示します <sup>3</sup> 。 |      |

（凡例） : サポートする

注 1 ソフトウェア中継の場合は 0 になります。

注 2 フラディングパケットが対象になった場合は 0 が収集されます。

注 3 未サポートのため、下位ビットは 0 固定です。

#### （b）基本データ形式

基本データ形式はヘッダ型、IPv4 型および IPv6 型の 3 種類があり、このうち一つだけ設定できます。基本データ形式のデフォルト設定はヘッダ型です。IPv4 型、IPv6 型を使用したい場合はコンフィグレーションコマンドで設定してください。各形式のフォーマットを以降の表に示します。

表 30-4 ヘッダ型のフォーマット

| 設定項目                    | 説明                                | サポート |
|-------------------------|-----------------------------------|------|
| packet_information_type | 基本データ形式のタイプ（ヘッダ型=1）               |      |
| header_protocol         | ヘッダプロトコル番号（ETHERNET=1）            |      |
| frame_length            | オリジナルのパケット長                       |      |
| header_length           | オリジナルからサンプリングした分のパケット長（デフォルト 128） |      |
| header<>                | サンプリングしたパケットの内容                   |      |

（凡例） : サポートする

注 IP パケットとして解析ができない場合は、このフォーマットになります。

表 30-5 IPv4 型のフォーマット

| 設定項目                    | 説明                          | サポート |
|-------------------------|-----------------------------|------|
| packet_information_type | 基本データ形式のタイプ（IPv4 型=2）       |      |
| length                  | IPv4 パケットの長さ                |      |
| protocol                | IP プロトコルタイプ（例：TCP=6，UDP=17） |      |
| src_ip                  | 送信元 IP アドレス                 |      |
| dst_ip                  | 宛先 IP アドレス                  |      |
| src_port                | 送信元ポート番号                    |      |

| 設定項目      | 説明            | サポート |
|-----------|---------------|------|
| dst_port  | 宛先ポート番号       |      |
| tcp_flags | TCP フラグ       |      |
| TOS       | IP のタイプオブサービス |      |

(凡例) : サポートする

表 30-6 IPv6 型のフォーマット

| 設定項目                    | 説明                             | サポート |
|-------------------------|--------------------------------|------|
| packet_information_type | 基本データ形式のタイプ (IPv6 型 =3)        |      |
| length                  | 低レイヤを除いた IPv6 パケットの長さ          |      |
| protocol                | IP プロトコルタイプ (例: TCP=6, UDP=17) |      |
| src_ip                  | 送信元 IP アドレス                    |      |
| dst_ip                  | 宛先 IP アドレス                     |      |
| src_port                | 送信元ポート番号                       |      |
| dst_port                | 宛先ポート番号                        |      |
| tcp_flags               | TCP フラグ                        |      |
| priority                | 優先度                            |      |

(凡例) : サポートする

(c) 拡張データ形式

拡張データ形式はスイッチ型・ルータ型・ゲートウェイ型・ユーザ型・URL 型の 5 種類があります。拡張データ形式のデフォルト設定ではすべての拡張形式を収集し、コレクタに送信します。本形式はコンフィグレーションにより変更可能です。各形式のフォーマットを以降の表に示します。

表 30-7 拡張データ形式の種別一覧

| 拡張データ種別 | 説明                                | サポート |
|---------|-----------------------------------|------|
| スイッチ型   | スイッチ情報 (VLAN 情報など) を収集する。         |      |
| ルータ型    | ルータ情報 (NextHop など) を収集する。         | 1 2  |
| ゲートウェイ型 | ゲートウェイ情報 (AS 番号など) を収集する。         | 1 2  |
| ユーザ型    | ユーザ情報 (TACACS/RADIUS 情報など) を収集する。 | 2    |
| URL 型   | URL 情報 (URL 情報など) を収集する。          | 2    |

(凡例) : サポートする

注 1 L2 中継時は sFlow パケットに収集されません。

注 2 2 段以上の VLAN Tag 付きフレームが対象になった場合は、sFlow パケットに収集されません。

表 30-8 スイッチ型のフォーマット

| 設定項目                      | 説明                     | サポート |
|---------------------------|------------------------|------|
| extended_information_type | 拡張データ形式のタイプ (スイッチ型 =1) |      |
| src_vlan                  | 受信パケットの 802.1Q VLAN ID |      |
| src_priority              | 受信パケットの 802.1p 優先度     |      |

| 設定項目         | 説明                     | サポート |
|--------------|------------------------|------|
| dst_vlan     | 送信パケットの 802.1Q VLAN ID | 1 2  |
| dst_priority | 送信パケットの 802.1p 優先度     | 3    |

（凡例） : サポートする

注 1 Tag 変換を使用している場合、変換前の値が収集されます。

注 2 フラディングパケットが対象になった場合は 0 が収集されます。

注 3 受信パケットの 802.1p 優先度と同じ値が収集されます。

表 30-9 ルータ型のフォーマット

| 設定項目                      | 説明                    | サポート |
|---------------------------|-----------------------|------|
| extended_information_type | 拡張データ形式のタイプ（ルータ型=2）   |      |
| nexthop_address_type      | 次の転送先ルータの IP アドレスタイプ  |      |
| nexthop                   | 次の転送先ルータの IP アドレス     |      |
| src_mask                  | 送信元アドレスのプレフィックスマスクビット |      |
| dst_mask                  | 宛先アドレスのプレフィックスマスクビット  |      |

（凡例） : サポートする

注 宛先アドレスへの経路がマルチパス経路の場合は 0 で収集されます。

表 30-10 ゲートウェイ型のフォーマット

| 設定項目                      | 説明                         | サポート |
|---------------------------|----------------------------|------|
| extended_information_type | 拡張データ形式のタイプ（ゲートウェイ型=3）     |      |
| as                        | 本装置の AS 番号                 |      |
| src_as                    | 送信元の AS 番号                 | 1    |
| src_peer_as               | 送信元への隣接 AS 番号              | 1 2  |
| dst_as_path_len           | AS 情報数（1 固定）               |      |
| dst_as_type               | AS 経路種別（2: AS_SEQUENCE）    |      |
| dst_as_len                | AS 数（2 固定）                 |      |
| dst_peer_as               | 宛先への隣接 AS 番号               | 1    |
| dst_as                    | 宛先の AS 番号                  | 1    |
| communities<>             | 本経路に関するコミュニティ <sup>3</sup> | ×    |
| localpref                 | 本経路に関するローカル優先 <sup>3</sup> | ×    |

（凡例） : サポートする × : サポートしない

注 1 送受信先がダイレクト経路は AS 番号が 0 で収集されます。

注 2 本装置から送信元へパケットを送信する場合に隣接 AS 番号として扱っている値が本フィールドに入ります。本装置へ到着前に実際に通過した隣接 AS 番号と異なる場合があります。

注 3 未サポートのため 0 固定です。

表 30-11 ユーザ型のフォーマット

| 設定項目                      | 説明                               | サポート |
|---------------------------|----------------------------------|------|
| extended_information_type | 拡張データ形式のタイプ（ユーザ型=4） <sup>1</sup> |      |

| 設定項目         | 説明                      | サポート |
|--------------|-------------------------|------|
| src_user_len | 送信元のユーザ名の長さ             |      |
| src_user<>   | 送信元のユーザ名                |      |
| dst_user_len | 宛先のユーザ名の長さ <sup>2</sup> | ×    |
| dst_user<>   | 宛先のユーザ名 <sup>2</sup>    | ×    |

(凡例) : サポートする × : サポートしない

注 1 RADIUS は宛先 UDP ポート番号 1812, TACACS は宛先 UDP ポート番号 49 が対象となります。

注 2 未サポートのため 0 固定です

表 30-12 URL 型のフォーマット

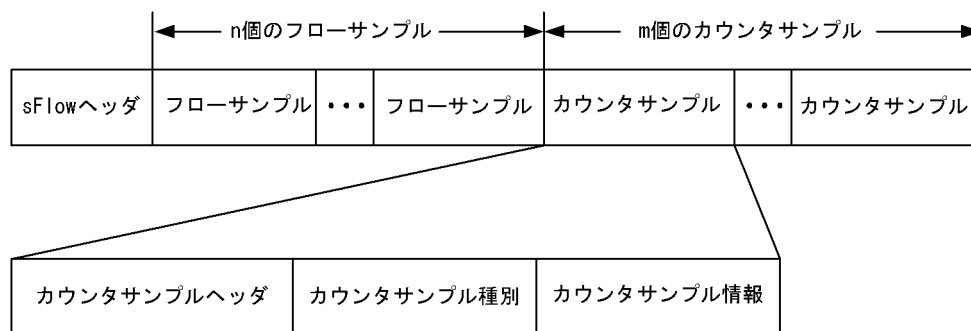
| 設定項目                      | 説明                                                     | サポート |
|---------------------------|--------------------------------------------------------|------|
| extended_information_type | 拡張データ形式のタイプ (URL 型 =5)                                 |      |
| url_direction             | URL 情報源<br>( source address=1, destination address=2 ) |      |
| url_len                   | URL 長                                                  |      |
| url<>                     | URL 内容                                                 |      |

(凡例) : サポートする

### (3) カウンタサンプル

カウンタサンプルは、インタフェース統計情報 (到着したパケット数や、エラーの数など) を送信します。また、インタフェースの種別よりコレクタに送信するフォーマットが決定されます。カウンタサンプルのフォーマットを次の図に示します。

図 30-6 カウンタサンプルのフォーマット



#### (a) カウンタサンプルヘッダ

カウンタサンプルヘッダへ設定される内容を次の表に示します。

表 30-13 カウンタサンプルヘッダのフォーマット

| 設定項目              | 説明                                                            | サポート |
|-------------------|---------------------------------------------------------------|------|
| sequence_number   | カウンタサンプルの生成ごとに増加する番号                                          |      |
| source_id         | カウンタサンプルの装置内の発生源 (特定のポート・VLAN ID) を表す<br>SNMP Interface Index |      |
| sampling_interval | コレクタへのカウンタサンプルの送信間隔                                           |      |

(凡例) : サポートする

### (b) カウンタサンプル種別

カウンタサンプル種別はインタフェースの種別ごとに分類され収集されます。カウンタサンプル種別として設定される内容を次の表に示します。

表 30-14 カウンタサンプル種別一覧

| 設定項目      | 説明                          | サポート |
|-----------|-----------------------------|------|
| GENERIC   | 一般的な統計 (counters_type=1)    | ×    |
| ETHERNET  | イーサネット統計 (counters_type=2)  |      |
| TOKENRING | トークンリング統計 (counters_type=3) | ×    |
| FDDI      | FDDI 統計 (counters_type=4)   | ×    |
| 100BaseVG | VG 統計 (counters_type=5)     | ×    |
| WAN       | WAN 統計 (counters_type=6)    | ×    |
| VLAN      | VLAN 統計 (counters_type=7)   |      |

(凡例) : サポートする × : サポートしない

注 本装置で未サポートなインタフェースタイプのためです。

### (c) カウンタサンプル情報

カウンタサンプル情報はカウンタサンプル種別により収集される内容が変わります。VLAN 統計以外は MIB で使われている統計情報 (RFC) に従って送信されます。カウンタサンプル情報として設定される内容を次の表に示します。

表 30-15 カウンタサンプル情報

| 設定項目      | 説明                                   | サポート |
|-----------|--------------------------------------|------|
| GENERIC   | 一般的な統計 [ RFC2233 参照 ]                | ×    |
| ETHERNET  | イーサネット統計 [ RFC2358 参照 ]              |      |
| TOKENRING | トークンリング統計 [ RFC1748 参照 ]             | ×    |
| FDDI      | FDDI 統計 [ RFC1512 参照 ]               | ×    |
| 100BaseVG | VG 統計 [ RFC2020 参照 ]                 | ×    |
| WAN       | WAN 統計 [ RFC2233 参照 ]                | ×    |
| VLAN      | VLAN 統計 [ 表 30-16 VLAN 統計のフォーマット参照 ] |      |

(凡例) : サポートする × : サポートしない

注 イーサネット統計のうち ifDirection, dot3StatsSymbolErrors は収集できません。

表 30-16 VLAN 統計のフォーマット

| 設定項目          | 説明           | サポート |
|---------------|--------------|------|
| vlan_id       | VLAN ID      |      |
| octets        | オクテット数       |      |
| ucastPkts     | ユニキャストパケット数  | 1    |
| multicastPkts | マルチキャストパケット数 | 2    |

| 設定項目          | 説明            | サポート |
|---------------|---------------|------|
| broadcastPkts | ブロードキャストパケット数 | 2    |
| discards      | 廃棄パケット数       | 3    |

(凡例) : サポートする

注 1 ユニキャストパケット数, マルチキャストパケット数, およびブロードキャストパケット数の合計値が入りません。

注 2 ユニキャストパケット数に含まれているため 0 固定です。

注 3 アクセスリストロギングの対象となった廃棄パケットは, VLAN 統計の廃棄パケット数にカウントされません。

### 30.1.4 本装置での sFlow 統計の動作について

#### (1) sFlow 統計収集の対象パケットに関する注意点

- 本装置での sFlow 統計は, 受信パケットと送信パケットを対象パケットとして扱います。
- 受信時に廃棄と判定されるパケット (フィルタ機能で廃棄判定されるパケットなど) は, sFlow 統計収集の対象外パケットとして扱います。ただし, QoS 機能の廃棄制御に従ってキューイング時に廃棄されるパケットは, sFlow 統計収集の対象パケットとして扱います。Null インタフェース宛てのパケットは収集可能です。
- sFlow 統計を有効にしているポートに対してアクセスリストロギングを有効にした場合, アクセスリストロギングの対象となった廃棄パケットは VLAN 統計の廃棄パケット数にカウントされなくなります。

#### (2) データ収集位置による注意点

- ingress 指定および egress 指定のどちらで検出されても, sFlow パケットの内容は本装置に入ってきた時点のパケット内容が収集されます (本装置内でパケット内容の変換などが行われても, sFlow パケットには反映されません)。
- 本装置での sFlow 統計は, 受信パケットまたは送信パケットをサンプリングしてコレクタに送信します。この性質上, 送信側にフィルタ機能や QoS 機能を設定してパケットを廃棄する条件でも, コレクタには中継しているように送信する場合があります。フィルタ機能や QoS 機能と併用するときは, パケットが廃棄される条件を確認して運用してください。他機能と併用時の sFlow 統計収集条件を次の表と図に示します。

表 30-17 他機能と併用時の sFlow 統計収集条件

| 機能                        | 受信パケットが sFlow 統計対象 | 送信パケットが sFlow 統計対象 |
|---------------------------|--------------------|--------------------|
| フィルタ機能 (受信側)              | 廃棄対象は収集されない        | 廃棄対象は収集されない        |
| QoS 機能 (受信側)              | 廃棄対象は収集されない        | 廃棄対象は収集されない        |
| フィルタ機能 (送信側) <sup>1</sup> | 廃棄対象でも収集される        | 廃棄対象は収集されない        |
| QoS 機能 (送信側) <sup>1</sup> | 廃棄対象でも収集される        | 廃棄対象は収集されない        |
| 自宛 (Null インタフェースなど)       | 収集される              | -                  |
| 自発 (本装置からの ping など)       | -                  | 収集される              |
| ポリシーベースルーティング             | 収集される <sup>2</sup> | 収集される <sup>2</sup> |

(凡例) - : 該当なし

注 1

sFlow パケットの内容は本装置に入ってきた時点のパケット内容が収集されます。

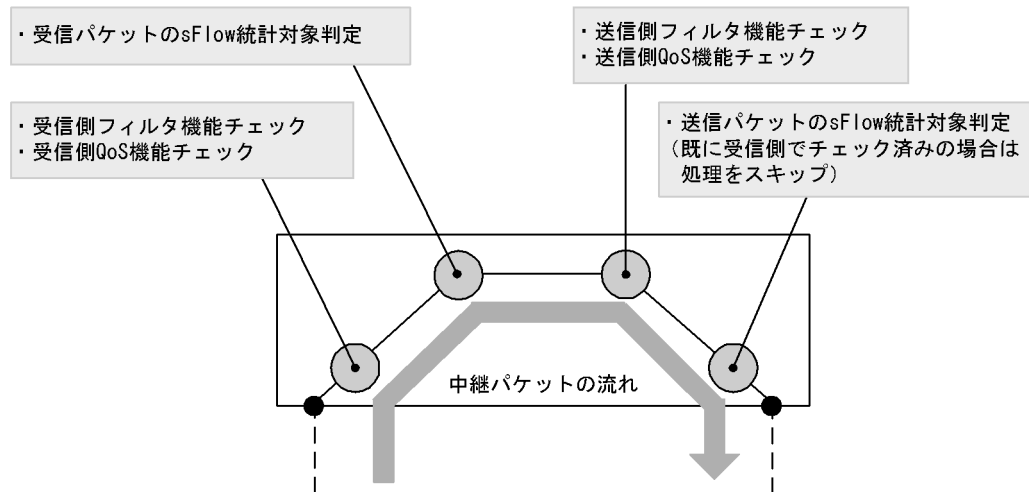
注 2



次の情報はポリシーベースルーティングによる中継先の経路情報ではなく、ルーティングプロトコルに従った中継先の経路情報となります。

- ・ ルータ型のフォーマットのうち、nextHop および dst\_mask
- ・ ゲートウェイ型のフォーマットのうち、dst\_peer\_as および dst\_as

図 30-7 他機能と併用時の sFlow 統計対象判定位置



## 30.2 コンフィグレーション

### 30.2.1 コンフィグレーションコマンド一覧

sFlow 統計で使用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 30-18 コンフィグレーションコマンド一覧

| コマンド名                           | 説明                                                                                            |
|---------------------------------|-----------------------------------------------------------------------------------------------|
| sflow destination               | sFlow パケットの宛先であるコレクタの IP アドレスを指定します。                                                          |
| sflow extended-information-type | フローサンプルの各拡張データ形式の送信有無を指定します。                                                                  |
| sflow forward egress            | 指定したポートの送信トラフィックを sFlow 統計の監視対象にします。                                                          |
| sflow forward ingress           | 指定したポートの受信トラフィックを sFlow 統計の監視対象にします。                                                          |
| sflow max-header-size           | 基本データ形式 (sflow packet-information-type コマンド参照) にヘッダ型を使用している場合、サンプルパケットの先頭からコピーされる最大サイズを指定します。 |
| sflow max-packet-size           | sFlow パケットのサイズを指定します。                                                                         |
| sflow packet-information-type   | フローサンプルの基本データ形式を指定します。                                                                        |
| sflow polling-interval          | カウンタサンプルをコレクタへ送信する間隔を指定します。                                                                   |
| sflow sample                    | 装置全体に適用するサンプリング間隔を指定します。                                                                      |
| sflow source                    | sFlow パケットの送信元 (エージェント) に設定される IP アドレスを指定します。                                                 |
| sflow url-port-add              | 拡張データ形式で URL 情報を使用する場合に、HTTP パケットと判断するポート番号を 80 以外に追加指定します。                                   |
| sflow version                   | 送信する sFlow パケットのバージョンを設定します。                                                                  |

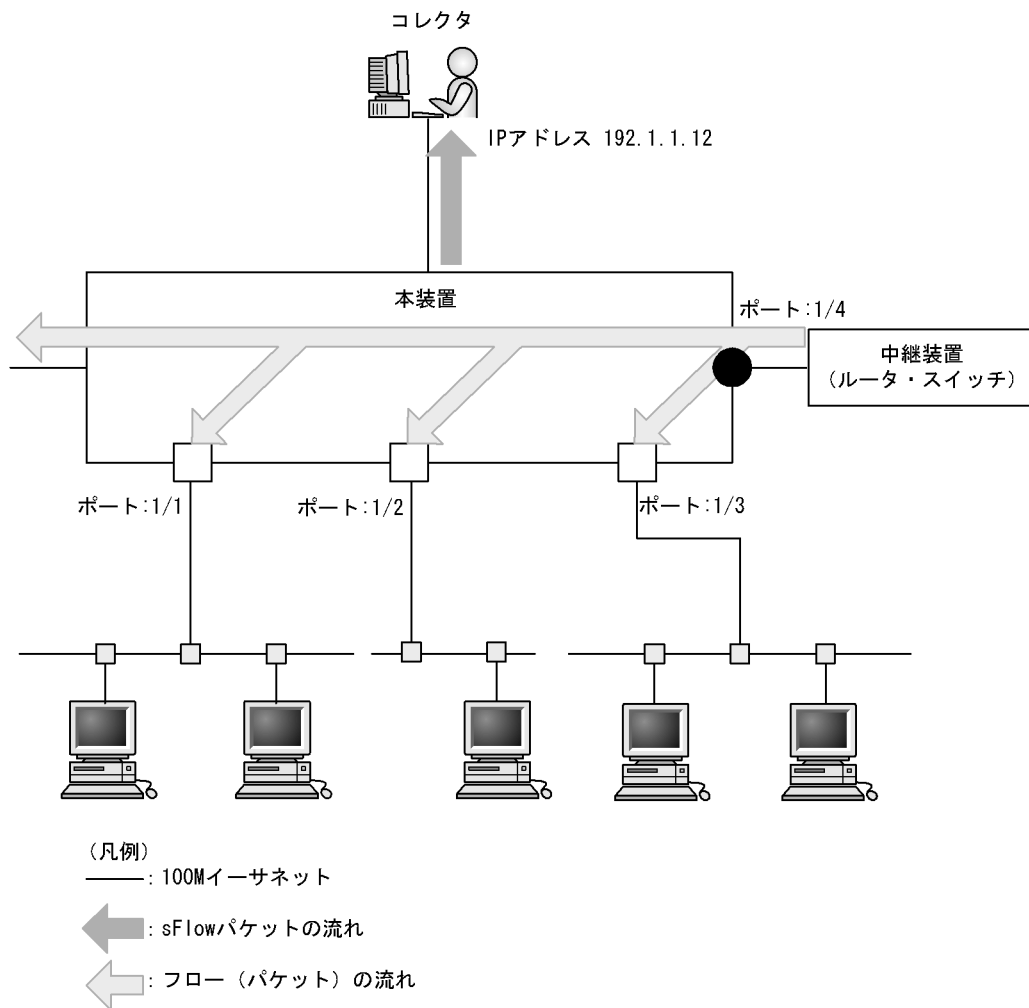
### 30.2.2 sFlow 統計の基本的な設定

#### (1) 受信パケットをモニタする設定

[ 設定のポイント ]

sFlow 統計のコンフィグレーションは装置全体で有効な設定と、実際に運用するポートを指定する設定の二つが必要です。ここではポート 1/4 に対して入ってくるパケットをモニタする設定を示します。

図 30-8 ポート 1/4 の受信パケットをモニタする設定例



## [ コマンドによる設定 ]

1. `(config)# sflow destination 192.1.1.12`  
コレクタとして IP アドレス 192.1.1.12 を設定します。
2. `(config)# sflow sample 512`  
512 パケットごとにトラフィックをモニタします。
3. `(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。
4. `(config-if)# sflow forward ingress`  
ポート 1/4 の受信パケットに対して sFlow 統計機能を有効にします。

## [ 注意事項 ]

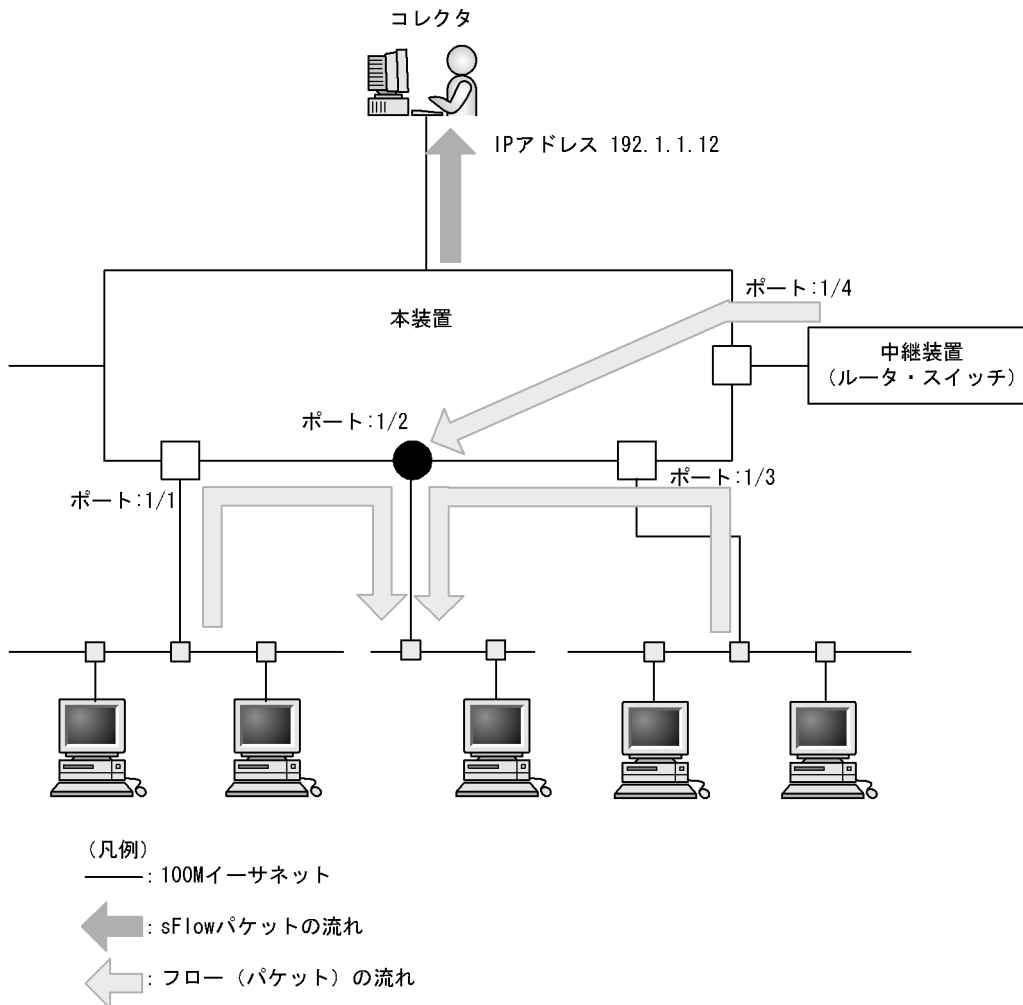
sflow sample コマンドで設定するサンプリング間隔については、インタフェースの回線速度を考慮して決める必要があります。詳細は、「コンフィグレーションコマンドレファレンス Vol.2 sflow sample」を参照してください。

## (2) 送信パケットをモニタする設定

## [ 設定のポイント ]

sFlow 統計機能を、受信パケットまたは送信パケットのどちらに対して有効にするかは、インタフェースコンフィグレーションモードで設定するときに `sflow forward ingress` コマンドまたは `sflow forward egress` コマンドのどちらを指定するかによって決まります。ここではポート 1/2 から出て行くパケットをモニタする設定を示します。

図 30-9 ポート 1/2 の送信パケットをモニタする設定例



## [ コマンドによる設定 ]

1. `(config)# sflow destination 192.1.1.12`  
コレクタとして IP アドレス 192.1.1.12 を設定します。
2. `(config)# sflow sample 512`  
512 パケットごとにトラフィックをモニタします。
3. `(config)# interface gigabitethernet 1/2`  
ポート 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。

## 4. (config-if)# sflow forward egress

ポート 1/2 の送信パケットに対して sFlow 統計機能を有効にします。

## [ 注意事項 ]

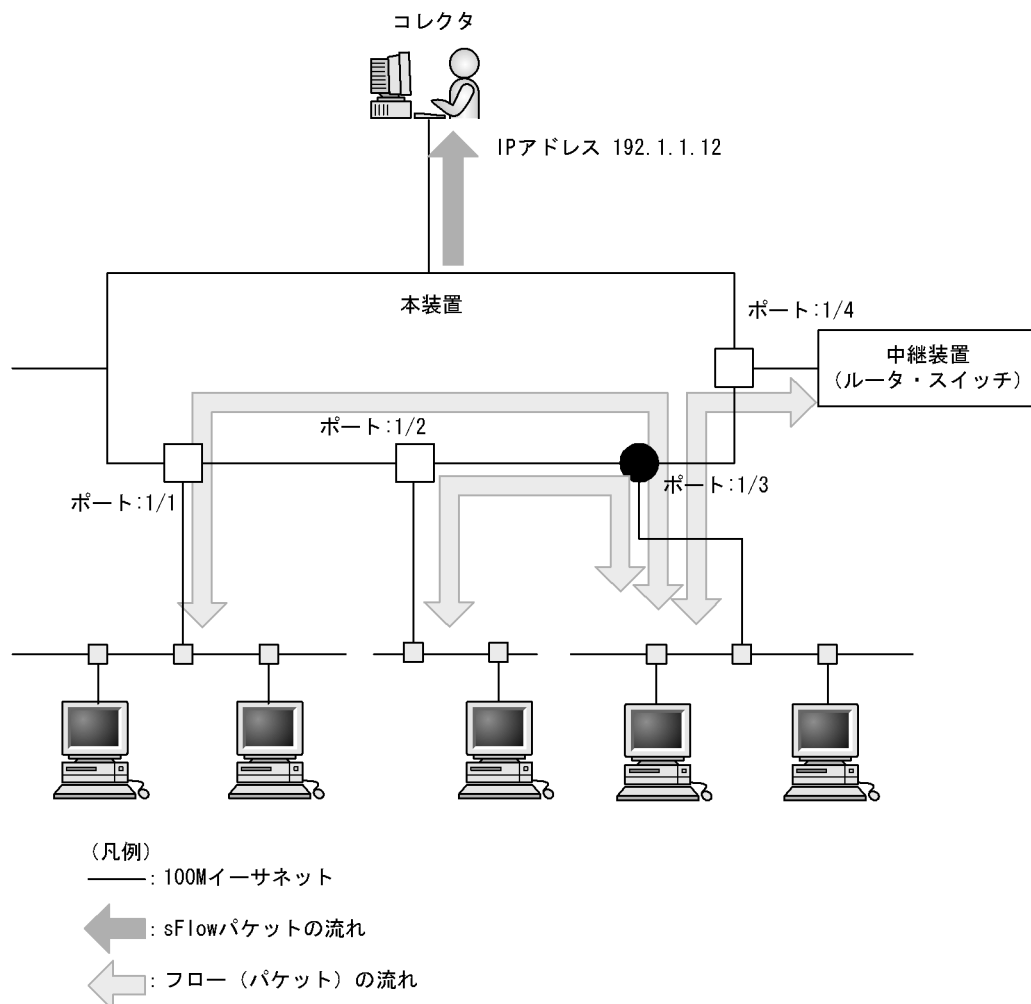
送信パケットを有効にすると本装置の自発パケットも収集されます。sFlow パケットも収集対象に入りますので、コレクタに繋がっているポートの出力を有効にする場合は注意してサンプリング間隔を設定してください。送信パケットを有効にしている場合は永久ループを避けるためサンプリング間隔は 2 以上でしか設定できません。

## (3) あるポートの送受信パケットをモニタする設定

## [ 設定のポイント ]

あるポートに対して送受信するトラフィックを両方とも sFlow 統計機能の対象にできます。ここではポート 1/3 に対して入ってくるパケットと出ていくパケットをモニタする設定を示します。

図 30-10 ポート 1/3 の送受信パケットをモニタする設定例



## [ コマンドによる設定 ]

## 1. (config)# sflow destination 192.1.1.12

コレクタとして IP アドレス 192.1.1.12 を設定します。

2. `(config)# sflow sample 2048`  
2048 パケットごとにトラフィックをモニタします。
3. `(config)# interface gigabitethernet 1/3`  
ポート 1/3 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。
4. `(config-if)# sflow forward ingress`  
ポート 1/3 の受信パケットに対して sFlow 統計機能を有効にします。
5. `(config-if)# sflow forward egress`  
ポート 1/3 の送信パケットに対して sFlow 統計機能を有効にします。

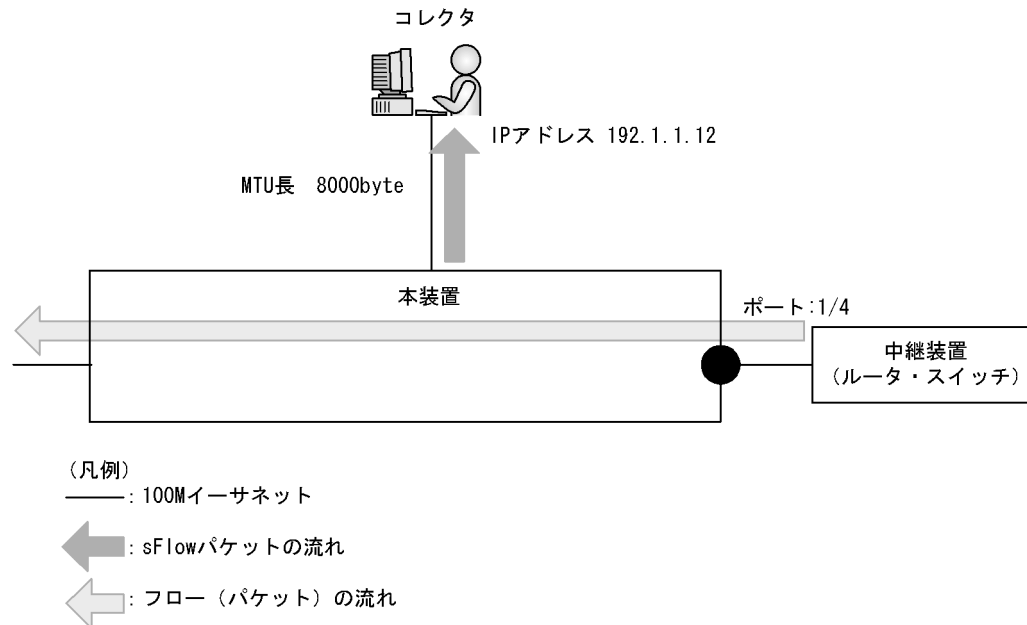
### 30.2.3 sFlow 統計コンフィギュレーションパラメータの設定例

#### (1) MTU 長と sFlow パケットサイズの調整

[ 設定のポイント ]

sFlow パケットはデフォルトでは 1400byte 以下のサイズでコレクタに送信されます。コレクタへの回線の MTU 値が大きい場合、同じ値に調整することでコレクタに対して効率よく送信できます。ここでは MTU 長が 8000byte の回線とコレクタが繋がっている設定を記述します。

図 30-11 コレクタへの送信を MTU=8000byte に設定する例



[ コマンドによる設定 ]

1. `(config)# sflow destination 192.1.1.12`  
コレクタとして IP アドレス 192.1.1.12 を設定します。
2. `(config)# sflow sample 32`

32 パケットごとにトラフィックをモニタします。

3. `(config)# sflow max-packet-size 8000`  
sflow パケットサイズの最大値を 8000byte に設定します。
4. `(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。
5. `(config-if)# sflow forward ingress`  
ポート 1/4 の受信パケットに対して sFlow 統計機能を有効にします。

## (2) 収集したい情報を絞る

### [ 設定のポイント ]

sFlow パケットの情報はコンフィグレーションを指定しないとすべて収集する条件になっています。しかし、不要な情報がある場合に、その情報を取らない設定をすることで CPU 使用率を下げることができます。ここでは IP アドレス情報だけがが必要な場合の設定を記述します。

### [ コマンドによる設定 ]

1. `(config)# sflow destination 192.1.1.12`  
コレクタとして IP アドレス 192.1.1.12 を設定します。
2. `(config)# sflow sample 512`  
512 パケットごとにトラフィックをモニタします。
3. `(config)# sflow packet-information-type ip`  
フローサンプルの基本データ形式に IP 形式を設定します。
4. `(config)# sflow extended-information-type router`  
フローサンプルの拡張データ形式に「ルータ」を設定します（ルータ情報だけが取得できます）。
5. `(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。
6. `(config-if)# sflow forward ingress`  
ポート 1/4 の受信パケットに対して sFlow 統計機能を有効にします。

## (3) sFlow パケットのエージェント IP アドレスを固定化する

### [ 設定のポイント ]

一般的なコレクタは、sFlow パケットに含まれるエージェント IP アドレスの値を基にして同一の装置かどうかを判断しています。この理由から、`sflow source` コマンドや `interface loopback` コマンドでエージェント IP アドレスを設定していない場合、コレクタ側で複数装置から届いているように表示されるおそれがあります。長期的に情報を見る場合はエージェント IP アドレスを固定化してください。ここでは loopback に割り当てられた IP アドレスをエージェント IP アドレスとして利用し、コレクタに送る設定を示します。

## [ コマンドによる設定 ]

1. (config)# interface loopback 0  
ループバック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 176.1.1.11  
ループバックインタフェースに IPv4 用として 176.1.1.11 を設定します。
3. (config-if)# ipv6 address 3ffe:100::1  
(config-if)# exit  
ループバックインタフェースに IPv6 用として 3ffe:100::1 を設定します。
4. (config)# sflow destination 192.1.1.12  
コレクタとして IP アドレス 192.1.1.12 を設定します。
5. (config)# sflow sample 512  
512 パケットごとにトラフィックをモニタします。
6. (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。
7. (config-if)# sflow forward ingress  
ポート 1/4 の受信パケットに対して sFlow 統計機能を有効にします。

## [ 注意事項 ]

loopback の IP アドレスを使う場合は、sflow source コマンドで設定する必要はありません。もし、sflow source コマンドで IP アドレスが指定されているとその IP アドレスが優先されます。

## (4) ローカルネットワーク環境での URL 情報収集

## [ 設定のポイント ]

本装置では sFlow 統計で URL 情報 (HTTP パケット) を収集する場合、宛先のポート番号として 80 番を利用している環境がデフォルトになっています。しかし、ローカルなネットワークではポート番号が異なる場合があります。ローカルネットワーク環境で HTTP パケットのポート番号として 8080 番を利用している場合の設定を示します。

## [ コマンドによる設定 ]

1. (config)# sflow destination 192.1.1.12  
コレクタとして IP アドレス 192.1.1.12 を設定します。
2. (config)# sflow sample 512  
512 パケットごとにトラフィックをモニタします。
3. (config)# sflow url-port-add 8080  
拡張データ形式で URL 情報を使用する場合に、HTTP パケットと判断する宛先ポート番号 8080 を追加で設定します。
4. (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。

5. `(config-if)# sflow forward ingress`

ポート 1/4 の受信パケットに対して sFlow 統計機能を有効にします。

[ 注意事項 ]

本パラメータを設定した後でも、HTTP パケットの対象として宛先ポート番号 80 番は有効です。

## 30.3 オペレーション

### 30.3.1 運用コマンド一覧

sFlow 統計で使用する運用コマンド一覧を次の表に示します。

表 30-19 運用コマンド一覧

| コマンド名                  | 説明                                  |
|------------------------|-------------------------------------|
| show sflow             | sFlow 統計機能についての設定条件と動作状況を表示します。     |
| clear sflow statistics | sFlow 統計で管理している統計情報をクリアします。         |
| restart sflow          | フロー統計プログラムを再起動します。                  |
| dump sflow             | フロー統計プログラム内で収集しているデバック情報をファイル出力します。 |

### 30.3.2 コレクタとの通信の確認

本装置で sFlow 統計機能を設定してコレクタに送信する場合、次のことを確認してください。

#### (1) コレクタとの疎通確認

ping コマンドをコレクタの IP アドレスを指定して実行し、本装置からコレクタに対して IP 通信ができることを確認してください。通信ができない場合は、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。

#### (2) sFlow パケット通信確認

コレクタ側で sFlow パケットを受信していることを確認してください。

受信していない場合の対応は、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。

### 30.3.3 sFlow 統計機能の運用中の確認

本装置で sFlow 統計機能を使用した場合、運用中の確認内容には次のものがあります。

#### (1) sFlow パケット廃棄数の確認

show sflow コマンドを実行して sFlow 統計情報を表示し、sFlow 統計機能で廃棄しているパケット数を確認してください。廃棄数が増加する場合は、廃棄数が増加しないサンプリング間隔を設定してください。

図 30-12 show sflow コマンドの実行結果

```

> show sflow
Date 2006/10/13 14:10:32 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared: 16:00:05
sFlow agent data :
 sFlow service version : 4
 CounterSample interval rate: 60 seconds
 Default configured rate: 1 per 2048 packets
 Default actual rate : 1 per 2048 packets
 Configured sFlow ingress ports : 1/2-4
 Configured sFlow egress ports : 5/9-11
 Received sFlow samples :37269 Dropped sFlow samples(Dropped Que):2093(2041)...1
 Exported sFlow samples :37269 Couldn't export sFlow samples : 0
sFlow collector data :
 Collector IP address: 192.168.4.199 UDP:6343 Source IP address: 130.130.130.1
 Send FlowSample UDP packets : 12077 Send failed packets: 0
 Send CounterSample UDP packets: 621 Send failed packets: 0
 Collector IP address: 192.168.4.203 UDP:65535 Source IP address: 130.130.130.1
 Send FlowSample UDP packets : 12077 Send failed packets: 0
 Send CounterSample UDP packets: 621 Send failed packets: 0

```

1. 廃棄パケット数が増加している場合、サンプリング間隔の設定を見直してください。

## (2) CPU 使用率の確認

show cpu コマンドを実行して CPU 使用率を表示し、負荷を確認してください。CPU 使用率が高い場合は、コンフィグレーションコマンド sflow sample でサンプリング間隔を再設定してください。

図 30-13 show cpu コマンドの実行結果

```

>show cpu minutes
Date 2006/10/13 14:15:37 UTC
*** minute ***
date time cpu average
Oct 13 14:42:00-14:42:59 6
Oct 13 14:43:00-14:43:59 20
 :
 :
Oct 13 15:41:00-15:41:59 10 ...1

```

1. CPU 使用率が高くなっている場合、サンプリング間隔の設定を見直してください。

## 30.3.4 sFlow 統計のサンプリング間隔の調整方法

本装置で sFlow 統計機能を使用した場合、サンプリング間隔の調整方法として次のものがあります。

### (1) 回線速度から調整する

sFlow 統計機能を有効にしている全ポートの pps を show interfaces コマンドで確認し、受信パケットを対象にしている場合は「Input rate」を合計してください。もし、送信パケットを対象にしている場合は、「Output rate」も合計してください。その合計値を 500 で割った値が、目安となるサンプリング間隔となります。この値でサンプリング間隔を設定後、show sflow コマンドで廃棄数が増えないかどうかを確認してください。

ポート 1/4 とポート 1/5 に対して受信パケットをとる場合の目安となるサンプリング間隔の例を次に示します。

図 30-14 show interfaces コマンドの実行結果

```

> show interfaces gigabitethernet 1/4
Date 2006/10/24 17:18:54 UTC
NIF1: active 48-port 10BASE-T/100BASE-TX/1000BASE-T retry:0
 Average:150Mbps/24Gbps Peak:200Mbps at 15:44:37
Port4: active up 100BASE-TX full(auto) 0012.e220.ec30
 Time-since-last-status-change:1:47:47
 Bandwidth:10000kbps Average out:0Mbps Average in:5Mbps
 Peak out:5Mbps at 15:44:36 Peak in:5Mbps at 15:44:18
 Output rate: 0.0bps 0.0pps
 Input rate: 4063.5kbps 10.3kpps
 Flow control send :off
 Flow control receive:off
 TPID:8100
 :

> show interfaces gigabitethernet 1/5
Date 2006/10/24 17:19:34 UTC
NIF1: active 48-port 10BASE-T/100BASE-TX/1000BASE-T retry:0
 Average:150Mbps/24Gbps Peak:200Mbps at 15:44:37
Port5: active up 100BASE-TX full(auto) 0012.e220.ec31
 Time-since-last-status-change:1:47:47
 Bandwidth:10000kbps Average out:5Mbps Average in:5Mbps
 Peak out:5Mbps at 15:44:36 Peak in:5Mbps at 15:44:18
 Output rate: 4893.5kbps 16.8kpps
 Input rate: 4893.5kbps 16.8kpps
 Flow control send :off
 Flow control receive:off
 TPID:8100
 :

```

## 目安となるサンプリング間隔

```

= sFlow 統計機能を有効にしているポートの PPS 合計値 /500
= (10.3kpps+16.8kpps) /500
= 55

```

注 サンプリング間隔を 55 で設定すると実際は 128 で動作します。サンプリング間隔の詳細はコンフィグレーションコマンド `sflow sample` を参照してください。

## (2) 詳細情報から調整する

`show sflow detail` コマンドを実行して表示される Sampling rate to collector (コレクタから見たサンプリング間隔) の値をサンプリング間隔として設定します。設定後は `clear sflow statistics` コマンドを実行し、しばらく様子を見てまだ Sampling rate to collector の値が設定より大きい場合は同じ手順でサンプリング間隔を設定してください。

図 30-15 show sflow detail コマンドの実行結果

```

> show sflow detail
Date 2006/10/21 20:04:01 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared: 8:00:05
 :
Collector IP address: 192.168.4.203 UDP:65535 Source IP address:

```

```
130.130.130.1
 Send FlowSample UDP packets : 12077 Send failed packets: 0
 Send CounterSample UDP packets: 621 Send failed packets: 0
Detail data :
Max packet size: 1400 bytes
Packet information type: header
Max header size: 128 bytes
Extended information type: switch,router,gateway,user,url
Url port number: 80,8080
Sampling mode : random-number
Sampling rate to collector : 1 per 2163 packets
Target ports for CounterSample : 1/2-4 , 5/9-11
```



# 31 LLDP

この章では、本装置に隣接する装置の情報を収集する機能である LLDP の解説と操作方法について説明します。

---

31.1 解説

---

31.2 コンフィグレーション

---

31.3 オペレーション

---

## 31.1 解説

### 31.1.1 概要

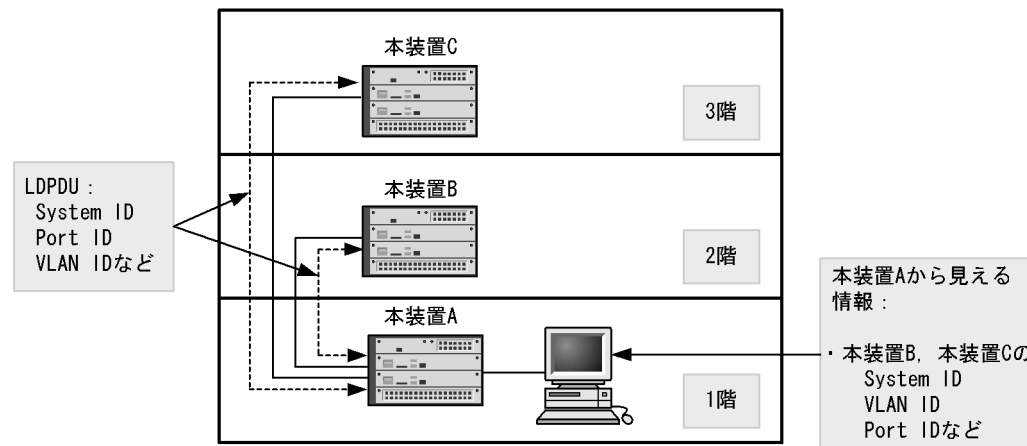
LLDP (Link Layer Discovery Protocol) は隣接する装置情報を収集するプロトコルです。運用・保守時に接続装置の情報を簡単に調査できることを目的とした機能です。

#### (1) LLDP の適用例

LLDP 機能を使用することで隣接装置と接続している各ポートに対して、自装置に関する情報および該当ポートに関する情報を送信します。該当ポートで受信した隣接装置の情報を管理することで自装置と隣接装置間の接続状態を把握できるようになります。

LLDP の適用例を次の図に示します。この例では、同一ビル内の各階に設置された本装置間の接続状態を、1階に設置した本装置 A から把握できるようになります。

図 31-1 LLDP の適用例



### 31.1.2 サポート仕様

この機能を用いて隣接装置に配布する情報は、IEEE 802.1AB Draft 6 をベースに拡張機能として本装置独自の情報をサポートしています。サポートする情報を次の表に示します。

表 31-1 LLDP でサポートする情報

| 項番 | 名称                 | 説明                                      |                       |
|----|--------------------|-----------------------------------------|-----------------------|
| 1  | Time-to-Live       | 情報の保持時間                                 |                       |
| 2  | Chassis ID         | 装置の識別子                                  |                       |
| 3  | Port ID            | ポート識別子                                  |                       |
| 4  | Port description   | ポート種別                                   |                       |
| 5  | System name        | 装置名称                                    |                       |
| 6  | System description | 装置種別                                    |                       |
| 7  | -                  | Organizationally-defined TLV extensions | ベンダー・組織が独自に定めた TLV    |
|    | a                  | VLAN ID                                 | 設定されている VLAN ID       |
|    | b                  | VLAN Address                            | VLAN に関連づけられた IP アドレス |



(凡例) - : 該当なし

LLDP でサポートする情報の詳細を以下に示します。

なお、MIB についてはマニュアル「MIB レファレンス」を参照してください。

### (1) Time-to-Live (情報の保持時間)

配布する情報を受信装置側で保持する時間を示します。

保持時間はコンフィグレーションで変更できますが、初期状態で使用することをお勧めします。

### (2) Chassis ID (装置の識別子)

装置を識別する情報です。この情報には subtype が定義され、subtype によって送信内容が異なります。subtype と送信内容を次の表に示します。

表 31-2 Chassis ID の subtype 一覧

| subtype | 種別                  | 送信内容                                        |
|---------|---------------------|---------------------------------------------|
| 1       | Chassis component   | Entity MIB の entPhysicalAlias と同じ値          |
| 2       | Chassis interface   | interface MIB の ifAlias と同じ値                |
| 3       | Port                | Entity MIB の portEntPhysicalAlias と同じ値      |
| 4       | Backplane component | Entity MIB の backplaneEntPhysicalAlias と同じ値 |
| 5       | MAC address         | LLDP MIB の macAddress と同じ値                  |
| 6       | Network address     | LLDP MIB の networkAddress と同じ値              |
| 7       | Locally assigned    | LLDP MIB の local と同じ値                       |

Chassis ID についての送受信条件は次のとおりです。

- 送信: subtype = 5 だけ送信します。送信する MAC アドレスは装置 MAC アドレスを使用します。
- 受信: 上記に示した全 subtype について受信できます。
- 受信データ最大長: 255byte

### (3) Port ID (ポート識別子)

ポートを識別する情報です。この情報には subtype が定義され、subtype によって送信内容が異なります。subtype と送信内容を次の表に示します。

表 31-3 Port ID の subtype 一覧

| subtype | 種別                  | 送信内容                                        |
|---------|---------------------|---------------------------------------------|
| 1       | Port                | Interface MIB の ifAlias と同じ値                |
| 2       | Port component      | Entity MIB の portEntPhysicalAlias と同じ値      |
| 3       | Backplane component | Entity MIB の backplaneEntPhysicalAlias と同じ値 |
| 4       | MAC address         | LLDP MIB の macAddress と同じ値                  |
| 5       | Network address     | LLDP MIB の networkAddress と同じ値              |
| 6       | Locally assigned    | LLDP MIB の local と同じ値                       |

Port ID についての送受信条件は次のとおりです。

- 送信：subtype = 4 だけ送信します。送信する MAC アドレスは該当 Port の MAC アドレスを使用します。
- 受信：上記に示した全 subtype について受信できます。
- 受信データ最大長：255Byte

#### (4) Port description (ポート種別)

ポートの種別を示す情報です。この情報には subtype はありません。

送信内容および受信条件は次のとおりです。

- 送信内容：「Interface MIB の ifDescr と同じ値」
- 受信データ最大長：255Byte

#### (5) System name (装置名称)

装置名称を示す情報です。この情報には subtype はありません。

送信内容および受信条件は次のとおりです。

- 送信内容：「systemMIB の sysName と同じ値」
- 受信データ最大長：255Byte

#### (6) System description (装置種別)

装置の種別を示す情報です。この情報には subtype はありません。

送信内容および受信条件は次のとおりです。

- 送信内容：「systemMIB の sysDescr と同じ値」
- 受信データ最大長：255Byte

#### (7) Organizationally-defined TLV extensions

本装置独自に以下の情報をサポートしています。

##### (a) VLAN ID

該当ポートが使用する VLAN Tag の VLAN ID を示します。Tag 変換を使用している場合は、変換後の VLAN ID を示します。この情報はトランクポートだけ有効な情報です。

##### (b) VLAN Address

この情報は、該当ポートにおいて IP アドレスが設定されている VLAN のうち、最も小さい VLAN ID とその IP アドレスを一つ示します。

### 31.1.3 LLDP 使用時の注意事項

#### (1) 本機能を設定した装置間に本機能をサポートしない別装置を接続した場合

次に示す構成とした場合、隣接装置との接続状態を正確に把握しにくい状態になります。

- スイッチを経由して接続した場合、スイッチは LLDP の配布情報を中継します。そのため、直接接続していない装置間で、隣接情報として配布情報を受信できるので、直接接続されている装置間の情報と区別が付きなくなります。
- ルータを経由して接続した場合、LLDP の配布情報はルータで廃棄されるため LLDP 機能を設定した

装置間では受信できません。

## (2) 他社接続について

他社が独自にサポートしている Link Layer Discovery Protocol との相互接続はできません。

注

Cisco Systems 社：CDP ( Cisco Discovery Protocol )

Extreme Networks 社：EDP ( Extreme Discovery Protocol )

Foundry Networks 社：FDP ( Foundry Discovery Protocol )

## (3) IEEE 802.1AB 規格との接続について

本装置の LLDP は IEEE 802.1AB Draft 6 をベースにサポートした独自機能です。IEEE 802.1AB 規格との接続性はありません。

## (4) 隣接装置の最大数について

装置当たり最大 192 の隣接装置情報を収容できます。最大数を超えた場合、受信した配布情報は廃棄します。受信済みの隣接装置情報がタイムアウトで削除される時間を確保するために、廃棄状態は一定時間継続されます。時間は、最大収容数の閾値以上になった隣接装置情報の保持時間と同一です。

## (5) VRF 機能との共存について【OP-NPAR】

VRF を設定した VLAN に設定された IP アドレスは配布しません。

## 31.2 コンフィグレーション

### 31.2.1 コンフィグレーションコマンド一覧

LLDP 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 31-4 コンフィグレーションコマンド一覧

| コマンド名              | 説明                                       |
|--------------------|------------------------------------------|
| lldp enable        | ポートで LLDP の運用を開始します。                     |
| lldp hold-count    | 本装置が送信する LLDP フレームに対して隣接装置が保持する時間を指定します。 |
| lldp interval-time | 本装置が送信する LLDP フレームの送信間隔を指定します。           |
| lldp run           | 装置全体で LLDP 機能を有効にします。                    |

### 31.2.2 LLDP の設定

#### (1) LLDP 機能の設定

##### [ 設定のポイント ]

LLDP 機能のコンフィグレーションは装置全体で機能を有効にする設定と、実際に運用するポートで有効にする設定が必要です。

ここでは、gigabitethernet 1/1 において LLDP 機能を運用させます。

##### [ コマンドによる設定 ]

1. (config)# lldp run  
装置全体で LLDP 機能を有効にします。
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グレーションモードに移行します。
3. (config-if)# lldp enable  
ポート 1/1 で LLDP 機能の動作を開始します。

#### (2) LLDP フレームの送信間隔，保持時間の設定

##### [ 設定のポイント ]

LLDP フレームの送信間隔を変更すると，装置の情報の変更が反映される時間を調整できます。送信間隔を短くすると変更が早く反映され，送信間隔を長くすると変更の反映が遅くなります。

##### [ コマンドによる設定 ]

1. (config)# lldp interval-time 60  
LLDP フレームの送信間隔を 60 秒に設定します。
2. (config)# lldp hold-count 3  
本装置が送信した情報を隣接装置が保持する時間を interval-time 時間の回数で設定します。この場合，60 秒 × 3 で 180 秒になります。

## 31.3 オペレーション

### 31.3.1 運用コマンド一覧

LLDP の運用コマンド一覧を次の表に示します。

表 31-5 運用コマンド一覧

| コマンド名                 | 説明                                                   |
|-----------------------|------------------------------------------------------|
| show lldp             | LLDP の設定情報および隣接装置情報を表示します。                           |
| show lldp statistics  | LLDP の統計情報を表示します。                                    |
| clear lldp            | LLDP の隣接情報をクリアします。                                   |
| clear lldp statistics | LLDP の統計情報をクリアします。                                   |
| restart lldp          | LLDP プログラムを再起動します。                                   |
| dump protocols lldp   | LLDP 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。 |

### 31.3.2 LLDP 情報の表示

LLDP 情報の表示は、運用コマンド show lldp で行います。show lldp コマンドは、LLDP の設定情報とポートごとの隣接装置数を表示します。show lldp detail コマンドは、隣接装置の詳細な情報を表示します。

図 31-2 show lldp コマンドの実行結果

```
> show lldp
Date 2006/03/09 19:16:20 UTC
Status: Enabled Chassis ID: Type=MAC Info=0012.e268.2c21
Interval Time: 30 Hold Count: 4 TTL:120
Port Counts=3
1/1 (CH:10) Link:Up Neighbor Counts: 2
1/2 Link:Down Neighbor Counts: 0
1/3 Link:Up Neighbor Counts: 0
>
```

図 31-3 show lldp detail コマンドの実行結果

```
> show lldp detail
Date 2006/03/09 19:16:34 UTC
Status: Enabled Chassis ID: Type= MAC Info=0012.e268.2c21
Interval Time: 30 Hold Count: 4 TTL:120
System Name: LLDP1
System Description: ALAXALA AX6300S AX-6300-S04 [AX6304S] Switching software Ver.
10.2 [OS-SE]
Total Neighbor Counts=2
Port Counts=3
Port 1/1 (CH:10) Link: Up Neighbor Counts: 2
Port ID: Type=MAC Info=0012.e298.5cc0
Port Description: GigabitEther 1/1
Tag ID: Tagged=1,10-20,4094
IPv4 Address: Tagged: 10 192.168.248.240
IPv6 Address: Tagged: 20 3ffe:501:811:ff01:200:8798:5cc0:e7f4
1 TTL:110 Chassis ID: Type=MAC Info=0012.e268.2505
System Name: LLDP2
System Description: ALAXALA AX6300S AX-6300-S04 [AX6304S] Switching software
```

## 31. LLDP

```
Ver. 10.2 [OS-SE]
Port ID: Type=MAC Info=0012.e298.dc20
Port Description: GigabitEthernet 1/5
Tag ID: Tagged=1,10-20,4094
IPv4 Address: Tagged: 10 192.168.248.220
 2 TTL:100 Chassis ID: Type=MAC Info=0012.e268.2c2d
System Name: LLDP3
System Description: ALAXALA AX6300S AX-6300-S08 [AX6308S] Switching software
Ver. 10.2 [OS-SE]
Port ID: Type=MAC Info=0012.e298.7478
Port Description: GigabitEthernet 1/24
Tag ID: Tagged=1,10-20,4094
IPv4 Address: Tagged: 10 192.168.248.200
IPv6 Address: Tagged: 20 3ffe:501:811:ff01:200:8798:7478:e7f4
Port 1/2 Link: Down Neighbor Counts: 0
Port 1/3 Link: Up Neighbor Counts: 0
>
```

# 32 OADP

この章では、本装置に隣接する装置の情報を収集する機能である OADP の解説と操作方法について説明します。

---

32.1 解説

---

32.2 コンフィグレーション

---

32.3 オペレーション

---

## 32.1 解説

---

### 32.1.1 概要

#### (1) OADP 機能の概要

OADP (Octopower Auto Discovery Protocol) 機能とは、本装置のレイヤ 2 レベルで動作する機能で、OADP PDU (Protocol Data Unit) のやりとりによって隣接装置の情報を収集し、隣接装置の接続状況を表示できます。

この機能では、隣接装置の装置情報やポート情報を表示することで隣接装置との接続状況を容易に把握できることから、隣接装置にログインしたりネットワーク構成図を参照したりしなくても、装置間の接続の状況を確認できます。また、この機能によって表示される接続状況とネットワーク構成図を比較することで、装置間が正しく接続されているかどうかを確認できます。

隣接装置として認識できる装置には、本装置のほかに、CDP を実装した装置、OADP を実装した装置があります。

#### (2) CDP 受信機能の概要

OADP 機能では、CDP (Cisco Discovery Protocol) を解釈できるため、CDP PDU を送信する隣接装置との接続構成も確認できます。ただし、本装置は CDP PDU を送信しません。CDP とは、Cisco Systems 社製装置のレイヤ 2 レベルで動作する隣接装置検出プロトコルです。

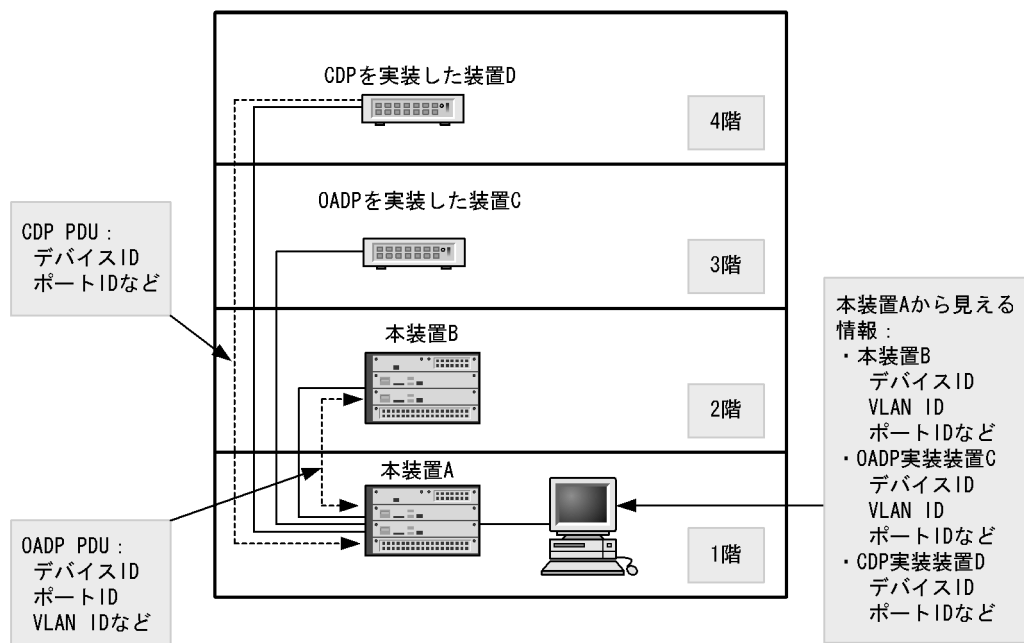
#### (3) OADP の適用例

OADP 機能を使用することで、隣接装置と接続している各ポートに対して自装置に関する情報および該当ポートに関する情報を送信します。自装置やポートに関する情報としては、デバイス ID、ポート ID、IP アドレス、VLAN ID などがあります。隣接装置から送られてきた情報を該当ポートで受信することで、自装置と隣接装置間の接続状態を把握できるようになります。

OADP の適用例を次の図に示します。この例では、同一ビル内の各階に設置された装置間の接続状態を、1 階に設置した本装置 A から把握することが可能となります。



図 32-1 OADP の適用例



## 32.1.2 サポート仕様

### (1) OADP のサポート仕様

OADP でサポートする項目と仕様を次の表に示します。

表 32-1 OADP 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 | ×                    |
| OADP PDU 送受信単位  |       | 物理ポートまたはリンクアグリゲーション  |
| リセット機能          |       |                      |
| OADP PDU 送信間隔   |       | 5 ~ 254 秒の範囲で 1 秒単位  |
| OADP PDU 情報保有時間 |       | 10 ~ 255 秒の範囲で 1 秒単位 |
| CDP 受信機能        |       |                      |

(凡例) : サポート × : 未サポート

### (2) OADP で使用する情報

OADP PDU で使用する情報を次の表に示します。

表 32-2 OADP でサポートする情報

| 項番 | 名称        | 説明                                                   |
|----|-----------|------------------------------------------------------|
| 1  | Device ID | 装置を一意に識別する識別子                                        |
| 2  | Address   | OADP PDU を送信するインタフェースに関連するアドレス、およびループバックインタフェースのアドレス |

| 項番 | 名称           | 説明                             |
|----|--------------|--------------------------------|
| 3  | Port ID      | OADP PDU を送信するポートの識別子          |
| 4  | Capabilities | 装置の機能                          |
| 5  | Version      | ソフトウェアバージョン                    |
| 6  | Platform     | プラットフォーム                       |
| 7  | Duplex       | OADP PDU を送信するポートの Duplex 情報   |
| 8  | ifIndex      | OADP PDU を送信するポートの ifIndex     |
| 9  | ifSpeed      | OADP PDU を送信するポートの ifSpeed     |
| 10 | VLAN ID      | OADP PDU を送信するポートの VLAN ID     |
| 11 | ifHighSpeed  | OADP PDU を送信するポートの ifHighSpeed |

受信する CDP PDU で使用される可能性のある情報を次の表に示します。項番 1 ~ 7 は OADP PDU と共通です。

表 32-3 CDP でサポートする情報

| 項番 | 名称           | 説明                          |
|----|--------------|-----------------------------|
| 1  | Device ID    | 装置を一意に識別する識別子               |
| 2  | Address      | CDP PDU を送信するポートに関連するアドレス   |
| 3  | Port ID      | CDP PDU を送信するポートの識別子        |
| 4  | Capabilities | 装置の機能                       |
| 5  | Version      | ソフトウェアバージョン                 |
| 6  | Platform     | プラットフォーム                    |
| 7  | Duplex       | CDP PDU を送信するポートの Duplex 情報 |

### 32.1.3 OADP 使用時の注意事項

#### (1) この機能を設定した装置間にこの機能をサポートしない別装置を接続した場合

次に示す構成とした場合、隣接装置との接続状態を正確に把握しにくい状態になります。

- スイッチを経由して接続した場合、スイッチは OADP の配布情報を中継します。そのため、直接接続していない装置間で隣接情報として配布情報を受信できるので、直接接続されている装置間の情報と区別が付きなくなります。
- ルータを経由して接続した場合、OADP の配布情報はルータで廃棄されるため OADP 機能を設定した装置間では受信できません。

#### (2) 隣接装置の最大数について

装置当たり最大 250 の隣接装置情報を収容できます。最大数を超えた場合、受信した配布情報は廃棄されます。受信済みの隣接装置情報がタイムアウトで削除される時間を確保するために廃棄状態は一定時間継続されます。時間は、最大収容数の閾値以上になった隣接装置情報の保持時間と同じです。

#### (3) OADP を使用するポートの VLAN について

OADP はポートに設定されている VLAN 上で OADP PDU を送受信します。VLAN を無効 (state suspend コマンド) に設定するとその VLAN では OADP は動作しません。

#### (4) CDP を実装した装置と接続した場合について

トランクポートで CDP を実装した装置と接続した場合は、そのポートが VLAN ID=1 の Tagged フレームも受信できるようなコンフィグレーションを設定してください。トランクポートにおいて VLAN ID=1 の Tagged フレームを受信しないコンフィグレーションを設定した場合、CDP PDU は本装置で廃棄されません。

#### (5) CDP を実装した装置間にあった L2 スイッチと本装置とを交換した場合について

CDP を実装した装置の間にあった (CDP を透過する) L2 スイッチを本装置に置き換えた場合に、本装置で CDP 受信機能を設定 (oadp cdp-listener コマンド) すると、本装置が CDP PDU を受信して透過しなくなるため、CDP を実装した装置同士がお互いを認識できなくなります。CDP 受信機能を設定 (oadp cdp-listener コマンド) しなければ、本装置は CDP PDU を受信しないで透過するので、装置を置き換える前と同様に CDP を実装した装置同士がお互いを認識できます。

#### (6) VRF 機能との共存について【OP-NPAR】

VRF を設定した VLAN に対して装置の情報を送信する場合、IP アドレスは配布しません。

## 32.2 コンフィグレーション

### 32.2.1 コンフィグレーションコマンド一覧

OADP 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 32-4 コンフィグレーションコマンド一覧

| コマンド名              | 説明                                          |
|--------------------|---------------------------------------------|
| oadp cdp-listener  | CDP 受信機能を有効にします。                            |
| oadp enable        | ポートおよびリンクアグリゲーションで OADP 機能を有効にします。          |
| oadp hold-time     | 本装置が送信する OADP フレームに対して隣接装置が保持する時間を指定します。    |
| oadp ignore-vlan   | 指定した VLAN ID から受信する OADP フレームを無視する場合に指定します。 |
| oadp interval-time | 本装置が送信する OADP フレームの送信間隔を指定します。              |
| oadp run           | 装置全体で OADP 機能を有効にします。                       |

### 32.2.2 OADP の設定

#### (1) OADP 機能の設定

##### [ 設定のポイント ]

OADP 機能のコンフィグレーションは装置全体で機能を有効にする設定と、実際に運用するポートで有効にする設定が必要です。

OADP を使用したいポートがリンクアグリゲーションを構成している場合は、ポートチャネルインタフェースに対して設定します。

ここでは、gigabitethernet 1/1 において OADP 機能を運用させます。

##### [ コマンドによる設定 ]

##### 1. (config)# oadp run

装置全体で OADP 機能を有効にします。

##### 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グレーションモードに移行します。

##### 3. (config-if)# oadp enable

ポート 1/1 で OADP 機能の動作を開始します。

##### [ 注意事項 ]

OADP は、設定したポートで有効な VLAN 上で動作します。suspend に設定されている VLAN では OADP は動作しません。

#### (2) OADP フレームの送信間隔、保持時間の設定

##### [ 設定のポイント ]

OADP フレームの送信間隔を変更すると、装置の情報の変更が反映される時間を調整できます。送信

間隔を短くすると変更が早く反映される一方で、自装置、隣接装置の負荷が高まる場合があります。送信間隔を長くすると負荷は低くなりますが変更の反映が遅くなります。通常、本設定は変更する必要はありません。

[ コマンドによる設定 ]

1. (config)# oadp interval-time 60  
OADP フレームの送信間隔を 60 秒に設定します。
2. (config)# oadp hold-time 180  
本装置が送信した情報を隣接装置が保持する時間を 180 秒に設定します。

### (3) CDP 受信機能の設定

[ 設定のポイント ]

CDP 受信機能を有効にすると、OADP が動作しているすべてのポートで CDP 受信機能が動作します。

ここでは、gigabitethernet 1/1 において CDP 受信機能を運用させます。

[ 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)# oadp enable  
ポート 1/1 で OADP 機能を有効にします。
3. (config-if)# exit  
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。
4. (config)# oadp cdp-listener  
CDP 受信機能を有効にします。OADP が動作しているポートで CDP 受信機能が動作します。

### (4) OADP フレームを無視する VLAN の設定

[ 設定のポイント ]

OADP は、トランクポートでは VLAN Tag を使用して 1 ポートに複数の OADP フレームを送受信します。トランクポートに所属している VLAN 数が増えると隣接装置情報も増加し、装置への負荷が増加します。受信した OADP フレームを無視する VLAN を設定することで装置への負荷を抑えられます。

[ コマンドによる設定 ]

1. (config)# oadp ignore-vlan 10-20  
VLAN10 ~ 20 で受信した OADP フレームを無視します。

## 32.3 オペレーション

### 32.3.1 運用コマンド一覧

OADP の運用コマンド一覧を次の表に示します。

表 32-5 運用コマンド一覧

| コマンド名                 | 説明                                                   |
|-----------------------|------------------------------------------------------|
| show oadp             | OADP/CDP の設定情報および隣接装置情報を表示します。                       |
| show oadp statistics  | OADP/CDP 統計情報を表示します。                                 |
| clear oadp            | OADP/CDP の隣接情報をクリアします。                               |
| clear oadp statistics | OADP/CDP の統計情報をクリアします。                               |
| restart oadp          | OADP プログラムを再起動します。                                   |
| dump protocols oadp   | OADP 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。 |

### 32.3.2 OADP 情報の表示

OADP 情報の表示は、運用コマンド show oadp で行います。show oadp コマンドは、OADP の設定情報とポートごとの簡易的な情報を示します。show oadp detail コマンドは、隣接装置の詳細な情報を表示します。

図 32-2 show oadp コマンドの実行結果

```
> show oadp
Date 2006/03/09 19:50:20 UTC
OADP/CDP status: Enabled/Disabled Device ID: OADP-1
Interval Time: 60 Hold Time: 180
ignore vlan: 2-4,10
Enabled Port: 1/1-5,16,20
 CH 10

Total Neighbor Counts=2
Local VID Holdtime Remote VID Device ID Capability Platform
1/1 0 35 1/8 0 OADP-2 RS AX6304S
1/16 0 9 1/1 0 OADP-3 RS AX6308S

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
 S - Switch, H - Host, I - IGMP, r - Repeater
>
```

図 32-3 show oadp detail コマンドの実行結果

```

> show oadp detail
Date 2006/03/09 19:55:52 UTC
OADP/CDP status: Enabled/Disabled Device ID: OADP-1
Interval Time: 60 Hold Time: 180
ignore vlan: 2-4,10
Enabled Port: 1/1-5,16,20

Total Neighbor Counts=2

Port: 1/1 VLAN ID: 0
Holdtime : 6(sec)
Port ID : 1/8 VLAN ID(TLV): 0
Device ID : OADP-2
Capabilities : Router, Switch
Platform : AX6304S
Entry address(es):
 IP address : 192.16.170.87
 IPv6 address: fe80::200:4cff:fe71:5d1c
IfSpeed : 1G Duplex : FULL
Version : ALAXALA AX6300S AX-6300-S04 [AX6304S] Switching software Ver.
10.2 [OS-SE]

Port: 1/16 VLAN ID: 0
Holdtime : 10(sec)
Port ID : 1/1 VLAN ID(TLV): 0
Device ID : OADP-3
Capabilities : Router, Switch
Platform : AX6308S
Entry address(es):
 IP address : 192.16.170.100
IfSpeed : 1G Duplex : FULL
Version : ALAXALA AX6300S AX-6300-S08 [AX6308S] Switching software Ver.
10.2 [OS-SE]

>

```





# 33 ポートミラーリング

ポートミラーリングは、送受信するフレームのコピーを指定した物理ポートへ送信する機能です。この章では、ポートミラーリングの解説と操作方法について説明します。

---

33.1 解説

---

33.2 コンフィグレーション

---

## 33.1 解説

### 33.1.1 ポートミラーリングの概要

ポートミラーリングは、送受信するフレームのコピーを指定した物理ポートへ送信する機能です。フレームをコピーすることをミラーリングと呼びます。この機能を利用して、ミラーリングしたフレームをアナライザなどで受信することによって、トラフィックの監視や解析ができます。

受信フレームおよび送信フレームに対するミラーリングのそれぞれの動作を次の図に示します。

図 33-1 受信フレームのミラーリング

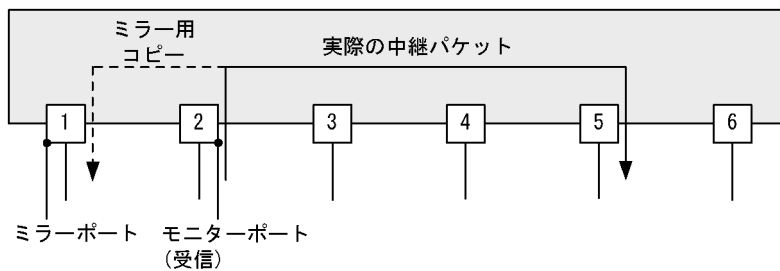
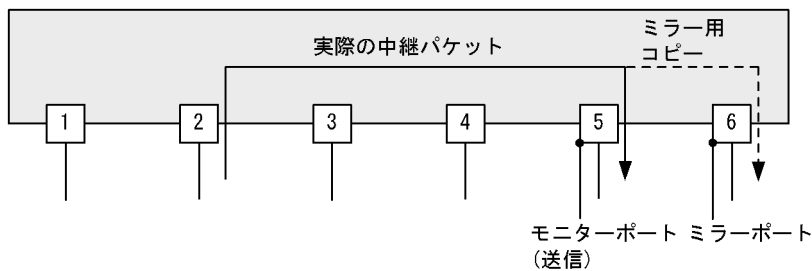


図 33-2 送信フレームのミラーリング



これらの図で示すとおり、トラフィックを監視する物理ポートをモニターポートと呼び、ミラーリングしたフレームの送信先となる物理ポートをミラーポートと呼びます。

ミラーポートからはミラーリングされたフレームだけ送信されます。それ以外の自発、自宛、中継フレームは廃棄されます。ただし、制御フレームが送信される設定をした場合、設定された制御フレームは送信されます。なお、ミラーリングしたフレームは、TTL (IPv4) またはホップリミット (IPv6) を減算しないで送信されます。

また、モニターポートとミラーポートは「多対一」の設定ができ、複数のモニターポートから受信したフレームのコピーを、一つのミラーポートへ送信できます。なお、モニターポートの受信フレームと送信フレームは別のミラーポートへ送信できます。ただし、モニターポートの受信フレームを複数のミラーポートへ送信したり、モニターポートの送信フレームを複数のミラーポートへ送信したりはできません。

なお、本装置では、ミラーリングする対象フレームをサンプリングすることができ、帯域の小さいミラーポートで、多数のモニターポートや、広帯域のモニターポートをミラーリングすることができます。

ポートミラーリングに関する運用コマンドはありません。ミラーポートに接続したアナライザで、フレームがミラーリングされていることを確認してください。

### 33.1.2 ポートミラーリングの注意事項

#### (1) 他機能との共存

- モニターポートでは、ほかの機能は制限なく動作します。
- ミラーポートでは、VLAN 機能およびレイヤ 3 通信機能が使用できません。VLAN 機能を前提とするスパンニングツリー、Ring Protocol、IGMP snooping/MLD snooping などの機能や、レイヤ 3 通信機能を前提とする SNMP、DHCP などの機能も使用できません。
- ミラーポートに制御フレームが送信される機能を設定すると、コピーされたフレームのほかに設定された制御フレームが送信されます。

#### (2) ポートミラーリング使用時の注意事項

- ポートミラーリングでコピーしたフレームは、ミラーポートの回線帯域を超えて出力することはできません。
- 受信したフレームの FCS が不正な場合、該当フレームはミラーリングされません。
- 送信フレームのミラーリングでは、次に示す動作をすることがあります。
  - モニターポートから送信されるフレームの順序と異なる順序で送信される
  - モニターポートから送信されるフレームがミラーリングされない
  - 廃棄するフレームがミラーリングされる
- フィルタ/QoS 制御やストームコントロールを設定しているポートをモニターポートに設定できます。この場合、モニターポートでの通信に影響はありません。
- フィルタを設定したポートをミラーリングした場合、受信フレームはフィルタの設定に関係なくミラーリングされます。送信フレームは廃棄対象のフレームがミラーリングされません。
- 送信フレームのミラーリングでは、ソフトウェアで送信するフレーム（自発、IP オプション付きパケットなど）を含めて、すべてのユーザ通信パケットをミラーリングします。本装置が送信する一部の制御フレームはミラーリングしません。受信フレームのミラーリングでは、自宛フレームや IP オプション付きパケット、制御フレームなどを含めた、すべての受信フレームをミラーリングします。
- 階層化シェーパのポートをミラーポートにする場合は、次の条件を満たすよう設定してください。
  - [ 送信フレームをミラーリングする場合 ]
    - モニターポートが階層化シェーパのポートの場合、モニターポートとミラーポートで同じ設定をしてください。モニターポートがレガシーシェーパのポートの場合、ミラーポートにデフォルトユーザを設定してください。
    - 複数の階層化シェーパのポートをモニターポートに設定して一つのミラーポートへ送信する場合、すべてのモニターポートで同じ階層化シェーパの設定をしてください。
  - [ 受信フレームをミラーリングする場合 ]
    - デフォルトユーザのユーザリストを設定してください。
  - [ 送受信フレームをミラーリングする場合 ]
    - デフォルトユーザのユーザリストを設定してください。
    - モニターポートが階層化シェーパのポートの場合、モニターポートとミラーポートで同じ設定をしてください。
    - 複数の階層化シェーパのポートをモニターポートに設定して一つのミラーポートへ送信する場合、すべてのモニターポートで同じ階層化シェーパの設定をしてください。

## 33.2 コンフィグレーション

### 33.2.1 コンフィグレーションコマンド一覧

ポートミラー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 33-1 コンフィグレーションコマンド一覧

| コマンド名           | 説明                        |
|-----------------|---------------------------|
| monitor option  | ポートミラーリングのサンプリング係数を設定します。 |
| monitor session | ポートミラーリングを設定します。          |

### 33.2.2 ポートミラーリングの設定

ポートミラーリングのコンフィグレーションでは、モニターポートとミラーポートの組み合わせをモニターセッションとして設定します。

設定したモニターセッションを削除する場合は、設定時のセッション番号を指定して削除します。設定済みのセッション番号を指定すると、モニターセッションの設定内容は変更されて、以前のモニターセッションの情報は無効になります。

モニターポートには、通信で使用するポートを指定します。ミラーポートには、トラフィックの監視や解析などのために、アナライザなどを接続するポートを指定します。ミラーポートではポートミラーリング以外の通信はできません。

ポートミラーリングでサンプリング機能を使用する場合は、サンプリング係数を設定します。

#### (1) 受信フレームのミラーリング

##### [ 設定のポイント ]

設定できるインタフェースはイーサネットインタフェースです。リンクアグリゲーションで使用している場合も、単独のイーサネットインタフェースを指定します。また、ミラーポートは VLANなどを設定していないポートに設定します。

##### [ コマンドによる設定 ]

1. (config)# monitor session 2 source interface gigabitethernet 1/1 rx destination interface gigabitethernet 1/5

アナライザをポート 1/5 に接続し、1G ビットイーサネットインタフェース 1/1 で受信するフレームをミラーリングすることを設定します。セッション番号は 2 を使用します。

#### (2) 送信フレームのミラーリング

##### [ 設定のポイント ]

設定できるインタフェースはイーサネットインタフェースです。リンクアグリゲーションで使用している場合も、単独のイーサネットインタフェースを指定します。また、ミラーポートは VLANなどを設定していないポートに設定します。

##### [ コマンドによる設定 ]

1. (config)# monitor session 1 source interface gigabitethernet 1/2 tx destination interface gigabitethernet 1/6

アナライザをポート 1/6 に接続し、1G ビットイーサネットインタフェース 1/2 で送信するフレームをミラーリングすることを設定します。セッション番号は 1 を使用します。

### (3) 送受信フレームのミラーリング

#### [ 設定のポイント ]

設定できるインタフェースはイーサネットインタフェースです。リンクアグリゲーションで使用している場合も、単独のイーサネットインタフェースを指定します。また、ミラーポートは VLAN などを設定していないポートに設定します。

#### [ コマンドによる設定 ]

1. (config)# monitor session 1 source interface gigabitethernet 1/3 both destination interface gigabitethernet 1/11

アナライザをポート 1/11 に接続し、1G ビットイーサネットインタフェース 1/3 で送受信するフレームをミラーリングすることを設定します。セッション番号は 1 を使用します。

### (4) サンプルミラーリング

#### [ 設定のポイント ]

ミラーリングのサンプリング係数を設定します。サンプリング係数は本装置の全ミラーリングに有効となります。

#### [ コマンドによる設定 ]

1. (config)# monitor option sample 32

ミラーリングのサンプリング係数を 32 に設定します。モニター対象フレームは、32 分の 1 の確率でミラーリングされます。

2. (config)# monitor session 1 source interface gigabitethernet 1/1-24 both destination interface gigabitethernet 3/1

アナライザをポート 3/1 に接続し、1G ビットイーサネットインタフェース 1/1 から 1/24 までのポートで送受信するフレームをミラーリングすることを設定します。

### (5) 送受信フレームの別ポートへのミラーリング

#### [ 設定のポイント ]

モニターポートの送信ミラーリングと受信ミラーリングを別のミラーポートに設定します。

#### [ コマンドによる設定 ]

1. (config)# monitor session 1 source interface gigabitethernet 1/3 rx destination interface gigabitethernet 1/11

(config)# monitor session 2 source interface gigabitethernet 1/3 tx destination interface gigabitethernet 1/12

1G ビットイーサネットインタフェース 1/3 で受信するフレームを 1/11 にミラーリングし、1/3 で送信するフレームを 1/12 にミラーリングすることを設定します。セッション番号は 1 と 2 を使用します。



# 付録

---

付録 A 準拠規格

## 付録 A 準拠規格

### 付録 A.1 uRPF

表 A-1 uRPF の準拠する規格および勧告

| 規格番号 (発行年月)      | 規格名                                       |
|------------------|-------------------------------------------|
| RFC3704(2004年3月) | Ingress Filtering for Multihomed Networks |

### 付録 A.2 Diff-serv

表 A-2 Diff-serv の準拠規格および勧告

| 規格番号 (発行年月)       | 規格名                                                                                    |
|-------------------|----------------------------------------------------------------------------------------|
| RFC2474(1998年12月) | Definition of the Differentiated Services Field(DS Field) in the IPv4 and IPv6 Headers |
| RFC2475(1998年12月) | An Architecture for Differentiated Services                                            |
| RFC2597(1999年6月)  | Assured Forwarding PHB Group                                                           |
| RFC3246(2002年3月)  | An Expedited Forwarding PHB (Per-Hop Behavior)                                         |
| RFC3260(2002年4月)  | New Terminology and Clarifications for Diffserv                                        |

### 付録 A.3 IEEE802.1X

表 A-3 IEEE802.1X の準拠規格および勧告

| 規格番号 (発行年月)         | 規格名                                                                              |
|---------------------|----------------------------------------------------------------------------------|
| IEEE802.1X(2001年6月) | Port-Based Network Access Control                                                |
| RFC2865(2000年6月)    | Remote Authentication Dial In User Service (RADIUS)                              |
| RFC2866(2000年6月)    | RADIUS Accounting                                                                |
| RFC2868(2000年6月)    | RADIUS Attributes for Tunnel Protocol Support                                    |
| RFC2869(2000年6月)    | RADIUS Extensions                                                                |
| RFC3162(2001年8月)    | RADIUS and IPv6                                                                  |
| RFC3579(2003年9月)    | RADIUS Support For Extensible Authentication Protocol (EAP)                      |
| RFC3580(2003年9月)    | IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines |
| RFC3748(2004年6月)    | Extensible Authentication Protocol (EAP)                                         |

### 付録 A.4 Web 認証

表 A-4 Web 認証の準拠規格および勧告

| 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                                   |



| 規格番号 (発行年月)      | 規格名             |
|------------------|-----------------|
| RFC3162(2001年8月) | RADIUS and IPv6 |

## 付録 A.5 MAC 認証

表 A-5 MAC 認証の準拠規格および勧告

| 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                                     |

## 付録 A.6 DHCP snooping

表 A-6 DHCP snooping の準拠規格および勧告

| 規格番号 (発行年月)      | 規格名                                 |
|------------------|-------------------------------------|
| RFC2131(1997年3月) | Dynamic Host Configuration Protocol |

## 付録 A.7 VRRP

表 A-7 VRRP の準拠規格および勧告

| 規格番号 (発行年月)                                  | 規格名                                                            |
|----------------------------------------------|----------------------------------------------------------------|
| RFC3768(2004年4月)                             | Virtual Router Redundancy Protocol                             |
| draft-ietf-vrrp-ipv6-spec-02<br>(2002年3月)    | Virtual Router Redundancy Protocol for IPv6                    |
| draft-ietf-vrrp-ipv6-spec-07<br>(2004年10月)   | Virtual Router Redundancy Protocol for IPv6                    |
| draft-ietf-vrrp-unified-spec-02<br>(2008年4月) | Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6 |

## 付録 A.8 IEEE802.3ah/UDLD

表 A-8 IEEE802.3ah/UDLD の準拠規格および勧告

| 規格番号 (発行年月)          | 規格名                                                                                                                                                                                                                                            |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IEEE802.3ah(2004年9月) | Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks |

## 付録 A.9 CFM

表 A-9 CFM の準拠規格および勧告

| 規格番号 (発行年月)                | 規格名                                                                            |
|----------------------------|--------------------------------------------------------------------------------|
| IEEE802.1ag-2007(2007年12月) | Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management |

## 付録 A.10 SNMP

表 A-10 SNMP の準拠規格および勧告

| 規格番号 (発行年月)       | 規格名                                                                                                  |
|-------------------|------------------------------------------------------------------------------------------------------|
| RFC1155(1990年5月)  | Structure and Identification of Management Information for TCP/IP-based Internets                    |
| RFC1157(1990年5月)  | A Simple Network Management Protocol (SNMP)                                                          |
| RFC1901(1996年1月)  | Introduction to Community-based SNMPv2                                                               |
| RFC1902(1996年1月)  | Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2) |
| RFC1903(1996年1月)  | Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)                 |
| RFC1904(1996年1月)  | Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)              |
| RFC1905(1996年1月)  | Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)                 |
| RFC1906(1996年1月)  | Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)                  |
| RFC1907(1996年1月)  | Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)         |
| RFC1908(1996年1月)  | Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework    |
| RFC2578(1999年4月)  | Structure of Management Information Version 2 (SMIv2)                                                |
| RFC2579(1999年4月)  | Textual Conventions for SMIv2                                                                        |
| RFC2580(1999年4月)  | Conformance Statements for SMIv2                                                                     |
| RFC3410(2002年12月) | Introduction and Applicability Statements for Internet Standard Management Framework                 |
| RFC3411(2002年12月) | An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks       |
| RFC3412(2002年12月) | Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)                 |
| RFC3413(2002年12月) | Simple Network Management Protocol (SNMP) Applications                                               |
| RFC3414(2002年12月) | User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)     |
| RFC3415(2002年12月) | View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)             |
| RFC3416(2002年12月) | Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)               |
| RFC3417(2002年12月) | Transport Mappings for the Simple Network Management Protocol (SNMP)                                 |

| 規格番号 (発行年月)      | 規格名                                                                                                            |
|------------------|----------------------------------------------------------------------------------------------------------------|
| RFC3584(2003年8月) | Coexistence between Version 1, Version 2, and Version 3 of the Internet- standard Network Management Framework |

表 A-11 MIB の準拠規格および勧告

| 規格番号 (発行年月)                | 規格名                                                                                                             |
|----------------------------|-----------------------------------------------------------------------------------------------------------------|
| IEEE8023-LAG-MIB(2000年3月)  | Aggregation of Multiple Link Segments                                                                           |
| IEEE8021-PAE-MIB(2001年6月)  | Port-Based Network Access Control                                                                               |
| IEEE8021-CFM-MIB(2007年12月) | Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management                                  |
| RFC1158(1990年5月)           | Management Information Base for Network Management of TCP/IP-based internets: MIB-II                            |
| RFC1213(1991年3月)           | Management Information Base for Network Management of TCP/IP-based internets: MIB-II                            |
| RFC1354(1992年7月)           | IP Forwarding Table MIB                                                                                         |
| RFC1493(1993年6月)           | Definitions of Managed Objects for Bridges                                                                      |
| RFC1643(1994年7月)           | Definitions of Managed Objects for the Ethernet-like Interface Types                                            |
| RFC1657(1994年7月)           | Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIV2        |
| RFC1757(1995年2月)           | Remote Network Monitoring Management Information Base                                                           |
| RFC1850(1995年11月)          | OSPF Version2 Management Information Base                                                                       |
| RFC2233(1997年11月)          | The Interfaces Group MIB using SMIV2                                                                            |
| RFC2452(1998年12月)          | IP Version 6 Management Information Base for the Transmission Control Protocol                                  |
| RFC2454(1998年12月)          | IP Version 6 Management Information Base for the User Datagram Protocol                                         |
| RFC2465(1998年12月)          | Management Information Base for IP Version 6: Textual Conventions and General Group                             |
| RFC2466(1998年12月)          | Management Information Base for IP Version 6: ICMPv6 Group                                                      |
| RFC2674(1999年8月)           | Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions |
| RFC2787(2000年3月)           | Definitions of Managed Objects for the Virtual Router Redundancy Protocol                                       |
| RFC2934(2000年10月)          | Protocol Independent Multicast MIB for IPv4                                                                     |
| RFC3411(2002年12月)          | An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks                  |
| RFC3412(2002年12月)          | Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)                            |
| RFC3413(2002年12月)          | Simple Network Management Protocol (SNMP) Applications                                                          |
| RFC3414(2002年12月)          | User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)                |
| RFC3415(2002年12月)          | View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)                        |
| RFC3418(2002年12月)          | Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)                             |

| 規格番号 (発行年月)                                 | 規格名                                                            |
|---------------------------------------------|----------------------------------------------------------------|
| draft-ietf-ospf-ospfv3-mib-03<br>(2000年11月) | Management Information Base for OSPFv3                         |
| draft-ietf-vrrp-unified-mib-04<br>(2005年9月) | Definitions of Managed Objects for the VRRP over IPv4 and IPv6 |

## 付録 A.11 SYSLOG

表 A-12 SYSLOG の準拠する規格および勧告

| 規格番号 (発行年月)      | 規格名                     |
|------------------|-------------------------|
| RFC3164(2001年8月) | The BSD syslog Protocol |

## 付録 A.12 sFlow

表 A-13 sFlow の準拠規格および勧告

| 規格番号 (発行年月)      | 規格名                                                                                        |
|------------------|--------------------------------------------------------------------------------------------|
| RFC3176(2001年9月) | InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks |

## 付録 A.13 LLDP

表 A-14 LLDP の準拠規格および勧告

| 規格番号 (発行年月)                | 規格名                                                                                                           |
|----------------------------|---------------------------------------------------------------------------------------------------------------|
| IEEE802.1AB/D6.0(2003年10月) | Draft Standard for Local and Metropolitan Networks: Station and Media Access Control - Connectivity Discovery |

---

# 索引

## A

---

absolute 方式〔MIB 監視〕 557  
Acct-Terminate-Cause での切断要因 171  
ADVERTISEMENT パケットの送信 448  
ADVERTISEMENT パケットの認証 449  
alarm グループ 557  
ARP パケットの受信レート制限 346

## B

---

BCU/CSU/MSU の冗長化 365  
BSU の冗長化 375  
BSU の冗長構成を管理する上で必要な運用コマンド  
一覧 385  
BSU の冗長構成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 382

## C

---

CC 520  
CCM 520  
CDP でサポートする情報 610  
CFM 509  
CFM で使用するデータベース 528  
CFM の運用コマンド一覧 536  
CFM のコンフィグレーションコマンド一覧 532  
Chassis ID (装置の識別子) 601  
Chassis ID の subtype 一覧 601  
Continuity Check 520

## D

---

delta 方式〔MIB 監視〕 557  
DHCP snooping 333  
DHCP snooping の運用コマンド一覧 359  
DHCP snooping のコンフィグレーションコマンド  
一覧 349  
DHCP パケットの監視 335  
DHCP パケットの受信レート制限 340  
Down MEP 513

## E

---

EAP-Request/Identity フレーム送信の時間間隔設定  
193  
event グループ 559

## G

---

GetBulkRequest オペレーション 547  
GetNextRequest オペレーション 546  
GetRequest オペレーション 545  
GSRP の運用コマンド一覧 441  
GSRP の解説 403  
GSRP のコンフィグレーションコマンド一覧 432  
GSRP の設定と運用 431

## H

---

history グループ 557

## I

---

IEEE802.1X 基本構成 166  
IEEE802.1X 状態の表示 196  
IEEE802.1X 認証状態の変更 198  
IEEE802.1X の解説 165  
IEEE802.1X の概要 166  
IEEE802.1X の基本的な設定 187  
IEEE802.1X のコンフィグレーションコマンド一覧  
186  
IEEE802.1X の状態を確認する運用コマンド一覧  
196  
IEEE802.1X の設定と運用 185  
IEEE802.3ah/OAM 機能の運用コマンド一覧 488  
IEEE802.3ah/UDLD 483  
IEEE802.3ah/UDLD のコンフィグレーションコマン  
ド一覧 486  
Inform 555  
IPv4/IPv6 SNMP マネージャからの MIB 要求と応答  
の例 542  
IP アドレスによるオペレーション制限 550

## L

---

L2 ループ検知 497  
L2 ループ検知の運用コマンド一覧 507  
L2 ループ検知のコンフィグレーションコマンド一覧  
504  
Linktrace 523  
LLDP 599  
LLDP 使用時の注意事項 602  
LLDP でサポートする情報 600  
LLDP の運用コマンド一覧 605  
LLDP のコンフィグレーションコマンド一覧 604  
LLDP の適用例 600

Loopback 522

## M

---

MA 512

MAC 認証の運用コマンド一覧 310

MAC 認証の解説 283

MAC 認証のコンフィグレーションコマンド一覧 300

MAC 認証の設定と運用 299

MEP 513

MIB オブジェクトの表し方 544

MIB 概説 543

MIB 構造 544

MIB 取得の例 541

MIB を設定できない場合の応答 548

MIP 514

## N

---

NIF の冗長化 395

NIF の冗長構成を管理する上で必要な運用コマンド一覧 401

NIF の冗長構成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 399

## O

---

OADP 607

OADP 使用時の注意事項 610

OADP でサポートする項目・仕様 609

OADP でサポートする情報 609

OADP の運用コマンド一覧 614

OADP のコンフィグレーションコマンド一覧 612

Organizationally-defined TLV extensions 602

## P

---

Port description (ポート種別) 602

Port ID (ポート識別子) 601

Port ID の subtype 一覧 601

PSP の冗長化 387

PSP の冗長構成を管理する上で必要な運用コマンド一覧 393

PSP の冗長構成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 392

PS 管理の運用コマンド一覧 363

PS 管理のコンフィグレーションコマンド一覧 363

## Q

---

QoS 制御共通の運用コマンド一覧 52

QoS 制御共通のコンフィグレーションコマンド一覧 50

QoS 制御構造 48

QoS 制御の概要 47

QoS 制御の各機能ブロックの概要 48

## R

---

RADIUS Accounting がサポートする属性 170

RADIUS サーバ関連の設定 195

RADIUS サーバ接続機能 180

RMON MIB 556

## S

---

SetRequest オペレーション 547

sFlow 統計 (フロー統計) 機能 575

sFlow 統計で使用する運用コマンド一覧 594

sFlow 統計で使用するコンフィグレーションコマンド一覧 586

shortcut, disable の EAP-Request/Identity のシーケンス 179

SNMP/RMON に関する運用コマンド一覧 568

SNMP/RMON に関するコンフィグレーションコマンド一覧 560

SNMPv1, SNMPv2C オペレーション 545

SNMPv3 オペレーション 551

SNMPv3 でのオペレーション制限 553

SNMPv3 による MIB アクセス許可の設定 561

SNMP エージェント 540

SNMP エンジン 542

SNMP エンティティ 542

SNMP オペレーションのエラーステータスコード 550

SNMP 概説 540

SNMP マネージャとの接続時の注意事項 559

SNMP を使用したネットワーク管理 539

statistics グループ 556

syslog サーバへの出力設定 195

System description (装置種別) 602

System name (装置名称) 602

## T

---

Time-to-Live (情報の保持時間) 601

Trap 554

trust ポート [DHCP パケットの監視] 335

trust ポート [ダイナミック ARP 検査] 343

## U

---

untrust ポート [DHCP パケットの監視] 335

untrust ポート〔ダイナミック ARP 検査〕 343  
 Up MEP 513  
 uRPF 39  
 uRPF で使用する運用コマンド一覧 45  
 uRPFで使用するコンフィグレーションコマンド一覧  
 43

## V

VLAN 単位認証 (静的) 174  
 VLAN 単位認証 (静的)での認証除外ポート設定例  
 178  
 VLAN 単位認証 (動的) 174  
 VLAN 単位認証 (動的)で VLAN を動的に割り当て  
 るときの設定 180  
 VLAN 単位認証 (動的)での MAC アドレス学習の  
 エージング時間設定について 182  
 VLAN 単位認証 (動的)での認証除外端末構成例  
 177  
 VRRP 445  
 VRRP における障害検出の仕組み 448  
 VRRP の運用コマンド一覧 480  
 VRRP のコンフィグレーションコマンド一覧 465  
 VRRP のコンフィグレーションの流れ 466  
 VRRP ボーリング 452

## W

Web 認証の運用コマンド一覧 263  
 Web 認証の解説 199  
 Web 認証のコンフィグレーションコマンド一覧 234  
 Web 認証の設定と運用 233

## あ

アクセスリストロギング 25  
 アクセスリストロギングの運用コマンド一覧 36  
 アクセスリストロギングのコンフィグレーションコマ  
 ンド一覧 33  
 アクセスリストログ 26  
 アクセスリストログ情報 26  
 アクセプトモード 450

## い

インデックス 544  
 インフォーム 555  
 インフォーム概説 555  
 インフォームリクエストフォーマット 556

## う

運用系システム, 待機系システムを管理する上で必要  
 な運用コマンド一覧 373

## え

エラーステータスコード 550

## お

オペレーション 480

## か

階層化シェーバ 107  
 仮想 MAC 宛てフレームの受信 447  
 仮想 MAC アドレスによる ARP 応答および NDP 応  
 答 447  
 仮想ルータの MAC アドレスと IP アドレス 446

## き

基本認証モード 173  
 強制的な再認証 198

## こ

コミュニティによるオペレーション 550  
 コミュニティによるオペレーション制限 549  
 コンフィグレーション〔VRRP〕 465

## さ

サポート仕様〔LLDP〕 600  
 サポート仕様〔OADP〕 609  
 サポートする認証アルゴリズム 169

## し

自動切り戻しおよび自動切り戻しの抑止 449  
 受信フレームのミラーリング 618  
 障害監視インタフェース 451  
 障害監視インタフェースと VRRP ボーリングの設定  
 470

## す

ストームコントロール 491  
 ストームコントロールのコンフィグレーションコマ  
 ンド一覧 494  
 スレッシュホールド機能〔アクセスリストロギング〕  
 27

## そ

---

送信制御 97  
送信フレームのミラーリング 618

## た

---

帯域監視 69  
帯域監視の位置づけ 69  
ダイナミック ARP 検査 343  
端末からの認証要求を抑止する機能の設定 192  
端末検出動作切り替えオプション 178  
端末検出動作の切替設定 190  
端末との間に L2 スイッチを配置した IEEE802.1X 構成 167  
端末フィルタ 341  
端末へ再認証を要求する機能の設定 191  
端末への EAP-Request フレーム再送の設定 191  
端末要求再認証抑止機能 180

## て

---

電源機構 ( P S ) の冗長化 361

## と

---

ドメイン 511  
トラッキング機能 450  
トラップ 554  
トラップ概説 554  
トラップの例 541  
トラップフォーマット ( SNMPv1 ) 555  
トラップフォーマット ( SNMPv2C , SNMPv3 ) 555

## な

---

内蔵 MAC 認証 DB 284  
内蔵 Web 認証 DB 200

## に

---

認証 VLAN 313  
認証 VLAN の運用コマンド一覧 332  
認証 VLAN のコンフィグレーションコマンド一覧 323  
認証後 VLAN ( MAC 認証 ) 284  
認証後 VLAN ( Web 認証 ) 200  
認証サーバ応答待ち時間のタイマ設定 194  
認証サブモード 176  
認証失敗時の認証処理再開までの待機時間設定 193  
認証状態の初期化 198  
認証除外端末オプションの設定 188  
認証除外ポートオプションの設定 189

認証処理に関する設定 191  
認証端末数制限オプション 178  
認証端末数制限の設定 189  
認証で使用する属性名 167  
認証前 VLAN ( MAC 認証 ) 284  
認証前 VLAN ( Web 認証 ) 200  
認証モード 173  
認証モードオプション 177  
認証モードオプションの設定 188  
認証モードとオプションの関係 173

## ね

---

ネットワーク管理 540

## は

---

バインディングデータベース 334

## ひ

---

標準 MIB 543

## ふ

---

フィルタ 1  
フィルタで使用する運用コマンド一覧 22  
フィルタで使用するコンフィグレーションコマンド一覧 16  
フィルタを使用したネットワーク構成例 2  
フォロー仮想ルータ 459  
複数端末からの認証要求時の通信遮断時間の設定 194  
プライベート MIB 543  
プライマリ VLAN 513  
プライマリ仮想ルータ 459  
フロー制御 53

## ほ

---

ポート単位認証 173  
ポート単位認証の構成例 174  
ポートミラーリング 617  
ポートミラーリングのコンフィグレーションコマンド一覧 620  
本装置のサポート MIB 545

## ま

---

マーカー 79  
マーカーの位置づけ 79  
マスタの選出方法 448



## み

---

ミラーポート 618

ミラーリング 618

## も

---

モニターポート 618

## ゆ

---

ユーザ認証とプライバシー機能 542

優先度 448

優先度決定 85

## れ

---

レイヤ2 認証 145

レイヤ2 認証のコンフィグレーションコマンド一覧  
164

レガシーシェーパ 98

## ろ

---

ログ出力インターバル機能〔アクセスリストロギン  
グ〕 27

ログ出力機能 571

ログ出力機能に関するコンフィグレーションコマンド  
一覧 573