AX2630S ソフトウェアマニュアル

コンフィグレーションガイド Vol.2

Ver. 2.7 対応

AX26S-S002-60

■対象製品

このマニュアルは AX2630S を対象に記載しています。また，ソフトウェア OS-L2N Ver.2.7 の機能について記載しています。

■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，富士フイルムビジネスイノベーション株式会社の登録商標です。
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。
OpenSSL は，米国およびその他の国における米国 OpenSSL Software Foundation の登録商標です。
Python は，Python Software Foundation の登録商標です。
RSA および RC4 は，米国およびその他の国における米国 EMC Corporation 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。
ssh は，SSH Communications Security,Inc.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。
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，富士フイルムビジネスイノベーション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

２０２４年　１２月　（第７版）　ＡＸ２６Ｓ－Ｓ００２－６０

■著作権

変更内容

【Ver. 2.7 対応版】

表　変更内容

章・節・項・タイトル	追加・変更内容
5.3.3　強制認証	・IEEE802.1X も対応しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 2.6 対応版】

表　変更内容

章・節・項・タイトル	追加・変更内容
送信キュー長指定	・送信キュー長指定のサポートに伴い，記述を変更しました。
RADIUS サーバ通信の dead interval 機能	・IEEE802.1X も対応しました。
RADIUS 認証方式のダイナミック VLAN モードにおける認証後 VLAN の決定	・本項を追加しました。

【Ver. 2.5 対応版】

表　変更内容

章・節・項・タイトル	追加・変更内容
同一ポート内での共存	・Web 認証の MAC ポート＋dot1q 設定のサポートを拡張しました。
MAC ポートに dot1q 設定時の動作	・Web 認証の MAC ポート＋dot1q 設定のサポート拡張に対応しました。
ダイナミック ACL/QoS	・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コマンドのパラメータ設定	・ダイナミック ACL/QoS の設定例を追加しました。
ユーザ切り替えオプション	・本項を追加しました。
Web 認証のパラメータ設定	・ユーザ切り替えオプションの設定例を追加しました。
流量制限	・本項を追加しました。
ポート閉塞時の自動復旧	・本項を追加しました。
流量制限の設定	・本項を追加しました。
ポート閉塞時の自動復旧の設定	・本項を追加しました。

【Ver. 2.4 対応版】

表　変更内容

項目	追加・変更内容
認証前端末の通信許可	・認証専用アクセスリスト数の拡張に伴い，記述を変更しました。
認証解除方式	・無通信監視による認証解除の記述を追加しました。
認証ネットワークからのログアウト	・リンクダウンによる認証解除のサポートを拡張しました。
RADIUS サーバの準備	・RADIUS 属性 ID のサポート項目を追加しました。
Web 認証画面入れ替え機能	・Web 認証画面の複数サポートに伴い，記述を変更をしました。
定期的再認証要求	・本項を追加しました。
認証解除方式	・定期的再認証要求による認証解除を追加しました。

項目	追加・変更内容
	・リンクダウンによる認証解除のサポートを拡張しました。
RADIUS サーバの準備	・RADIUS 属性 ID のサポート項目を追加しました。
認証端末の管理と認証解除	・IEEE802.1X の無通信監視による認証解除の記述を追加しました。

【Ver. 2.3 対応版】

表　変更内容

項目	追加・変更内容
同一ポート内での共存	・IEEE802.1X の固定 VLAN モードで，同一ポート内で共存できるポートの種類にトランクポートを追加しました。
認証モード	・「(1) 基本認証モード」で，固定 VLAN モードとダイナミック VLAN モードで設定できるポートの種類の記述を追加しました。
認証失敗後の動作	・再認証時間間隔を経過後に認証処理を行う時間を変更しました。

【Ver. 2.2 対応版】

表　変更内容

項目	追加・変更内容
レイヤ 2 認証	・認証対象ポートにチャネルグループをサポートしたことに伴い，記述を変更しました。 ・IGMP snooping との共存時の記述を変更しました。 ・認証専用 MAC アクセスリストの記述を追加しました。 ・認証対象外ポートへ移動時の認証解除について記述を追加しました。 ・リンクダウン時の認証解除の抑止について記述を追加しました。
認証解除方式	・本項を追加しました。
コマンドガイド	・IEEE802.1X 専用の RADIUS サーバ指定の記述を追加しました。
コマンドガイド	・Web 認証専用の RADIUS サーバ指定の記述を追加しました。
概要	・DHCP snooping でのスタック構成時の記述を追加しました。
DHCP パケットの監視	・DHCP snooping でのスタック構成時の記述を追加しました。
サポート仕様	・アップリンク・リダンダントのサポート仕様にスタック構成時の記述を追加しました。

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 AX2630S を対象に記載しています。また，ソフトウェア OS-L2N Ver.2.7 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ています。
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使いやすい場所に保管してください。

■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。
https://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。

●ハードウェアの設備条件，取扱方法を調べる

ハードウェア取扱説明書 （AX26S-H001）

トランシーバ ハードウェア取扱説明書 （AX-COM-H001）

●ソフトウェアの機能とコマンド，コンフィグレーションの設定を知りたい

コンフィグレーションガイド Vol.1 （AX26S-S001）

Vol.2 （AX26S-S002）

●コンフィグレーションコマンドの入力シンタックス，パラメータ詳細について知りたい

コンフィグレーション コマンドレファレンス （AX26S-S003）

●運用コマンドの入力シンタックス，パラメータ詳細について知りたい

運用コマンドレファレンス （AX26S-S004）

●メッセージとログについて調べる

メッセージ・ログレファレンス （AX26S-S005）

●MIBについて調べる

MIBレファレンス （AX26S-S006）

●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 （AX23S-T001）

■このマニュアルでの表記

AC	Alternating Current
ACK	ACKnowledge
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
bit/s	bits per second　*bps と表記する場合もあります。
BPDU	Bridge Protocol Data Unit
CA	Certificate Authority
CBC	Cipher Block Chaining
CC	Continuity Check
CFM	Connectivity Fault Management
CIST	Common and Internal Spanning Tree
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CST	Common Spanning Tree
DA	Destination Address

DC	Direct Current
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DRR	Deficit Round Robin
DSA	Digital Signature Algorithm
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DSS	Digital Signature Standard
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
ECDHE	Elliptic Curve Diffie-Hellman key exchange, Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EEE	Energy Efficient Ethernet
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
GCM	Galois/Counter Mode
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
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
MLD	Multicast Listener Discovery
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NDP	Neighbor Discovery Protocol
NTP	Network Time Protocol
OAM	Operations,Administration,and Maintenance
OUI	Organizationally Unique Identifier
packet/s	packets per second　　*pps と表記する場合もあります。
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PDU	Protocol Data Unit
PGP	Pretty Good Privacy
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PoE	Power over Ethernet
PQ	Priority Queueing
PS	Power Supply
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RMON	Remote Network Monitoring MIB
RQ	ReQuest
RSA	Rivest, Shamir, Adleman
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SFP+	enhanced Small Form-factor Pluggable
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SSAP	Source Service Access Point
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
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
USB	Universal Serial Bus
VLAN	Virtual LAN
WAN	Wide Area Network
WWW	World-Wide Web

■KB（キロバイト）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

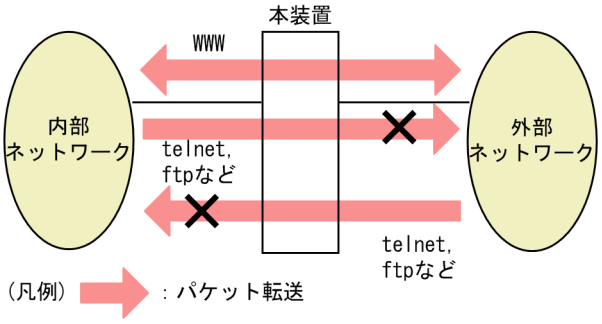
1 フィルタ

フィルタは，ある特定の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

フィルタは，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。

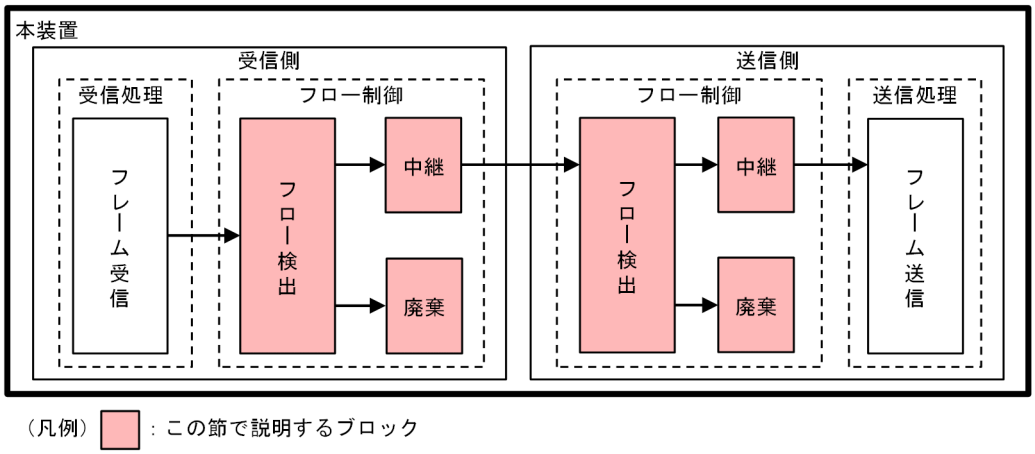
図 1-1　フィルタを使用したネットワーク構成例



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



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，ICMP ヘッダ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，ICMP ヘッダ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，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。

注意

受信側インタフェースでフレームが廃棄された場合，送信側インタフェースではフロー検出しません。

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，ICMP 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および VLAN インタフェースに対してアクセスリストを設定できます。アクセスリストを設定したイーサネットインタフェース，VLAN インタフェースともに，レイヤ 2 中継のイーサネット V2 形式および IEEE802.3 の SNAP/RFC1042 形式フレームをフロー検出できます。

受信側インタフェースでフロー検出を指定した場合，イーサネットインタフェース，VLAN インタフェースともに，イーサネットインタフェースで受信した段階でフロー検出します。なお，本装置宛ての受信フレームもフロー検出対象です。

送信側インタフェースでフロー検出を指定した場合，イーサネットインタフェース，VLAN インタフェースともに，イーサネットインタフェースで送信する段階でフロー検出します。なお，本装置が自発的に送信するフレームもフロー検出対象です。

1.1.3 フロー検出モード

本装置では，ネットワーク構成や運用形態を想定してフロー検出モードを用意しています。フロー検出モードは，フィルタ・QoS・ポリシーベースミラーリングのエントリの配分パターンを決めるモードです。エントリの配分については「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，使い方に合わせてモードを選択してください。

フロー検出モードは flow detection mode コマンドで指定します。なお，選択したフロー検出モードはフィルタ・QoS・ポリシーベースミラーリング，かつ受信側と送信側で共通です。フロー検出モードを変更する場合，インタフェースに設定された次のコマンドをすべて削除する必要があります。

- mac access-group
- ip access-group
- ipv6 traffic-filter
- mac qos-flow-group
- ip qos-flow-group
- ipv6 qos-flow-group

なお，フロー検出モードを指定しない場合，layer2-1 がデフォルトのモードとして設定されます。

フロー検出モードとフロー動作の関係を次の表に示します。

表 1-2　フロー検出モードとフロー動作の関係

フロー検出モード名称	運用目的	フロー動作
layer2-1	MAC ヘッダ（VLAN Tag 含む）でフィルタを使用したい	すべてのフレームを対象に，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。
layer2-2	IPv4 ヘッダ，L4 ヘッダでフィルタを使用したい	IPv4 パケットについて，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。
layer2-3	IPv4 ヘッダ，IPv6 ヘッダ，L4 ヘッダでフィルタを使用したい	IPv4 パケットまたは IPv6 パケットについて，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。
layer2-1-mirror	MAC ヘッダ（VLAN Tag 含む）でフィルタおよびポリシーベースミラーリングを使用したい	すべてのフレームを対象に，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。
layer2-2-mirror	IPv4 ヘッダ，L4 ヘッダでフィルタおよびポリシーベースミラーリングを使用したい	IPv4 パケットについて，IP ヘッダ，TCP/UDP ヘッダ，ICMP 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。受信側および送信側インタフェースでのフロー検出条件を次に示します。

(1)　受信側インタフェースのフロー検出条件

受信側インタフェースで指定できるフロー検出条件を次の表に示します。

表 1-3　受信側インタフェースで指定できるフロー検出条件

種別		設定項目
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
		ユーザ優先度※2
IPv4 条件	コンフィグレーション	VLAN ID※1
	MAC ヘッダ	ユーザ優先度※2
	IPv4 ヘッダ※3	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
	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※4
	IPv4-UDP ヘッダ	送信元ポート番号
		宛先ポート番号

種別		設定項目
	IPv4-ICMP ヘッダ	ICMP タイプ値
		ICMP コード値
IPv6 条件	コンフィグレーション	VLAN ID※1
	MAC ヘッダ	ユーザ優先度※2
	IPv6 ヘッダ※5	上位プロトコル
		送信元 IP アドレス
		宛先 IP アドレス
		トラフィッククラス
		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※4
	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 タイプ値
		ICMP コード値

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。受信フレームの属する VLAN ID を検出します。

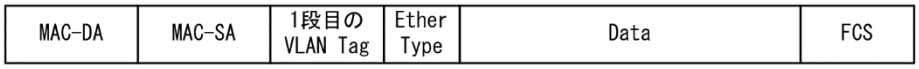
注※2

次に示すフレームについてはユーザ優先度を検出できません。常に，ユーザ優先度 3 として検出します。

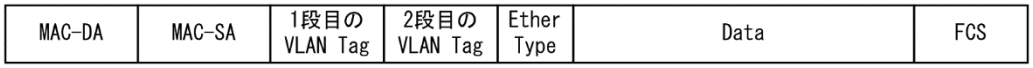
- VLAN Tag なしのフレーム

VLAN Tag が複数あるフレームに対してユーザ優先度を検出する場合，MAC アドレス側から 1 段目の VLAN Tag にあるユーザ優先度が対象となります。次の図に VLAN Tag が複数あるフレームの例を示します。

(i) VLAN Tag 1段のフォーマット



(ii) VLAN Tag 2段のフォーマット

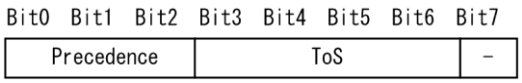


注※3

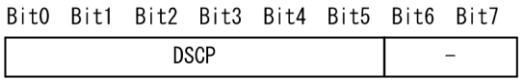
ToS フィールドの指定についての補足

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。



DSCP　　：ToS フィールドの上位 6 ビットの値です。



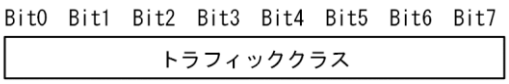
注※4

ack/fin/psh/rst/syn/urg フラグが 1 のパケットを検出します。

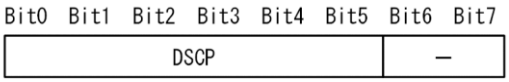
注※5

トラフィッククラスフィールドの指定についての補足

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。



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。



(2)　送信側インタフェースのフロー検出条件

送信側インタフェースで指定できるフロー検出条件を次の表に示します。ただし，該当 VLAN に属するすべてのイーサネットインタフェースに対してどれか一つでも Tag 変換を設定している VLAN インタフェースでは，フィルタエントリを適用できません。

表 1-4　送信側インタフェースで指定できるフロー検出条件

種別		設定項目
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
		ユーザ優先度※2
IPv4 条件	コンフィグレーション	VLAN ID※1
	MAC ヘッダ	ユーザ優先度※2
	IPv4 ヘッダ※3	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
	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※4
	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
IPv6 条件	コンフィグレーション	VLAN ID※1

種別		設定項目
	MAC ヘッダ	ユーザ優先度※2
	IPv6 ヘッダ※5	上位プロトコル
		送信元 IP アドレス
		宛先 IP アドレス
		トラフィッククラス
		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※4
	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 タイプ値
		ICMP コード値

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。送信フレームの属する VLAN ID を検出します。

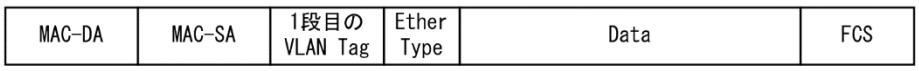
次に示す場合，VLAN ID を指定できません。

- Tag 変換を設定したイーサネットインタフェースに指定する場合
- VLAN トンネリングを設定したイーサネットインタフェースに指定する場合

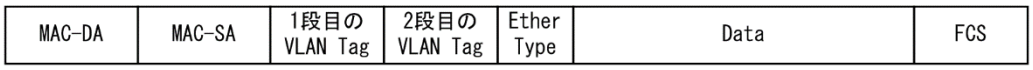
注※2

送信フレームの VLAN Tag にあるユーザ優先度を検出します。VLAN Tag が複数あるフレームに対してユーザ優先度を検出する場合，MAC アドレス側から 1 段目の VLAN Tag にあるユーザ優先度が対象となります。次の図に VLAN Tag が複数あるフレームの例を示します。

(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，受信側でマーカー（ユーザ優先度の書き換え）を使用した場合は，マーカー後のユーザ優先度を検出します。受信側でマーカーを使用していない場合で，かつ受信フレームが VLAN Tag なしのときは，ユーザ優先度 3 として検出します。受信側でマーカーを使用していない場合で，かつ受信フレームが VLAN Tag ありのときは，受信時のユーザ優先度を検出します。

ただし，次に示すフレームは優先度 3 として検出します。

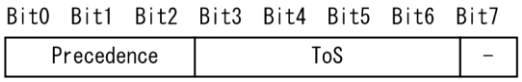
- VLAN トンネリングを設定したポートで受信したフレーム

注※3

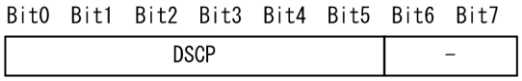
ToS フィールドの指定についての補足

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。



DSCP　：ToS フィールドの上位 6 ビットの値です。



受信側インタフェースでマーカー機能の DSCP 書き換えを使用した場合，送信側インタフェースでの ToS，DSCP および Precedence の検出は，DSCP 書き換え後のフレームに対して実施します。

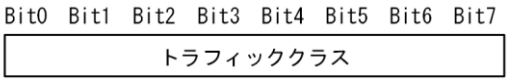
注※4

ack/fin/psh/rst/syn/urg フラグが 1 のパケットを検出します。

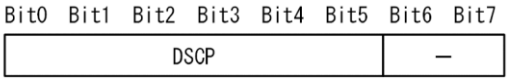
注※5

トラフィッククラスフィールドの指定についての補足

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。



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。



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に示します。

表 1-5　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	アクセスリスト	対応するフロー検出モード	検出可能なフレーム種別		
			非 IP	IPv4	IPv6
MAC 条件	mac access-list	layer2-1 layer2-1-mirror	○	○	○
IPv4 条件	access-list ip access-list	layer2-2 layer2-2-mirror	－	○	－
IPv6 条件	ipv6 access-list	layer2-3	－	－	○

（凡例）○：検出できる　　－：検出できない

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)　複数のフロー検出条件を同時に設定した場合の動作

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，次の表に示す順序でフレームを検出します。複数のフィルタエントリには一致しません。

表 1-6　フロー検出順序

フロー検出順序	インタフェース
1	イーサネット
2	VLAN

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，すべてのフレームを中継します。

1.1.7 フィルタ使用時の注意事項

(1)　VLAN Tag 付きフレームに対する受信側フィルタ

2 段の VLAN Tag があるフレームに対して，MAC 条件のイーサネットタイプ，IPv4 条件，または IPv6 条件をフロー検出条件としたフィルタを受信側で実施するためには，次の条件のどちらかを満たす必要があります。

- 本装置で VLAN トンネリング機能が動作していない
- 本装置で VLAN トンネリング機能が動作していて，フレームを受信したポートがトランクポートである

(2)　VLAN Tag 付きフレームに対する送信側フィルタ

受信ポートがトンネリングポートで受信ポート以外に設定した 0x8100 以外の TPID を含みかつ 2 段の VLAN Tag があるフレーム，または受信ポートがトンネリングポート以外でどれかのポートに設定した 0x8100 以外の TPID を含みかつ 2 段の VLAN Tag があるフレームを，以下の条件で送信する際にフィルタを送信側で実施する場合は，MAC アクセスリストでだけ検出できます。

- 受信ポートと送信ポートが異なるメンバスイッチ
- AX2630S-48T4XW または AX2630S-48P4XW で，受信ポートと送信ポートがポート 1～24，49～50 のどれかと，ポート 25～48，51～54 のどれか

(3)　IPv4 フラグメントパケットに対するフィルタ

IPv4 フラグメントパケットに対して TCP/UDP ヘッダ・ICMP ヘッダをフロー検出条件としたフィルタを行った場合，2 番目以降のフラグメントパケットは TCP/UDP ヘッダ・ICMP ヘッダがパケット内にないため，検出できません。フラグメントパケットを含めたフィルタを実施する場合は，フロー検出条件に MAC ヘッダ，IP ヘッダを指定してください。

(4)　拡張ヘッダのある IPv6 パケットに対するフィルタ

受信側では，IPv6 拡張ヘッダが 1 段の Hop-by-Hop Options 以外の IPv6 パケットに対して，TCP/UDP ヘッダ・ICMP ヘッダをフロー検出条件としたフィルタはできません。該当パケットに対してフィルタを実施する場合は，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。

送信側では，IPv6 拡張ヘッダのある IPv6 パケットに対して，TCP/UDP ヘッダ・ICMP ヘッダをフロー検出条件としたフィルタはできません。該当パケットに対してフィルタを実施する場合は，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。

(5)　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，設定したフィルタエントリが適用されるま

での間，暗黙の廃棄を含むほかのフィルタエントリで検出される場合があります。その場合，検出した暗黙の廃棄を含むフィルタ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で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で適用し，エントリを追加する場合
- 装置起動時に，フィルタエントリを適用する場合

(6)　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。

(7)　ほかの機能との同時動作

(a)　sFlow 統計およびポートミラーリング併用時のフィルタ統計

送信側フィルタを VLAN インタフェースに適用して，かつ該当 VLAN に属するイーサネットインタフェースで sFlow 統計の送信サンプリングをしている場合，およびポートミラーリングで送信ミラーのモニターポートに指定している場合，該当フィルタの統計情報が多く加算されることがあります。

1.2 コマンドガイド

1.2.1 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 1-7　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。
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。
flow detection mode※	フィルタ・QoS 制御のフロー検出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」　「27　フロー検出モード/フロー動作」を参照してください。

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 1-8　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）で設定したアクセスリスト（mac access-list，access-list，ip access-list，ipv6 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）で設定したアクセスリスト（mac access-list，access-list，ip access-list，ipv6 access-list）の統計情報をクリアします。

1.2.2 フロー検出モードの設定

フィルタのフロー検出モードを指定する例を次に示します。

［設定のポイント］

フロー検出モードは，ハードウェア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)# flow detection mode layer2-2
   フロー検出モード layer2-2 を有効にします。

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. (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 1/0/1
   ポート 1/0/1 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
   受信側に 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-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。
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
受信側に 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
受信側に IPv4 フィルタを有効にします。

(3) TCP/UDP ポート番号をフロー検出条件とする設定

UDP ポート番号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 UDP ヘッダの宛先ポート番号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 PORT_RANGE_DENY
ip access-list（PORT_RANGE_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 udp any any eq 10
UDP ヘッダの宛先ポート番号が 10 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 PORT_RANGE_DENY in
受信側に IPv4 フィルタを有効にします。

(4)　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，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 IPv6 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 IPv6 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 1/0/1
   ポート 1/0/1 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
   受信側に IPv6 フィルタを有効にします。

1.2.5 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 1/0/1-4
   ポート 1/0/1-4 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
   受信側に IPv4 フィルタを有効にします。

2 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。

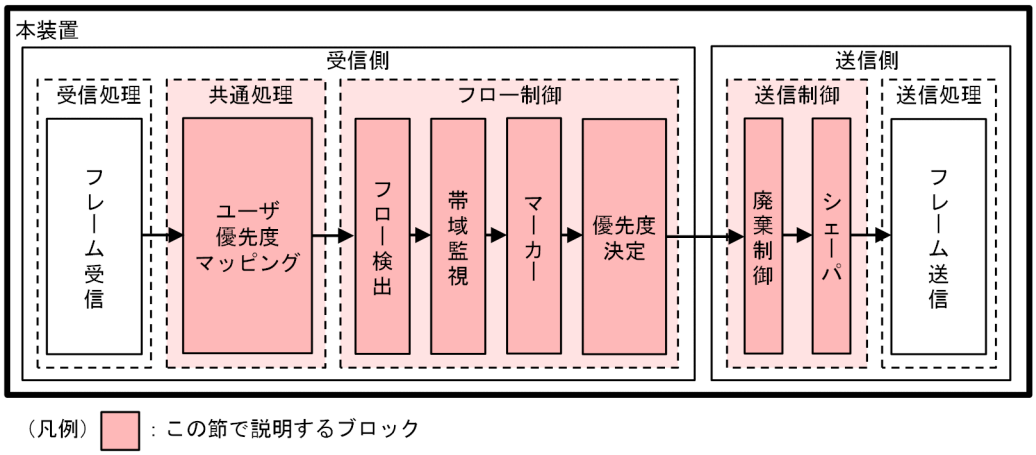
2.1 QoS 制御構造

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 2-1　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 2-1　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	フレームを受信します。
共通処理部	ユーザ優先度マッピング	受信フレームの VLAN Tag のユーザ優先度に従い，優先度を決定します。
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，ICMP ヘッダ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，受信フレームの優先度をユーザ優先度マッピング，またはフロー制御によって決定します。ユーザ優先度マッピングは，受信フレームの VLAN Tag 内にあるユーザ優先度に基づいて優先度を決定します。ユーザ優先度ではなく，MAC アドレスや IP アドレスなどの特定の条件に一致するフレー

ムに対して優先度を決定したい場合は，フロー制御を使用します。

フロー制御による優先度の決定は，ユーザ優先度マッピングよりも優先されます。また，フロー制御は，優先度決定のほかに帯域監視やマーカーも実施できます。フロー検出で検出したフローに対して，帯域監視，マーカー，優先度決定の各機能は同時に動作できます。

送信制御は，ユーザ優先度マッピングや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。

2.2 共通処理解説

2.2.1 ユーザ優先度マッピング

ユーザ優先度マッピングは，受信フレームの VLAN Tag 内にあるユーザ優先度に基づいて優先度を決定する機能です。本装置では，常にユーザ優先度マッピングが動作し，すべてのフレームに対して優先度を決定します。

優先度の値には，装置内の優先度を表す CoS 値を用います。受信フレームのユーザ優先度の値から CoS 値にマッピングし，CoS 値によって送信キューを決定します。CoS 値と送信キューの対応については，「3.7.3 CoS マッピング機能」を参照してください。

ユーザ優先度は，Tag Control フィールド（VLAN Tag ヘッダ情報）の上位 3 ビットを示します。なお，VLAN Tag がないフレームは，常に CoS 値 3 を使用します。

フロー制御による優先度決定が動作する場合，ユーザ優先度マッピングよりも優先して動作します。

表 2-2　ユーザ優先度と CoS 値のマッピング

フレームの種類		マッピングされる CoS 値
VLAN Tag の有無	ユーザ優先度値	
VLAN Tag なし	－	3
VLAN Tag あり※	0	0
	1	1
	2	2
	3	3
	4	4
	5	5
	6	6
	7	7

（凡例）－：該当なし

注※

次の場合，受信時のユーザ優先度値に関係なく，常に CoS 値 3 でマッピングされます。

- VLAN トンネリングを設定したポートで受信したフレーム

2.3 QoS 制御共通のコマンドガイド

2.3.1 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 2-3　コンフィグレーションコマンド一覧

コマンド名	説明
ip qos-flow-group	イーサネットインタフェースまたは VLAN 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 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。
mac qos-flow-group	イーサネットインタフェースまたは VLAN 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。
qos	QoS フローリストでのフロー検出条件および動作指定を設定します。
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，レガシー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モードを設定します。
remark	QoS の補足説明を記述します。
traffic-shape rate	イーサネットインタフェースにポート帯域制御を設定します。
flow detection mode※	フィルタ・QoS 制御のフロー検出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」　「27　フロー検出モード/フロー動作」を参照してください。

QoS 制御共通の運用コマンド一覧を次の表に示します。

表 2-4　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）で設定した QoS フローリスト（mac qos-flow-list，ip qos-flow-list，ipv6 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）で設定した QoS フローリスト（mac qos-flow-list，ip qos-flow-list，ipv6 qos-flow-list）の統計情報をクリアします。
show qos queueing	イーサネットインタフェースの送信キューの統計情報を表示します。

コマンド名	説明
clear qos queueing	イーサネットインタフェースの送信キューの統計情報をクリアします。

3 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。

3.1 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，ICMP 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，「3.1.3　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および VLAN インタフェースに対して QoS フローリストを設定できます。QoS フローリストを設定したイーサネットインタフェース，VLAN インタフェースともに，レイヤ 2 中継のイーサネット V2 形式および IEEE802.3 の SNAP/RFC1042 形式フレームをフロー検出できます。

受信側インタフェースでフロー検出を指定した場合，イーサネットインタフェース，VLAN インタフェースともに，イーサネットインタフェースで受信した段階でフロー検出します。なお，本装置宛ての受信フレームもフロー検出対象です。

3.1.1 フロー検出モード

本装置では，ネットワーク構成や運用形態を想定してフロー検出モードを用意しています。フロー検出モードは，フィルタ・QoS エントリの配分パターンを決めるモードです。エントリの配分については「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，使い方に合わせてモードを選択してください。

フロー検出モードは flow detection mode コマンドで指定します。なお，選択したフロー検出モードはフィルタ・QoS，かつ受信側と送信側で共通です。フロー検出モードを変更する場合，インタフェースに設定された次のコマンドをすべて削除する必要があります。

- mac access-group
- ip access-group
- ipv6 traffic-filter
- mac qos-flow-group
- ip qos-flow-group
- ipv6 qos-flow-group

なお，フロー検出モードを指定しない場合，layer2-1 がデフォルトのモードとして設定されます。

フロー検出モードとフロー動作の関係を次の表に示します。

表 3-1　フロー検出モードとフロー動作の関係

フロー検出モード名称	運用目的	フロー動作
layer2-1	MAC ヘッダ（VLAN Tag 含む）でフローを制御したい	すべてのフレームを対象に，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。
layer2-2	IPv4 ヘッダ，L4 ヘッダでフローを制御したい	IPv4 パケットについて，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。
layer2-3	IPv4 ヘッダ，IPv6 ヘッダ，L4 ヘッダでフローを制御したい	IPv4 パケットまたは IPv6 パケットについて，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。

3.1.2 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。受信側イ

ンタフェースでのフロー検出条件を次に示します。

(1)　受信側インタフェースのフロー検出条件

受信側インタフェースで指定できるフロー検出条件を次の表に示します。

表 3-2　受信側インタフェースで指定できるフロー検出条件

種別		設定項目
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
		ユーザ優先度※2
IPv4 条件	コンフィグレーション	VLAN ID※1
	MAC ヘッダ	ユーザ優先度※2
	IPv4 ヘッダ※3	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
	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※4
	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
IPv6 条件	コンフィグレーション	VLAN ID※1
	MAC ヘッダ	ユーザ優先度※2
	IPv6 ヘッダ※5	上位プロトコル
		送信元 IP アドレス
		宛先 IP アドレス
		トラフィッククラス
		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※4
	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 タイプ値
		ICMP コード値

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。受信フレームの属する VLAN ID を検出します。

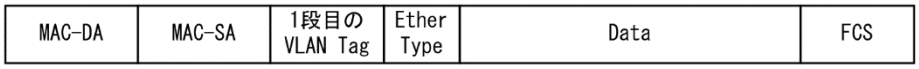
注※2

次に示すフレームについてはユーザ優先度を検出できません。常に，ユーザ優先度 3 として検出します。

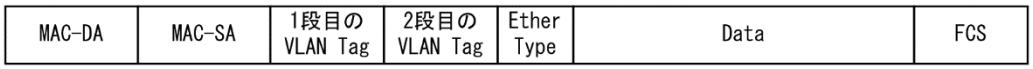
- VLAN Tag なしのフレーム

VLAN Tag が複数あるフレームに対してユーザ優先度を検出する場合，MAC アドレス側から 1 段目の VLAN Tag にあるユーザ優先度が対象となります。次の図に VLAN Tag が複数あるフレームの例を示します。

(i) VLAN Tag 1段のフォーマット



(ii) VLAN Tag 2段のフォーマット

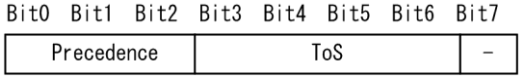


注※3

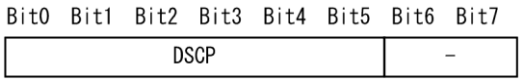
ToS フィールドの指定についての補足

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。



DSCP　　：ToS フィールドの上位 6 ビットの値です。



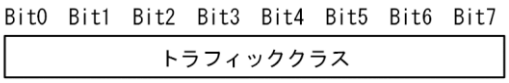
注※4

ack/fin/psh/rst/syn/urg フラグが 1 のパケットを検出します。

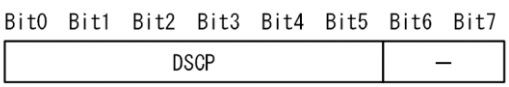
注※5

トラフィッククラスフィールドの指定についての補足

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。



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。



3.1.3 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 3-3　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

フロー検出条件	対応する QoS フローリスト	対応するフロー検出モード	検出可能なフレーム種別		
			非 IP	IPv4	IPv6
MAC 条件	mac qos-flow-list	layer2-1	○	○	○
IPv4 条件	ip qos-flow-list	layer2-2, layer2-3	－	○	－
IPv6 条件	ipv6 qos-flow-list	layer2-3	－	－	○

（凡例）○：検出できる　　－：検出できない

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)　複数のフロー検出条件を同時に設定した場合の動作

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受信フレームに対して QoS フロー検出を実施した場合，次の表に示す順序でフレームを検出します。複数の QoS エントリには一致しません。

表 3-4　フロー検出順序

フロー検出順序	インタフェース
1	イーサネット
2	VLAN

3.1.4 フロー検出使用時の注意事項

(1)　VLAN Tag 付きフレームに対する QoS フロー検出

2 段の VLAN Tag があるフレームに対して，MAC 条件のイーサネットタイプ，IPv4 条件，または IPv6 条件をフロー検出条件とした QoS フロー検出を受信側で実施するためには，次の条件のどちらかを満たす必要があります。

- 本装置で VLAN トンネリング機能が動作していない
- 本装置で VLAN トンネリング機能が動作していて，フレームを受信したポートがトランクポートである

(2)　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 TCP/UDP ヘッダ・ICMP ヘッダをフロー検出条件とした QoS フロー検出を行った場合，2 番目以降のフラグメントパケットは TCP/UDP ヘッダ・ICMP ヘッダがフレーム内にないため検出できません。フラグメントパケットを含めた QoS フロー検出を実施する場合は，フロー検出条件に MAC ヘッダ，IP ヘッダを指定してください。

(3)　拡張ヘッダのある IPv6 パケットに対する QoS フロー検出

IPv6 拡張ヘッダが 1 段の Hop-by-Hop Options 以外の IPv6 パケットに対して，TCP/UDP ヘッダ・ICMP ヘッダをフロー検出条件とした QoS フロー検出はできません。

該当パケットに対して QoS フロー検出を実施する場合は，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。

(4) QoS 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 QoS エントリを適用する※と，設定した QoS エントリが適用されるまでの間，ほかの QoS エントリで検出される場合があります。その場合，検出した QoS 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 QoS フローリストを QoS フローグループコマンドでインタフェースに適用する場合
- QoS フローリストを QoS フローグループコマンドで適用し，エントリを追加する場合
- 装置起動時に，QoS エントリを適用する場合

(5) 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。

(6) ほかの機能との同時動作

以下の場合フレームは廃棄しますが，受信側のインタフェースに対して帯域監視を未使用の QoS エントリを設定し一致した場合，一致した QoS エントリの統計情報が採られます。

- VLAN のポートのデータ転送状態が Blocking（データ転送停止中）の状態で，該当ポートからフレームを受信した場合
- ポート間中継遮断機能で指定したポートからフレームを受信した場合
- ネイティブ VLAN をトランクポートで送受信する VLAN に設定しないで，VLAN Tag なしフレームを受信した場合
- トランクポートで送受信する VLAN に設定していない VLAN Tag 付きフレームを受信した場合
- アクセスポート，プロトコルポートおよび MAC ポートで VLAN Tag 付きフレームを受信した場合
- 廃棄動作を指定したフィルタエントリ（暗黙の廃棄のエントリを含む）に一致するフレームを受信した場合
- MAC アドレス学習機能によってフレームが廃棄された場合
- IGMP snooping および MLD snooping によってフレームが廃棄された場合
- ストームコントロールによってフレームが廃棄された場合
- IP レイヤ処理によってパケットが廃棄された場合

3.2 フロー検出のコマンドガイド

3.2.1 フロー検出モードの設定

QoS 制御のフロー検出モードを指定する例を示します。

［設定のポイント］

フロー検出モードは，ハードウェア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)# flow detection mode layer2-2
   フロー検出モード layer2-2 を有効にします。

3.2.2 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 cos 6
   192.168.100.10 の IP アドレスを宛先とし，CoS 値＝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グレーションモードに戻ります。
4. (config)# interface range gigabitethernet 1/0/1-4
   ポート 1/0/1-4 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 in
   受信側に IPv4 QoS フローリストを有効にします。

3.2.3 TCP/UDP ポート番号で QoS 制御する設定

UDP ポート番号をフロー検出条件とし，QoS 制御を設定する例を示します。

［設定のポイント］

フレーム受信時に UDP ヘッダの宛先ポート番号によってフロー検出を行い，QoS 制御を実施します。

［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 udp any any eq 10 action cos 6
   UDP ヘッダの宛先ポート番号 10 をフロー検出条件とし，CoS 値＝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グレーションモードに戻ります。
4. (config)# interface gigabitethernet 1/0/1

ポート 1/0/1 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
受信側に IPv4 QoS フローリストを有効にします。

3.3 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。

3.3.1 帯域監視

フロー検出で検出したフレームのフレーム長（MAC アドレスから 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。

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，Token Bucket アルゴリズムを用いています。

バーストサイズは，バーストトラフィックを遵守フレームとして転送できる最大フレーム容量です。バーストサイズの特徴を次の表に示します。

表 3-5　バーストサイズの特徴

バーストサイズ	特徴
小さくする	バーストトラフィックが比較的廃棄されやすい。通信をしていない状態でトラフィックを送信した際，送信帯域の揺らぎが比較的小さい。
大きくする	バーストトラフィックが比較的廃棄されにくい。通信をしていない状態でトラフィックを送信した際，送信帯域の揺らぎが比較的大きい。

本機能は，最低帯域監視と最大帯域制御から成り，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 3-6　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	○	－

（凡例）○：使用可能なペナルティ　　－：使用不可能なペナルティ

3.3.2 帯域監視使用時に採取可能な統計情報

帯域監視ごとに採取可能な統計情報が異なります。帯域監視使用時に採取可能な統計情報を次の表に示します。

表 3-7　帯域監視使用時に採取可能な統計情報

帯域監視種別	採取可能な統計情報			
	最大帯域違反	最大帯域遵守	最低帯域違反	最低帯域遵守
最低帯域監視	－	－	○	○
最大帯域制御	○	○	－	－
最低帯域監視と最大帯域制御の組み合わせ	○	○	－	－

（凡例）○：採取可能　　－：採取不可能

3.3.3 帯域監視使用時の注意事項

(1) VLAN インタフェースで帯域監視を使用

一部のモデルやスタック構成では，VLAN インタフェースで帯域監視する場合に，使用できるポートの組み合わせがあります。使用可能なポートの組み合わせを次の表に示します。対象外の組み合わせでは帯域監視を使用しないでください。

表 3-8　使用可能なポートの組み合わせ

モデル	構成	
	スタンドアロン	スタック
AX2630S-48T4XW AX2630S-48P4XW	ポート 1～24，49～50， または ポート 25～48，51～54 の組み合わせ	一つのメンバスイッチ内で， ポート 1～24，49～50， または ポート 25～48，51～54 の組み合わせ
上記以外	制限なし	一つのメンバスイッチ内

(2) 帯域監視と送信イーサネットインタフェース・送信キューの関係

次のような場合に，送信イーサネットインタフェースまたは送信キューで遵守フレームを廃棄するおそれがあります。

- 帯域監視で指定する監視帯域値を，該当フローの送信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より大きい値とした場合
- 帯域監視を使用しないフローと使用するフローを，同じ送信イーサネットインタフェースまたは送信キューに送信した場合

特に，複数のフローで複数の帯域監視を使用する場合は，各帯域監視の監視帯域値の合計に注意してください。

(3) 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には，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ことがあります。

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」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いで，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。

(4) ほかの機能との同時動作

ポート間中継遮断機能で指定したポートからフレームを受信した場合，フレームは廃棄しますが，帯域監視対象になります。

3.4 帯域監視のコマンドガイド

3.4.1 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 512
   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=512kbyte 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 1/0/1
   ポート 1/0/1 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
   受信側に IPv4 QoS フローリスト（QOS-LIST1）を有効にします。

3.4.2 最低帯域監視違反時のキューイング優先度の設定

特定のフローに対して最低帯域監視（違反フレームはキューイング優先度の変更）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 64 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=64kbyte，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 1/0/3
   ポート 1/0/3 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 in
   受信側に IPv4 QoS フローリスト（QOS-LIST2）を有効にします。

3.4.3 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 64 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=64kbyte，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 gigabitethernet 1/0/5
   ポート 1/0/5 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
   受信側に IPv4 QoS フローリスト（QOS-LIST3）を有効にします。

3.4.4 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 512 min-rate 1M min-rate-burst 64 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=512kbyte，最低監視帯域=1Mbit/s，最低監視帯域のバーストサイズ=64kbyte，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 gigabitethernet 1/0/7
   ポート 1/0/7 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
   受信側に IPv4 QoS フローリスト（QOS-LIST4）を有効にします。

3.5 マーカー解説

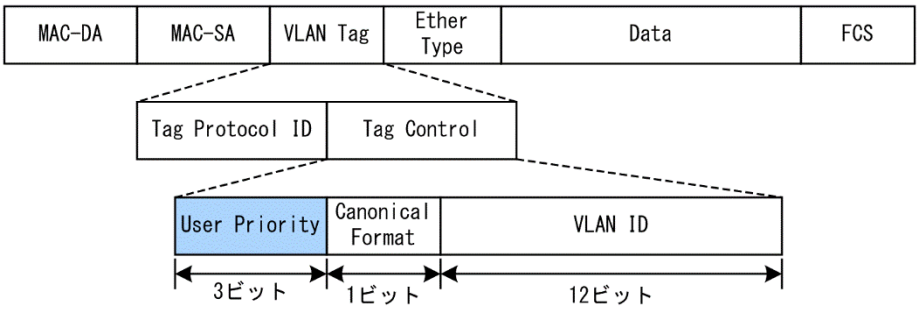
マーカーは，フロー検出で検出したフレームの VLAN Tag 内のユーザ優先度および IP ヘッダ内の DSCP を書き換える機能です。

本装置がソフトウェアで中継するフレームは，マーカーによるユーザ優先度や DSCP の書き換えができません。ソフトウェア中継になるフレームについては，「コンフィグレーションガイド Vol.1」　「表 24-8 レイヤ 2 フレーム中継がソフトウェア中継になる機能とフレーム種別」を参照してください。

3.5.1 ユーザ優先度書き換え

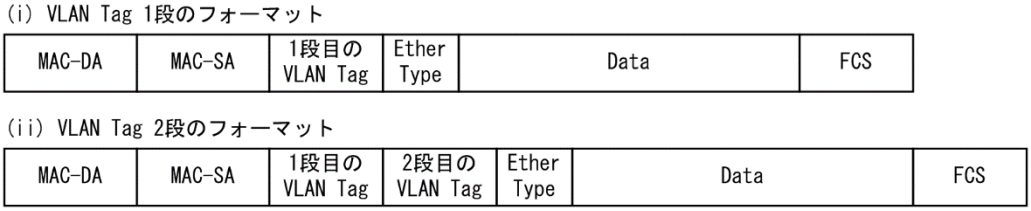
フロー検出で検出したフレームの VLAN Tag 内にあるユーザ優先度（User Priority）を書き換える機能です。ユーザ優先度は，次の図に示す Tag Control フィールドの先頭 3 ビットを指します。

図 3-1　VLAN Tag のヘッダフォーマット



VLAN Tag が複数あるフレームに対してユーザ優先度書き換えを行う場合，MAC アドレス側から 1 段目の VLAN Tag にあるユーザ優先度を書き換えます。次の図に VLAN Tag が複数あるフレームフォーマットを示します。

図 3-2　VLAN Tag が複数あるフレームフォーマットの概略図



VLAN Tag なしで受信して，VLAN Tag ありで送信する中継フレームにユーザ優先度書き換えを指定した場合，送信時の VLAN Tag のユーザ優先度は，書き換え後の優先度になります。

ユーザ優先度書き換えを実施しない場合は，次の表に示すユーザ優先度となります。

表 3-9　フレーム送信時のユーザ優先度

フレーム送信時のユーザ優先度	対象となるフレーム
7	・本装置が自発的に送信するフレーム ・DHCP snooping 有効時の DHCP パケット ・DHCP snooping のダイナミック ARP 検査有効時の ARP パケット ・GSRP Flush request フレーム
3	・VLAN Tag なしで受信し，VLAN Tag ありで送信するフレーム ・VLAN トンネリング機能で，アクセス回線からバックボーン回線に中継するフ

フレーム送信時のユーザ優先度	対象となるフレーム
	レーム
受信フレームのユーザ優先度	・VLAN トンネリング機能で，アクセス回線からアクセス回線に中継する VLAN Tag ありフレーム ・Tag 変換を設定してない，かつ VLAN トンネリングを設定していないポートで VLAN Tag ありフレームを受信し，VLAN Tag ありで送信するフレーム ・IGMP snooping 有効時の IGMP パケット，PIM プロトコルの Hello メッセージ，224.0.0.0/24 を宛先とする IPv4 パケット ・MLD snooping 有効時の MLD パケット，ff02::/16 を宛先とする IPv6 パケット ・レイヤ 2 認証の ARP パケットのリレー機能有効時の ARP パケット ・CFM 有効時のリンクトレースメッセージ

3.5.2 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 フィールドおよびトラフィッククラスフィールドのフォーマットを次の図に示します。

図 3-3　TOS フィールドのフォーマット

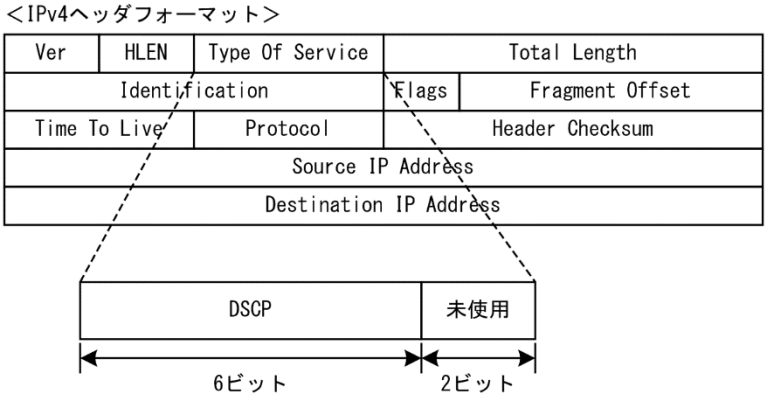
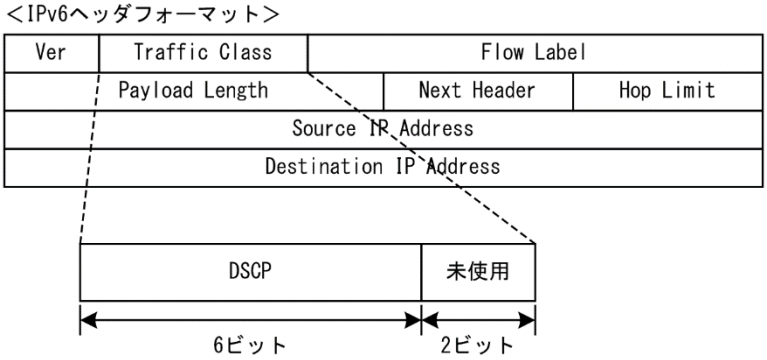


図 3-4　トラフィッククラスフィールドのフォーマット



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。

また，帯域監視からの指示によって，最低監視帯域を超えたフローの DSCP を書き換えることができます。例えば，最低監視帯域を超えたフローに対して，DSCP 値を 0 に設定できます。

最低帯域監視と同時に設定した場合の違反フレームの動作については，違反時のペナルティ指定動作が優先されます。

3.6 マーカーのコマンドガイド

3.6.1 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 gigabitethernet 1/0/1
   ポート 1/0/1 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
   受信側の IPv4 QoS フローリスト（QOS-LIST1）を有効にします。

3.6.2 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-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 192.168.100.10 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 gigabitethernet 1/0/3
   ポート 1/0/3 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-LIST3 in
   受信側の IPv4 QoS フローリスト（QOS-LIST3）を有効にします。

3.7 優先度決定の解説

優先度決定は，フロー検出で検出したフレームの優先度を CoS 値で指定して，送信キューを決定する機能です。本機能の対象となるフレームは装置構成と優先度決定動作変更の設定有無によって異なります。詳細は，「3.7.1　優先度決定の対象フレーム」を参照してください。

3.7.1 優先度決定の対象フレーム

本装置が中継するフレームだけが優先度決定の対象です。優先度決定の対象フレームを次の表に示します。

表 3-10　優先度決定の対象フレーム

装置構成	フレーム種別	
	本装置宛てのフレーム	本装置が中継するフレーム
全モデル共通	×	○※

（凡例）　○：優先度決定の対象となる　×：優先度決定の対象とならない

注※

本装置がソフトウェアで中継するフレームを除きます。ソフトウェア中継になるフレームについては，「コンフィグレーションガイド Vol.1」　「表 24-8　レイヤ 2 フレーム中継がソフトウェア中継になる機能とフレーム種別」を参照してください。

3.7.2 CoS 値・キューイング優先度

CoS 値は，フレームの装置内における優先度を表すインデックスを示します。キューイング優先度は，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します。

CoS 値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 3-11　CoS 値とキューイング優先度の指定範囲

項目	指定範囲
CoS 値	0～7
キューイング優先度	1～3

フロー制御の優先度決定が行われていないフレームは，デフォルトの CoS 値とキューイング優先度を使用します。デフォルトの CoS 値とキューイング優先度を次の表に示します。

表 3-12　デフォルトの CoS 値とキューイング優先度

フレーム種別	デフォルト値	
	CoS 値	キューイング優先度
中継するフレーム	ユーザ優先度マッピングに従います※	3

注※

次の QoS フロー条件に一致する中継フレームは，ユーザ優先度マッピングに従わないで，CoS 値は 3 固定となります。

- マーカーを指定して，CoS 値を指定していない
- 優先度決定でキューイング優先度を指定して，CoS 値を指定していない
- 帯域監視を指定して，CoS 値を指定していない

なお，次に示すフレームは，固定的に CoS 値とキューイング優先度を決定します。

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 3-13　優先度決定で変更できないフレーム一覧

フレーム種別	CoS 値	キューイング優先度
本装置が自発的に送信するフレーム 本装置がソフトウェアで中継するフレーム	7	3
ミラーリングフレーム	0	3

3.7.3 CoS マッピング機能

CoS マッピング機能は，ユーザ優先度マッピングで決定した CoS 値，またはフロー制御の優先度決定で指定した CoS 値に基づいて，送信キューを決定する機能です。

(1)　CoS 値とポートの送信キューのマッピング

ポート当たりの送信キューとして 8 キューあります。CoS 値とポートの送信キューのマッピングを次に示します。

表 3-14　CoS 値とポートの送信キューのマッピング

CoS 値	送信時のキュー番号
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

3.7.4 優先度決定使用時の注意事項

(1)　フレームの優先度決定

「フレームの優先度を上げる」動作を指定すると，本装置が自発的に送信するフレームを送信できなくなることによって，通信が切断される場合があります。このような現象が発生した場合は，「フレームの優先度を下げる」動作を実施してください。

3.8 優先度決定のコマンドガイド

3.8.1 CoS 値の設定

特定のフローに対して CoS 値を設定します。

［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，CoS 値を設定します。

［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 cos 6
   192.168.100.10 の IP アドレスを宛先とし，CoS 値＝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 gigabitethernet 1/0/1
   ポート 1/0/1 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
   IPv4 QoS フローリスト（QOS-LIST1）を有効にします。

4 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。

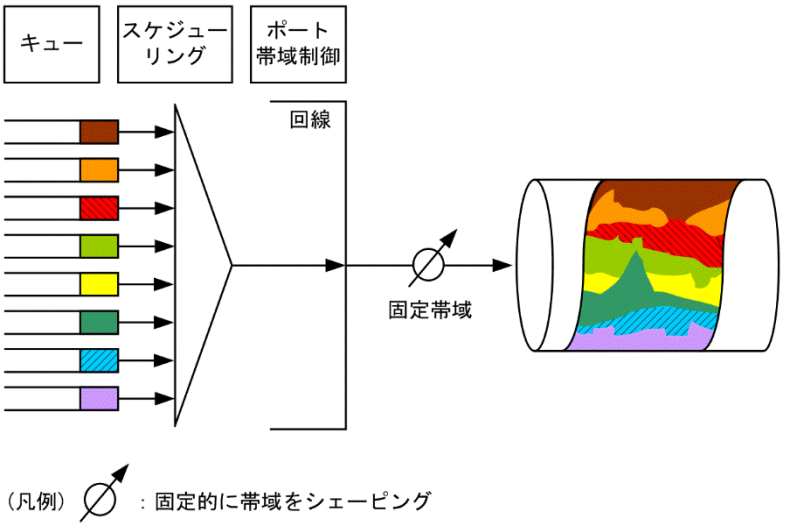
4.1 シェーパ解説

4.1.1 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順序や出力帯域を制御する機能です。

レガシーシェーパは，次の図に示すように，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と，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ています。レガシーシェーパの概念を次の図に示します。

図 4-1　レガシーシェーパの概念



4.1.2 送信キュー長指定

送信キュー長とは，一つのキューにキューイングできるバッファ数のことです。一つのバッファには 256 バイトまで格納でき，256 バイトを超えたフレームの場合は，複数のバッファを使用して格納します。また，一つのバッファに複数のフレームを格納できません。

本装置では，ネットワーク構成や運用形態に合わせて送信キュー長を変更できます。送信キュー長の変更はコンフィグレーションコマンド system queue-length-mode で設定します。送信キュー長を拡大することによって，バーストトラフィックによるキューあふれを低減させることができます。なお，設定した送信キュー長は本装置のすべてのイーサネットインタフェースのすべてのキューに対して有効になります。ただし，装置のパケットバッファ量は一定のため，送信キュー長を拡大し複数のキューでキューイングをすると，パケットバッファの枯渇が発生しやすくなります。パケットバッファの枯渇が定期的に発生する場合，ネットワーク設計の見直しが必要です。

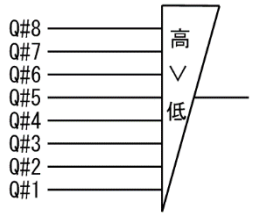
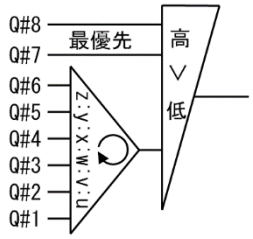
送信キュー長を設定しない場合，キュー長 192 で動作します。

4.1.3 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，次に示す二つのスケジューリング種別があります。デフォルト動作は PQ です。スケジューリングの動作説明を次の表に示します。

表 4-1　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		完全優先制御。ポート当たり 8 キュー。 複数のキューにフレームが存在する場合，優先度の高いキューから（Q#8，Q#7，…，Q#1）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
2PQ+6DRR		最優先キューと重み（バイト数）付きラウンドロビン。ポート当たり 8 キュー。 最優先のキュー8（Q#8）は，常に最優先でフレームを送信します。キュー7（Q#7）は，キュー8（Q#8）の次に優先的にフレームを送信します。キュー8，7 にフレームが存在しない場合，キュー6～1（Q#6～Q#1）は各キューに設定した比率（z：y：x：w：v：u）に応じたバイト数でフレームを送信します。	最優先キューに映像，音声，DRR キューにデータ系トラフィック

スケジューリングの仕様について次の表に示します。

表 4-2　スケジューリング仕様

項目		仕様
キュー数		8 キュー
2PQ+6DRR	キュー1～6 の重みの設定範囲	1～254

4.1.4 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後に，該当する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，回線帯域が 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。

ポート帯域制御は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。

設定帯域は回線速度以下になるように設定してください。設定できない場合，運用ログが表示されポート帯域制御の設定は無効となります。

Leaky Bucket アルゴリズムの特性によるバーストサイズの特徴を次の表に示します。

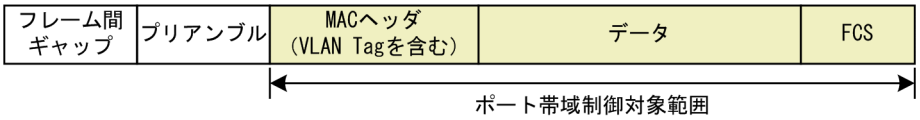
表 4-3　バーストサイズの特徴

バーストサイズ	特徴
小さくする	バーストトラフィックが比較的廃棄されやすい。通信をしていない状態でトラフィックを送信した際，送信帯域の揺らぎが比較的小さい。
大きくする	バーストトラフィックが比較的廃棄されにくい。通信をしていない状態でトラフィックを送信した際，送信帯域の揺らぎが比較的大きい。

ポート帯域制御の設定範囲とバーストサイズの設定範囲は，「コンフィグレーションコマンドレファレンス」で traffic-shape rate コマンドの説明を参照してください。

ポート帯域制御の対象となるフレームの範囲は MAC ヘッダから 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 4-2　ポート帯域制御の対象範囲



4.1.5 シェーパ使用時の注意事項

(1)　パケットバッファ枯渇時のスケジューリングの注意事項

出力回線の帯域を上回るトラフィックを受信したとき，本装置のパケットバッファの枯渇が発生する場合があります。そのため，受信したフレームがキューにキューイングされず廃棄されるため，指定したスケジューリングどおりにフレームが送信されない場合があります。

パケットバッファの枯渇については，show qos queueing コマンドの HOL1 カウンタがインクリメントされていることで確認できます。

パケットバッファの枯渇が定常的に発生する場合，ネットワーク設計の見直しが必要です。

4.2 シェーパのコマンドガイド

4.2.1 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 1/0/1
   ポート 1/0/1 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。

4.2.2 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）およびバーストサイズの設定（4kbyte）を行います。

［コマンドによる設定］

1. (config)# interface gigabitethernet 1/0/13
   ポート 1/0/13 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 4
   ポート帯域を 20Mbit/s，バーストサイズを 4kbyte に設定します。

4.3 廃棄制御解説

4.3.1 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。

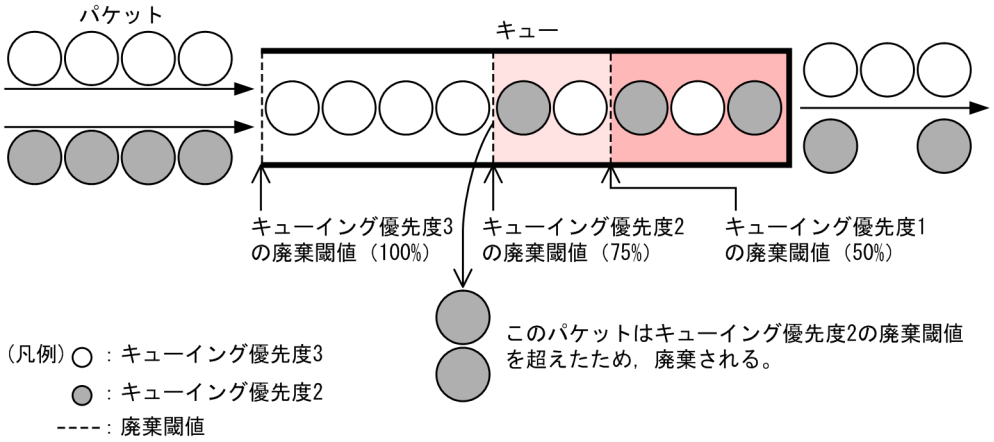
一つのキューにキューイングできるフレーム量を「キュー長」と呼びます。

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 4-3　テールドロップの概念



次に，テールドロップ機能における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，キュー長に対するキューの溜まり具合を百分率で表します。

表 4-4　テールドロップでの廃棄閾値

キューイング優先度	廃棄閾値［%］
1	50
2	75
3	100

4.4 廃棄制御のコマンドガイド

4.4.1 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 discard-class 2
   192.168.100.10 の IP アドレスを宛先とし，キューイング優先度＝2 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 gigabitethernet 1/0/1
   ポート 1/0/1 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-LIST2 in
   受信側に QoS フローリスト（QOS-LIST2）を有効にします。

5 レイヤ 2 認証

この章では，本装置のレイヤ 2 認証の概要について説明します。

5.1 概要

5.1.1 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 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。

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「5.2　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 5-1　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	固定 VLAN モード	認証成功後は，VLAN 内で通信できます。また，固定 VLAN モード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。
	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 内へ通信できます。また，ダイナミック VLAN モードでは，シングルモードと端末認証モードの認証サブモードがあります。
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。
MAC 認証	固定 VLAN モード	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	認証成功後は，MAC VLAN で切り替えた VLAN 内へ通信できます。

本装置では，複数のレイヤ 2 認証を組み合わせた 2 段階認証を行うマルチステップ認証ができます。マルチステップ認証では，1 段目の認証を端末認証，2 段目の認証をユーザ認証と呼びます。また，マルチステップ認証では，端末認証とユーザ認証の 2 段階で認証を許可する動作をマルチステップ認証，単一のレイヤ 2 認証だけで認証を許可する動作をシングル認証と呼びます。

マルチステップ認証で，端末認証とユーザ認証に使用できるレイヤ 2 認証の組み合わせを次の表に示します。なお，レイヤ 2 認証の組み合わせの際，認証モードは固定 VLAN モードまたはダイナミック VLAN モードのどちらかに合わせてください。

表 5-2　端末認証とユーザ認証に使用できるレイヤ 2 認証の組み合わせ

組み合わせパターン	端末認証	ユーザ認証
MAC 認証と IEEE802.1X の組み合わせ	MAC 認証	IEEE802.1X※
MAC 認証と Web 認証の組み合わせ	MAC 認証	Web 認証
IEEE802.1X と Web 認証の組み合わせ	IEEE802.1X※	Web 認証

注※

認証サブモードに端末認証モードを設定し，端末検出動作に auto を設定してください。

5.1.2 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。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 5-3　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	固定 VLAN モード	×	○
	ダイナミック VLAN モード	×	○
Web 認証	固定 VLAN モード	○	○
	ダイナミック VLAN 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

5.1.3 MAC VLAN の動的 VLAN 設定とレイヤ 2 認証

次の表に示すレイヤ 2 認証と認証モードで，MAC VLAN の認証対象ポートに認証済み端末を収容する認証後 VLAN（mac-based を設定しているすべての VLAN）を動的に設定します。認証ポートの動的に設定された認証後 VLAN は，レイヤ 2 認証で認証済み端末が存在する VLAN でだけ通信できます。すべての端末で認証が解除されると，該当する VLAN では通信できません。

表 5-4　動的に VLAN が設定できるレイヤ 2 認証と認証モード

レイヤ 2 認証	認証モード
IEEE802.1X	ダイナミック VLAN モード
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

なお，コンフィグレーションコマンド switchport mac vlan が設定されている認証対象の MAC ポートでは，コンフィグレーションコマンドで設定された認証後 VLAN 以外の VLAN 切り替えはできません。さらに，認証対象の MAC ポートに動的に VLAN が設定されている状態で，コンフィグレーションコマンド switchport mac vlan が設定された場合，該当ポートに動的に設定された VLAN を認証後 VLAN とした認証端末はすべて認証が解除されます。

5.1.4 レイヤ 2 認証の認証対象ポートについて

レイヤ 2 認証の認証対象ポート（以降，認証対象ポートまたは認証ポートと呼びます）には，物理ポート

またはチャネルグループを設定できます。認証対象ポートとしてチャネルグループを設定した場合，該当チャネルグループが単一の認証対象ポートとして扱われます。

5.2 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。

5.2.1 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 5-5　他機能との共存仕様

レイヤ 2 認証	機能名		共存仕様
IEEE802.1X	MAC アドレステーブル	MAC アドレス学習抑止	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。
		スタティック MAC アドレス	スタティック MAC アドレスを設定したポートでは使用できません。
	VLAN	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。
	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。
	スパニングツリー		スパニングツリーを設定したポートでは使用できません。
	Ring Protocol		Ring Protocol を設定したリングポートでは使用できません。
	IGMP snooping		使用できますが，認証ポートでは，IGMP snooping のパケットは認証の対象外となります。 ダイナミック VLAN モードでは，認証ポートにマルチキャストルータを接続しないでください。
	MLD snooping		装置で同時に使用できません。
	DHCP snooping		DHCP snooping の端末フィルタを設定したポートでは使用できません。 ダイナミック VLAN モードの認証ポートで使用する場合は，DHCP snooping を有効にする VLAN にネイティブ VLAN を含めてください。
	GSRP aware		GSRP aware が動作するポートでは使用できません。
	アップリンク・リダンダント		アップリンクポートで使用できません。
	IEEE802.3ah/UDLD		IEEE802.3ah/UDLD を設定したポートでは使用できません。
	CFM		CFM を設定したポートで同時に使用できません。
Web 認証	MAC アドレステーブル	MAC アドレス学習抑止	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。
		スタティック MAC アドレス	スタティック MAC アドレスを設定したポートでは使用できません。
	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。

レイヤ2認証	機能名		共存仕様
	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。
		EAPOL フォワーディング	共存できます。
	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使用できません。
	Ring Protocol		Ring Protocol を設定したリングポートでは使用できません。
	IGMP snooping		使用できますが，認証ポートでは，IGMP snooping のパケットは認証の対象外となります。 ダイナミック VLAN モードでは，認証ポートにマルチキャストルータを接続しないでください。
	MLD snooping		装置で同時に使用できません。
	DHCP snooping		DHCP snooping の端末フィルタを設定したポートでは使用できません。 ダイナミック VLAN モードの認証ポートで使用する場合は，DHCP snooping を有効にする VLAN にネイティブ VLAN を含めてください。
	GSRP aware		GSRP aware が動作するポートで使用できません。
	アップリンク・リダンダント		アップリンクポートで使用できません。
	IEEE802.3ah/UDLD		IEEE802.3ah/UDLD を設定したポートでは使用できません。
	CFM		CFM を設定したポートで同時に使用できません。
MAC 認証	MAC アドレステーブル	MAC アドレス学習抑止	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。
		スタティック MAC アドレス	スタティック MAC アドレスを設定したポートでは使用できません。
	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。
		EAPOL フォワーディング	共存できます。
	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使用できません。
	Ring Protocol		Ring Protocol を設定したリングポートでは使用できません。
	IGMP snooping		使用できますが，認証ポートでは，IGMP snooping のパケットは認証の対象外となります。 ダイナミック VLAN モードでは，認証ポートにマルチキャストルータを接続しないでください。

レイヤ 2 認証	機能名	共存仕様
	MLD snooping	装置で同時に使用できません。
	DHCP snooping	DHCP snooping の端末フィルタを設定したポートでは使用できません。 ダイナミック VLAN モードの認証ポートで使用する場合は，DHCP snooping を有効にする VLAN にネイティブ VLAN を含めてください。
	GSRP aware	GSRP aware が動作するポートで使用できません。
	アップリンク・リダンダント	アップリンクポートで使用できません。
	IEEE802.3ah/UDLD	IEEE802.3ah/UDLD を設定したポートでは使用できません。
	CFM	CFM を設定したポートで同時に使用できません。

5.2.2 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
- 固定 VLAN モードとダイナミック VLAN モードの共存

(1) 同一ポートの固定 VLAN モードの共存

表 5-6　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	MAC 認証
アクセスポート	○※	○	○
トランクポート	○※	○	○
上記以外	×	×	×

（凡例）

○：動作できる

×：動作できない

注※

Web 認証および MAC 認証を設定したポートに IEEE802.1X を設定した場合（マルチステップ認証の場合も同じ）は，認証サブモードに端末認証モードを設定し，端末検出動作に auto を設定してください。認証サブモードに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。また，次に示すコンフィグレーションコマンドは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 port-control force-authorized

dot1x port-control force-unauthorized

dot1x multiple-hosts

(2)　同一ポートのダイナミック VLAN モードの共存

表 5-7　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	Web 認証	MAC 認証
MAC ポート	○※	○	○
上記以外	×	×	×

（凡例）　○：動作できる　×：動作できない

注※

Web 認証および MAC 認証を設定したポートに IEEE802.1X を設定した場合（マルチステップ認証の場合も同じ）は，認証サブモードに端末認証モードを設定し，端末検出動作に auto を設定してください。認証サブモードに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。また，次に示すコンフィグレーションコマンドは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］

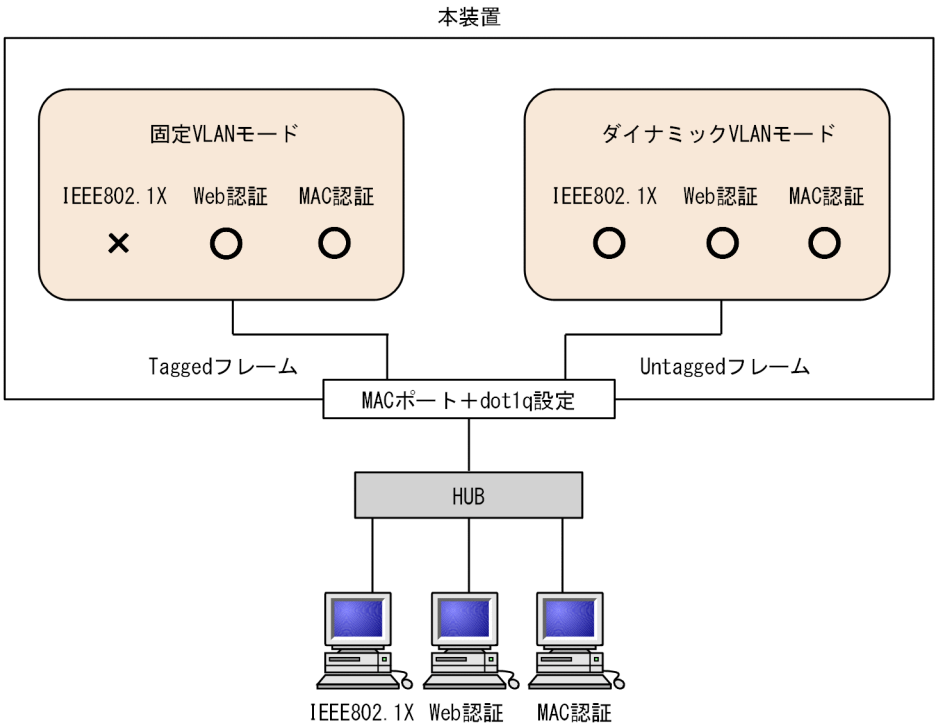
dot1x port-control force-authorized

dot1x port-control force-unauthorized

dot1x multiple-hosts

(3)　同一ポートのダイナミック VLAN モードと固定 VLAN モードの共存

図 5-1　同一ポートのダイナミック VLAN モードと固定 VLAN モードの共存



（凡例）○：動作できる　×：動作できない

表 5-8　同一ポートのダイナミック VLAN モードと固定 VLAN モードの共存

ポートの種類	受信フレームの種類	IEEE802.1X		Web 認証		MAC 認証	
		固定 VLAN モード	ダイナミック VLAN モード	固定 VLAN モード	ダイナミック VLAN モード	固定 VLAN モード	ダイナミック VLAN モード
MAC ポート＋ dot1q 設定	Tagged フレーム	×	×	○	×	○	×
	Untagged フレーム	○※	○	○※	○	○※	○

（凡例）　○：動作できる　×：動作できない

注※

RADIUS 認証方式で，RADIUS サーバから認証後 VLAN が送られてこなかった場合，ネイティブ VLAN に収容して固定 VLAN と同様に扱います。ただし，ポート間の移動については，ダイナミック VLAN モードの動作に従います。

5.2.3 レイヤ 2 認証共存時の認証優先

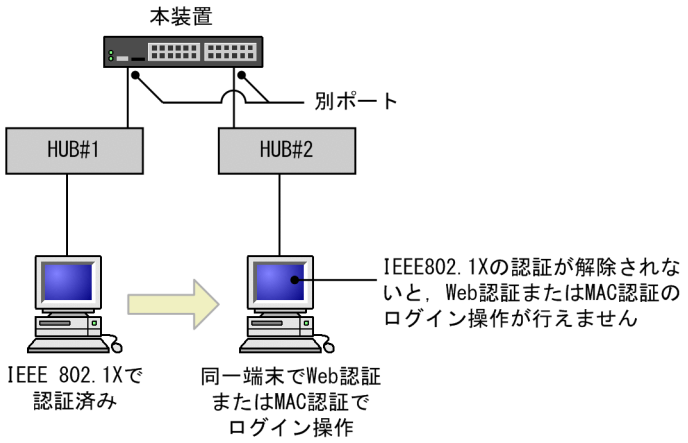
(1) IEEE802.1X と Web 認証または MAC 認証との共存時の認証優先

マルチステップ認証を行わない場合，IEEE802.1X の固定 VLAN モードは，Web 認証および MAC 認証より優先します。なお，IEEE802.1X のダイナミック VLAN モードでは，Web 認証および MAC 認証と等しい優先度を持ち，先に認証成功したレイヤ 2 認証の認証結果が維持されます。IEEE802.1X の固定 VLAN モードの認証優先の動作を次に説明します。

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 の固定 VLAN モード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）。

なお，IEEE802.1X の認証済みの端末が，MAC 認証や Web 認証のポートへ移動したときに，IEEE802.1X の認証は自動的に解除されません。例えば，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（端末認証モード）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 5-2　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



(2) Web 認証と MAC 認証との共存時の認証優先

マルチステップ認証を行わない場合，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)。

5.3 レイヤ 2 認証共通の機能

レイヤ 2 認証共通の機能について説明します。

- 認証前端末の通信許可
- 認証数制限
- 強制認証
- 認証済み端末のポート間移動および認証対象外ポートへ移動時の認証解除
- RADIUS サーバ通信の dead interval 機能
- MAC ポートに dot1q 設定時の動作
- リンクダウン時の認証解除の抑止
- ダイナミック ACL/QoS
- RADIUS 認証方式のダイナミック VLAN モードにおける認証後 VLAN の決定

5.3.1 認証前端末の通信許可

(1) 認証専用アクセスリスト

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。

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，認証専用のアクセスリスト（以降，**認証専用アクセスリスト**と呼びます）を認証前 VLAN に設定します。

認証専用アクセスリストには，次の 2 種類を使用できます。

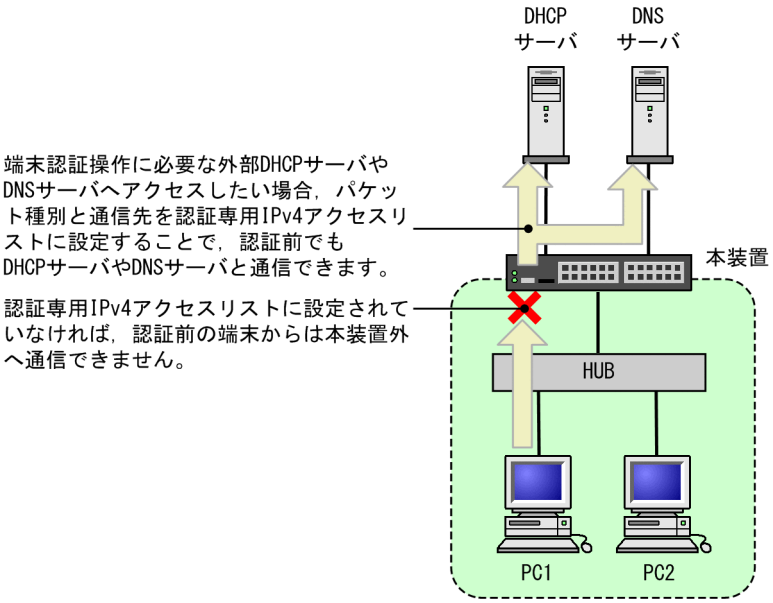
- 認証専用 IPv4 アクセスリスト（IPv4 パケットフィルタ）
- 認証専用 MAC アクセスリスト（MAC フィルタ）

なお，認証専用 IPv4 アクセスリストと認証専用 MAC アクセスリストを同一インタフェースへ設定した場合に，両方のアクセスリストにヒットするフレームを該当ポートで受信したときは，認証専用 MAC アクセスリストのフィルタ条件の動作が優先されます。

［認証専用アクセスリストの設定後の通信例］

認証専用アクセスリストの設定後の通信について，認証専用 IPv4 アクセスリストを例に説明します。

図 5-3　認証専用 IPv4 アクセスリスト設定後の通信



認証専用 IPv4 アクセスリストは，通常のアクセスリスト（コンフィグレーションコマンド ip access-group など）とは異なり，認証後は設定されたフィルタ条件が適用されません。

認証前の端末に本装置内蔵の DHCP サーバ機能から IP アドレスを配布する場合，および外部 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 DHCP 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，認証対象端末のネットワークが 10.10.10.0/24 の場合

```
permit udp 10.10.10.0 0.0.0.255 host 10.10.10.254 eq bootps
permit udp host 0.0.0.0 host 10.10.10.254 eq bootps
permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
```

［認証専用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。

- コンフィグレーションコマンド permit または deny によって次のフィルタ条件が指定されても，適用されません。
  - user-priority
  - vlan
- Web 認証専用 IP アドレスは認証専用 IPv4 アクセスリストのフィルタ条件の宛先 IP アドレスの対象外となるため，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設定をした場合でも，Web 認証専用 IP アドレスでのログイン操作ができます。

(2)　ARP パケットのリレー機能

認証前状態の端末から送信される ARP パケットは装置外へ転送できませんが，コンフィグレーションコマンド authentication arp-relay を設定すると，認証前状態の端末から送信された ARP パケットを装置外へ転送できます。

［ARP パケットのリレー機能の注意］

IEEE802.1X のみの認証ポートにおいて ARP パケットのリレー機能を使用する場合は，コンフィグレーシ

ョンコマンド dot1x supplicant-detection を auto に設定してください。auto 以外を設定して，かつ認証前端末からの ARP パケットを中継したい場合は，パケットのリレー機能は使用せず，認証専用 MAC アクセスリストで ARP パケットを permit に設定してください。

(3) 動作可能なレイヤ 2 認証

認証専用アクセスリストおよび ARP パケットのリレー機能は，すべてのレイヤ 2 認証で動作できます。

(4) DHCP snooping 設定時の注意

認証対象のポートに DHCP snooping で untrust ポートが設定された場合，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 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。

また，端末から送信される ARP パケットは DHCP snooping の対象となるため，DHCP snooping で許可された ARP パケットは装置外へ送信されます。

5.3.2 認証数制限

レイヤ 2 認証共通で認証数の制限を設定できます。

設定する単位を次に示します。

- ポート単位
- 装置単位

(1) ポート単位の認証数制限

コンフィグレーションコマンド authentication max-user で，ポート単位に認証数の制限を設定できます。各レイヤ 2 認証で認証された数がポート単位に設定された制限値を超えた場合，認証エラーとなります。

(2) 装置単位の認証数制限

コンフィグレーションコマンド authentication max-user で，装置単位に認証数の制限を設定できます。各レイヤ 2 認証で認証された合計数が装置単位に設定された制限値を超えた場合，認証エラーとなります。

(3) 認証数制限を設定できるレイヤ 2 認証

ポート単位の認証数制限，および装置単位の認証数制限を設定できるレイヤ 2 認証を次の表に示します。

表 5-9　認証数制限を設定できるレイヤ 2 認証

機能	IEEE802.1X		Web 認証		MAC 認証	
	固定 VLAN モード	ダイナミック VLAN モード	固定 VLAN モード	ダイナミック VLAN モード	固定 VLAN モード	ダイナミック VLAN モード
ポート単位の認証数制限	○※	○※	○	○	○	○
装置単位の認証数制限	○※	○※	○	○	○	○

（凡例）　○：設定できる

注※

疎通制限されている認証端末は対象外です。詳細については，「6.2.9　認証端末の疎通制限」を参照してください。

5.3.3 強制認証

コンフィグレーションコマンド authentication force-authorized enable が設定された場合，次に示すどれかの

状態が発生すると，すべてのログイン要求を認証成功とします。

- RADIUS 認証方式で，設定された RADIUS サーバからの応答がなくなったとき
- RADIUS 認証方式で，RADIUS サーバが 1 台も設定されていないとき
- ローカル認証方式で，装置内蔵の認証データが 1 件も登録されていないとき
  - Web 認証の場合は，内蔵 Web 認証 DB に 1 件もユーザ登録がないとき
  - MAC 認証の場合は，内蔵 MAC 認証 DB に 1 件も MAC アドレス登録がないとき

強制認証されたユーザに対しては，認証が解除されるまで通常の認証成功と同様に扱います。強制認証が動作する認証モードを次の表に示します。

表 5-10　強制認証が動作する認証モード

機能	IEEE802.1X		Web 認証		MAC 認証	
	固定 VLAN モード	ダイナミック VLAN モード	固定 VLAN モード	ダイナミック VLAN モード	固定 VLAN モード	ダイナミック VLAN モード
強制認証	○	○※	○	○※	○	○※

（凡例）　○：動作できる　×：動作できない

注※

ダイナミック VLAN モードの場合，強制認証で切り替える VLAN ID をコンフィグレーションコマンド authentication force-authorized vlan で指定します。なお，コンフィグレーションコマンド authentication force-authorized vlan が省略された場合は，ネイティブ VLAN の VLAN ID に切り替えます。

IEEE802.1X で強制認証した端末から送信される認証要求の処理は次のようになります。

- 強制認証によって認証成功した端末から送信される EAPOL-Start フレームは，認証成功状態の間は廃棄します。
- 強制認証によって認証成功した端末から送信される EAP フレームは，認証処理状態が認証完了の場合は廃棄します。

［強制認証設定時の注意］

強制認証は，セキュリティ上の問題となるおそれがありますので，使用する際は十分に検討してください。

例：MAC 認証専用 RADIUS サーバ使用時

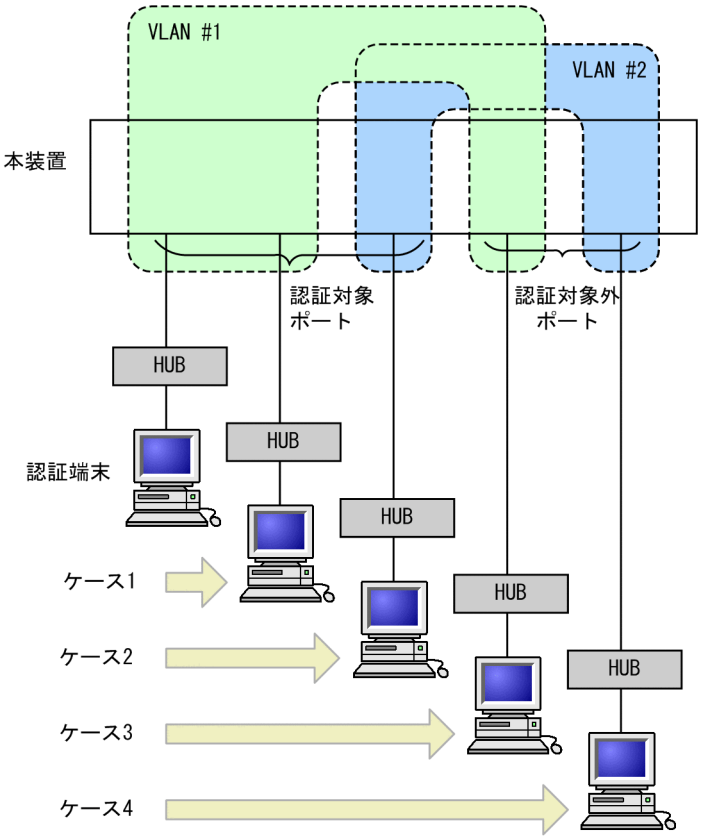
強制認証，および同一ポートに Web 認証と MAC 認証を同時に設定し，さらに，MAC 認証専用 RADIUS サーバが設定されている場合，MAC 認証専用 RADIUS サーバへ通信できないために強制認証が動作すると，MAC 認証の強制認証動作によって，Web 認証の認証対象端末も Web 認証をしなくても通信できるため注意してください。

5.3.4 認証済み端末のポート間移動および認証対象外ポートへ移動時の認証解除

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 5-4　認証済み端末のポート間移動例



なお，MAC VLAN を使用した場合，次のようにケース 1 とケース 2 を判定します。

ケース 1：

移動先の認証対象ポートで，次の条件をすべて満たしている場合は，同一の VLAN への移動と見なします。

- コンフィグレーションコマンド switchport mac vlan を設定していない，または同じ VLAN ID を設定している
- コンフィグレーションコマンド switchport mac native vlan で同じ VLAN ID を設定している
- Web 認証と MAC 認証で，コンフィグレーションコマンド switchport mac dot1q vlan を設定していない，または同じ VLAN ID を設定している

ケース 2：

移動先の認証対象ポートで，上記の条件をひとつでも満たさない場合は，異なる VLAN への移動と見なします。

これら四つのケースについて，レイヤ 2 認証ごと，およびマルチステップ認証のポート移動の動作について説明します。なお，Web 認証と MAC 認証については，認証済み端末の認証対象外ポートへの移動を検知したとき，該当端末の認証状態を解除できます。

(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 5-11　IEEE802.1X 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	認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	移動前ポートの認証状態は解除	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	移動前ポートの認証状態は解除	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	移動前ポートの認証状態が残る	通信不可
4	認証対象外ポート	別 VLAN	移動前ポートの認証状態が残る	通信可

表 5-12　IEEE802.1X 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	認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	移動前ポートの認証状態は解除	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	移動前ポートの認証状態は解除	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	移動前ポートの認証状態が残る	通信不可
4	認証対象外ポート	別 VLAN	移動前ポートの認証状態が残る	通信不可

(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 5-13　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	認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	移動先ポートで通信状態を継続	通信可
2	認証対象ポート	別 VLAN	移動前ポートの認証状態が残る	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	移動前ポートの認証状態が残る※1	通信不可※2
4	認証対象外ポート	別 VLAN	移動前ポートの認証状態が残る※1	通信可

注※1

コンフィグレーションコマンド authentication auto-logout strayer が設定されている場合は，認証対象外ポートへの移動を検出したときに認証状態を解除します。

注※2

※1 によって，認証状態が解除された場合は通信可となります。

表 5-14　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	認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	移動先ポートで認証状態を継続	通信可
2	認証対象ポート	別 VLAN	移動先ポートで認証状	通信不可

ケース	移動先ポート	VLAN	認証状態	移動後の通信可否
			態を継続※1	
3	認証対象外ポート	同一 VLAN	移動前ポートの認証状態が残る※2	通信不可※3
4	認証対象外ポート	別 VLAN	移動前ポートの認証状態が残る※2	通信不可※3

注※1

認証状態は正常に見えますが，移動先ポートで通信はできません。

注※2

コンフィグレーションコマンド authentication auto-logout strayer が設定されている場合は，認証対象外ポートへの移動を検出したときに認証状態を解除します。

注※3

※2 によって，認証状態が解除された場合は通信可となります。

(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 5-15　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	認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	移動先ポートで通信状態を継続	通信可
2	認証対象ポート	別 VLAN	移動前ポートの認証状態は解除	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	移動前ポートの認証状態が残る※1	通信不可※2
4	認証対象外ポート	別 VLAN	移動前ポートの認証状態が残る※1	通信可

注※1

コンフィグレーションコマンド authentication auto-logout strayer が設定されている場合は，認証対象外ポートへの移動を検出したときに認証状態を解除します。

注※2

※1 によって，認証状態が解除された場合は通信可となります。

表 5-16　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	認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	移動先ポートで通信状態を継続	通信可
2	認証対象ポート	別 VLAN	移動前ポートの認証状態は解除	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	移動前ポートの認証状態が残る※1	通信不可※2
4	認証対象外ポート	別 VLAN	移動前ポートの認証状態が残る※1	通信不可※2

注※1

コンフィグレーションコマンド authentication auto-logout strayer が設定されている場合は，認証対象外ポートへの移動を検出したときに認証状態を解除します。

注※2

※1 によって，認証状態が解除された場合は通信可となります。

(4) マルチステップ認証でのポート間移動の動作

マルチステップ認証で認証された端末がポートを移動した場合の動作を次の表に示します。マルチステップ認証済みの端末の認証状態は最終認証で管理されるため，ポート移動時の動作についても最終認証の動作に従います。なお，シングル認証の端末（マルチステップ認証ポートで一つの認証で認証完了となった端末）は，認証に成功したレイヤ 2 認証のポート移動の動作に従います。

表 5-17　マルチステップ認証でのポート間移動時の動作（固定 VLAN モード）

端末認証	ユーザ認証	ポート間移動の動作
MAC 認証	IEEE802.1X	IEEE802.1X でのポート間移動時の動作に従う。
	Web 認証	Web 認証でのポート間移動時の動作（固定 VLAN モード）に従う。
IEEE802.1X	Web 認証	Web 認証でのポート間移動時の動作（固定 VLAN モード）に従う。

表 5-18　マルチステップ認証でのポート間移動時の動作（ダイナミック VLAN モード）

端末認証	ユーザ認証	ポート間移動の動作
MAC 認証	IEEE802.1X	IEEE802.1X でのポート間移動時の動作に従う。
	Web 認証	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）に従う。
IEEE802.1X	Web 認証	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）に従う。

［ポート移動時の注意］

1　認証ポート間で認証済み端末のポート移動をする場合は，移動前のポートと移動先のポートで，レイヤ 2 認証と VLAN のコンフィグレーションの設定を合わせてください。次に示すケースでは，ポート間移動ができません。

- MAC ポートの VLAN に所属している認証済みの端末が，同一 VLAN で，かつ MAC ポート以外の認証ポートに移動した場合，移動前のポートでの認証状態は解除されません。
- 移動前ポートでダイナミック VLAN モードの認証済み端末が所属する VLAN と，移動先ポートでコンフィグレーションコマンド switchport mac dot1q vlan に設定している VLAN が同一の場合，移動前ポートの認証状態は解除されません。
- 異なるレイヤ 2 認証の認証ポート，または認証対象外ポートへポートを移動した場合（例えば，IEEE802.1X のポートから MAC 認証のポートへポートを移動した場合），移動前のポートでの認証状態が解除されないことがあります。
- 移動先のポートが IEEE802.1X のシングルモードまたはマルチモードの認証対象ポートの場合，ポート移動を検知できず，移動前のポートでの認証状態が解除されないことがあります。
- マルチステップ認証ポートとシングル認証の認証ポートでポートを移動した場合（例えば，マルチステップ認証ポートから MAC 認証のポート（固定 VLAN モード）へポートを移動した場合），移動元のポートでの認証状態が解除されないことがあります。

上記のどの場合でも，移動元のポートに認証状態が残り，移動先のポートで該当端末の通信はできないため，次のどれかの運用コマンドを使用して，該当端末を認証解除する必要があります。

- IEEE802.1X：clear dot1x auth-state コマンド

- MAC 認証：clear mac-authentication auth-state コマンド
- Web 認証：clear web-authentication auth-state コマンド

2　マルチステップ認証ポート間のポート移動で，同一 VLAN の別ポートへ移動の際，移動前のポートと移動後のポートでレイヤ 2 認証およびマルチステップ認証のコンフィグレーション設定が異なる場合は，ポート移動時に認証状態が解除されます。

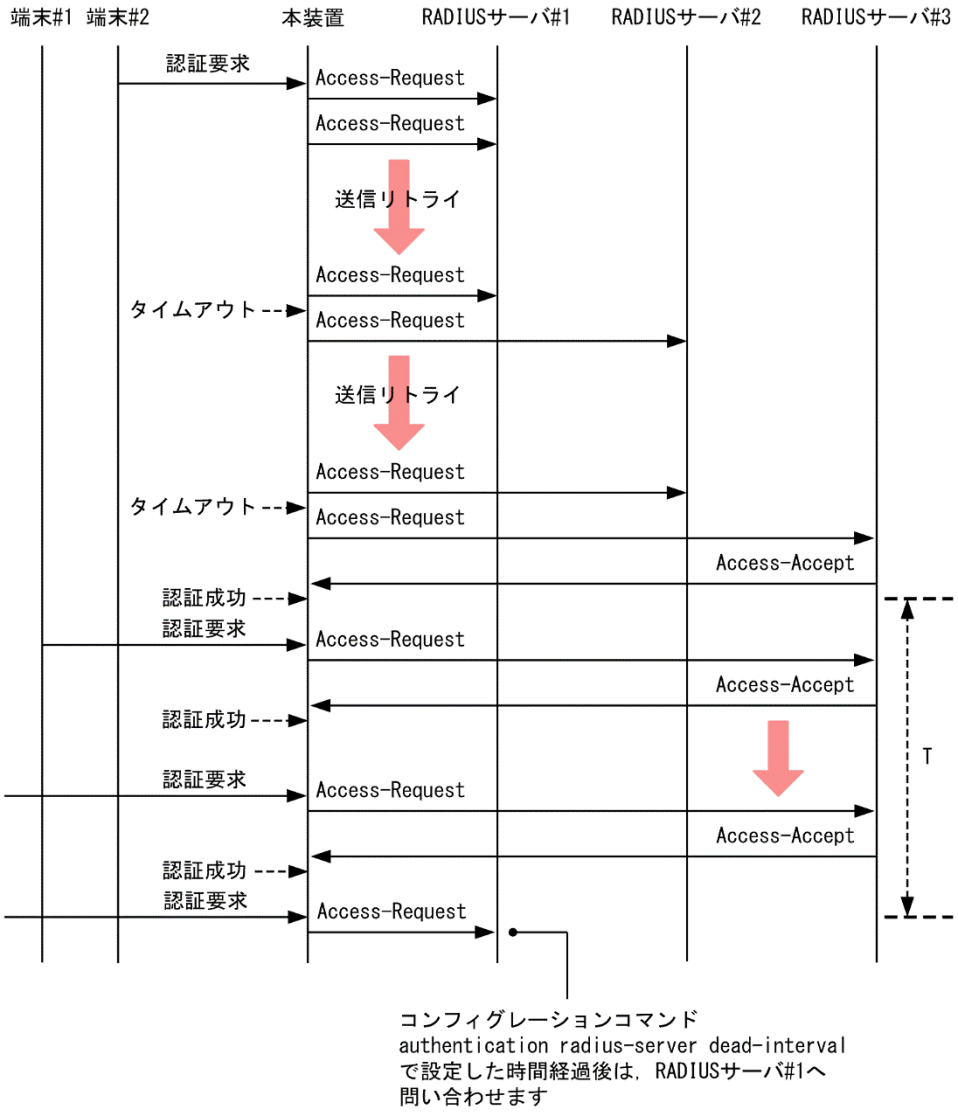
5.3.5 RADIUS サーバ通信の dead interval 機能

RADIUS サーバが無応答になったあと，コンフィグレーションコマンド authentication radius-server dead-interval で設定された時間の間，ほかの RADIUS サーバと通信して認証を実施します。また，設定された時間が経過したあとは，最初に設定した RADIUS サーバを使用して認証を実施します。また，設定されたすべての RADIUS サーバが無応答となった場合，コンフィグレーションコマンド authentication radius-server dead-interval で設定された時間の間は，RADIUS サーバとの通信が復旧しても認証失敗となります。なお，dead-interval 機能で認証失敗となった状態から最初に設定した RADIUS サーバへ通信状態に戻す場合は，次の運用コマンドを実行してください。

- IEEE802.1X：clear dot1x dead-interval-timer
- Web 認証：clear web-authentication dead-interval-timer
- MAC 認証：clear mac-authentication dead-interval-timer

RADIUS サーバ通信の dead interval 機能を次の図に示します。

図 5-5　RADIUS サーバ通信の dead interval 機能



T：コンフィグレーションコマンドauthentication radius-server dead-intervalでの設定時間

5.3.6 MAC ポートに dot1q 設定時の動作

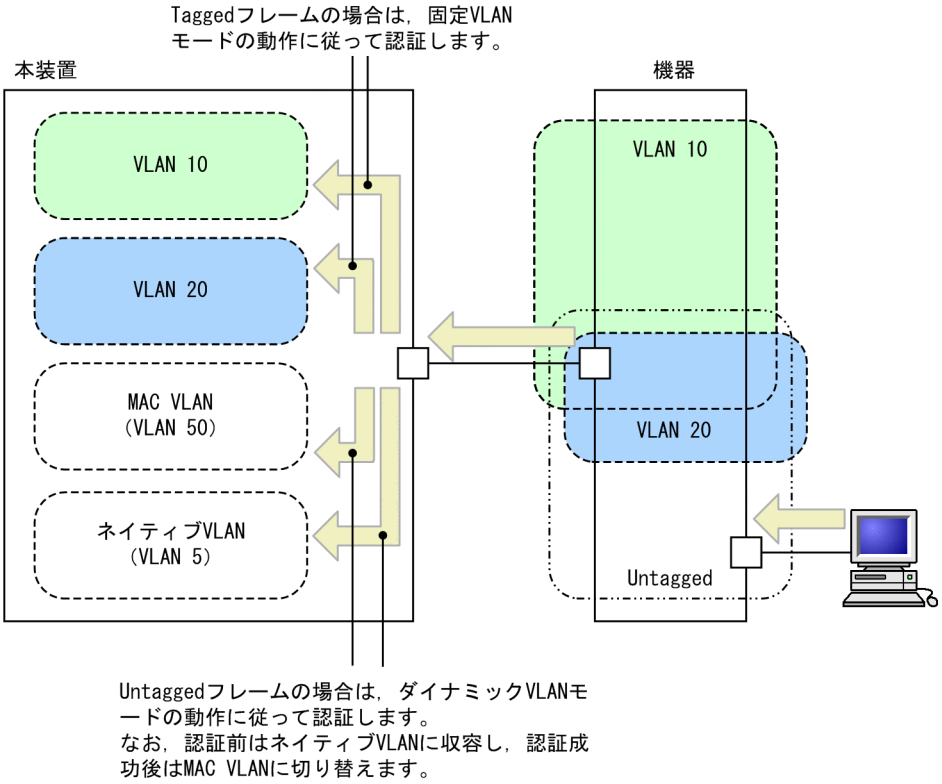
(1)　MAC ポートに dot1q 設定時の動作とレイヤ 2 認証の対応

MAC ポートにコンフィグレーションコマンド switchport mac dot1q vlan で dot1q が設定されている場合，Tagged フレームは固定 VLAN モードの動作に従って認証されます。

Untagged フレームはダイナミック VLAN モードの動作に従って認証されます。なお，Untagged フレームは認証前はネイティブ VLAN に収容され，認証成功後に認証後の VLAN ID に切り替わります。

MAC ポートに dot1q が設定されている場合の動作を次の図に示します。

図 5-6　MAC ポートに dot1q が設定されている場合の動作



MAC ポートに dot1q が設定されている場合のレイヤ 2 認証の動作を次の表に示します。

表 5-19　MAC ポートに dot1q が設定されている場合のレイヤ 2 認証の動作

受信フレーム	IEEE802.1X	Web 認証	MAC 認証
Untagged フレーム	ダイナミック VLAN モードで認証	ダイナミック VLAN モードで認証	
Tagged フレーム	認証できない	固定 VLAN モードで認証	

［MAC ポートに dot1q 設定時の注意］

コンフィグレーションコマンド switchport mac dot1q vlan に設定する VLAN ID は，該当の MAC ポートでダイナミック VLAN モードの認証後 VLAN で使用することはできません。

(2)　dot1q vlan における未認証での通信許可

MAC 認証では，コンフィグレーションコマンド switchport mac dot1q vlan で dot1q が設定されている MAC ポートに，コンフィグレーションコマンド mac-authentication dot1q-vlan force-authorized が設定されている場合，Tagged フレームの MAC アドレスに対しては認証除外と判断し，MAC 認証をしないで通信できます。

ただし，本装置ではその MAC アドレス（認証除外端末）を MAC 認証の認証端末として扱うため，次のことに注意してください。

- 認証除外端末は，該当ポートに設定された認証制限数に含まれます。
- 認証除外端末が解除された時，ログアウトを意味する動作ログメッセージが表示されます。また，認証除外端末をポート間で移動する場合も，いったん認証除外端末が解除されるため，ログアウトを意味する動作ログメッセージが表示されます。
- 次の契機で認証除外を解除します。
  - 運用コマンドによる認証除外解除

運用コマンド clear mac-authentication auth-state で認証除外端末の MAC アドレスを指定すると認証除外を解除します。
また，運用コマンド clear mac-authentication auth-state ですべての MAC 認証済み端末を解除するオプションを指定した場合も，認証除外を解除します。

- 認証除外端末接続ポートのリンクダウンによる認証除外解除
  認証除外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除外を解除します。
- 認証除外端末の MAC アドレステーブルエージングによる認証除外解除
  認証除外端末の MAC アドレステーブルのエージング時間経過後約 10 分間，認証除外端末からのアクセスがない状態が続いた場合に，認証除外を解除します。
- VLAN 設定変更による認証除外解除
  コンフィグレーションコマンドで認証除外端末が含まれる VLAN の設定を変更した場合，認証除外を解除します。
  ［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
- MAC 認証の停止による認証除外解除
  コンフィグレーションコマンド no mac-authentication system-auth-control で MAC 認証の設定が削除されて MAC 認証が停止した場合，認証除外を解除します。

5.3.7 リンクダウン時の認証解除の抑止

認証ポートがリンクダウンしたとき（チャネルグループの場合は，チャネルグループがダウンしたとき），該当ポートで，認証済みの端末の認証状態は解除されますが，コンフィグレーションコマンド no authentication logout linkdown を設定することで，認証ポートがリンクダウンしたときの認証状態を解除しないようにできます。

5.3.8 ダイナミック ACL/QoS

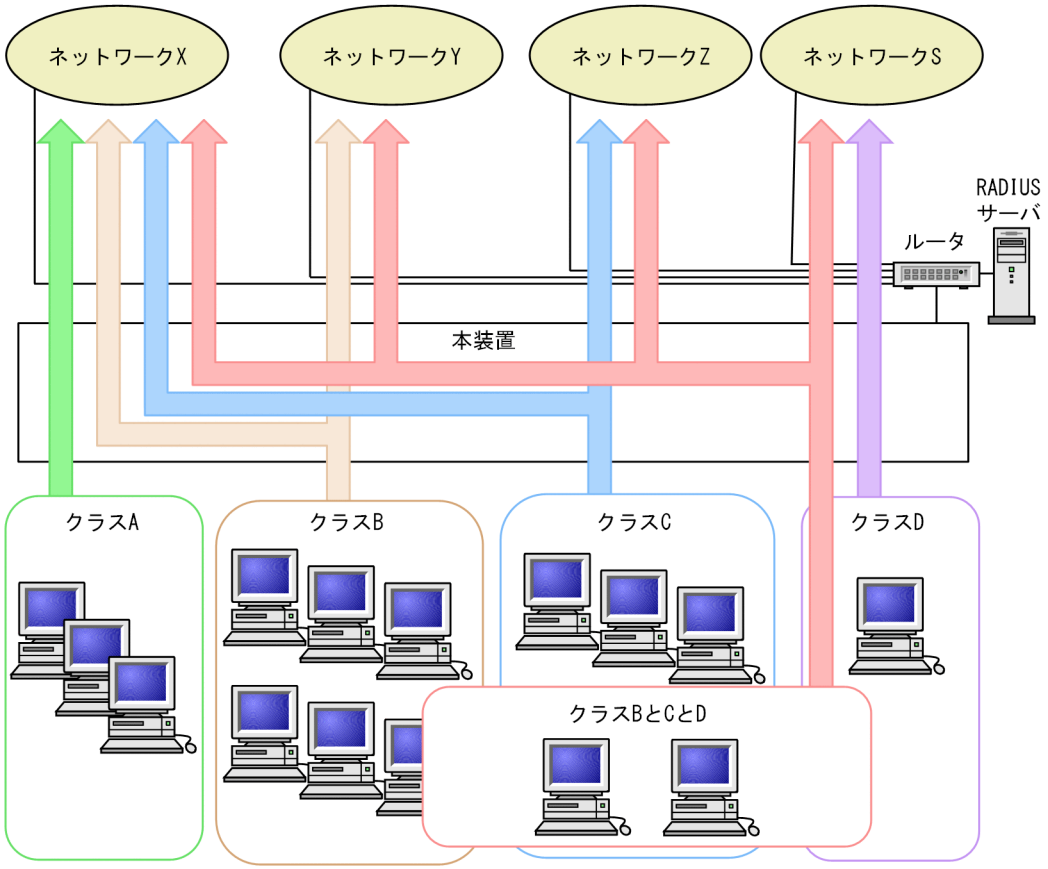
(1) 機能概要

ダイナミック ACL/QoS は，レイヤ 2 認証で認証済みとなった端末（またはユーザ）に対し，一律に通信を許可しないで，認証済み端末に付与されたクラスでネットワークのアクセス制御をします。本機能では，レイヤ 2 認証とフィルタ/QoS を併用します。

本機能では，RADIUS サーバが端末ごとにクラス情報を指定し，認証済み端末を 0～63 までの任意のクラスに所属させることができます。その上で，クラスごとのフィルタ/QoS を行うことで，ネットワークアクセス制御を実現します。

ダイナミック ACL/QoS を使用したネットワークアクセス制御を次の図に示します。

図 5-7　ダイナミック ACL/QoS を使用したネットワークアクセス制御



図中の所属するクラスとアクセス可能なネットワークの対応を次の表に示します。

表 5-20　所属するクラスとアクセス可能なネットワークの対応

所属するクラス	アクセス可能なネットワーク
クラス A の端末	ネットワーク X
クラス B の端末	ネットワーク X と Y
クラス C の端末	ネットワーク X と Z
クラス D の端末	ネットワーク S
クラス B と C と D の端末	ネットワーク X と Y と Z と S

(2)　認証方式

ダイナミック ACL/QoS は，RADIUS サーバを使用することを前提とするため，RADIUS 認証方式が使用できます。Web 認証と MAC 認証のローカル認証方式では使用できません。

(3)　クラス情報の設定と認証済み端末のクラス所属

クラス情報の設定に使用する RADIUS サーバの属性名を次の表に示します。なお，マルチステップ認証を使用する場合は，「12　マルチステップ認証」の「表 12-2　RADIUS サーバで使用する属性名」を参照してください。

表 5-21　クラス情報の設定に使用する RADIUS サーバの属性名

属性名	Type 値	説明
Filter-Id	11	クラス情報を識別するための文字列（"/Class=x"）。 （x には 0～63 までの数字が入る）

レイヤ 2 認証が成功すると，RADIUS サーバは認証済み端末ごとに 0～63 までの任意のクラス情報を通知し，認証済み端末はどれかのクラスへ所属します。なお，ダイナミック ACL/QoS を使用しない（RADIUS サーバからクラス情報を通知しない）場合，または強制認証で認証済みとなった認証済み端末の場合は，クラス 0 に所属します。

(4) サポートするフィルタ/QoS と検出条件の設定

ダイナミック ACL/QoS では，次の表に示すフィルタ/QoS のコンフィグレーションコマンドを使用できます。クラスごとに検出条件を設定することで，クラスごとのネットワークアクセス制御ができます。フロー検出条件のパラメータには，0～63 のユーザクラスと，同じく 0～63 のクラスマスクを設定できます。

なお，ユーザクラスとクラスマスクを設定する場合，フィルタ/QoS は受信側のインタフェースに設定してください。

表 5-22　ダイナミック ACL/QoS をサポートするフィルタ/QoS

機能	コンフィグレーションコマンド		サポート
フィルタ	MAC アクセスリスト	deny（mac access-list extended）	○
		permit（mac access-list extended）	
	IPv4 アクセスリスト	access-list	×
		deny（ip access-list standard）	
		permit（ip access-list standard）	
		deny（ip access-list extended）	○
		permit（ip access-list extended）	
	IPv6 アクセスリスト	deny（ipv6 access-list）	×
		permit（ipv6 access-list）	
QoS	MAC QoS フローリスト	mac qos-flow-list	○
	IPv4 QoS フローリスト	ip qos-flow-list	○
	IPv6 QoS フローリスト	ipv6 qos-flow-list	×

（凡例）　○：サポートする　×：サポートしない

(5) クラスマスクの使用方法

クラス情報とユーザクラスを 0～63 の整数として扱う場合，認証済み端末が所属するクラスとユーザクラスは同じ値を設定します。このとき，クラスマスクの設定は不要です。ところが，クラス情報とユーザクラスを 6bit のビットマップとして扱い，各ビットを特定のクラスと紐づけることで，単一クラスに所属する端末と複数クラスに所属する端末を混在させることができます。この場合に，クラスマスクの設定が必要となります。「図 5-7　ダイナミック ACL/QoS を使用したネットワークアクセス制御」のケースを用いて，説明します。

このケースでは 4 つのクラスを必要とします。各クラスの定義と，各クラスをフロー検出するための設定の例を次の表に示します。ここでは，1 ビット目から 4 ビット目を使って，4 つのクラスを表現しています。

表 5-23　クラス定義とフィルタ設定の例

クラス	クラスを示す値の定義	フィルタ（permit コマンド）の設定		
		許可するネットワーク	ユーザクラス	クラスマスク
クラス A	1 ビット目が 1 であれば，クラス A に所属とする。	X	1	同左
クラス B	2 ビット目が 1 であれば，	X と Y	2	同左

クラス	クラスを示す値の定義	フィルタ（permit コマンド）の設定		
		許可するネットワーク	ユーザクラス	クラスマスク
	クラス B に所属とする。			
クラス C	3 ビット目が 1 であれば，クラス C に所属とする。	X と Z	4	同左
クラス D	4 ビット目が 1 であれば，クラス D に所属とする。	S	8	同左

クラスマスクを設定することで，それぞれのフィルタ設定では，クラスと無関係なビットがフロー検出のチェック対象外になります。その上で，端末ごとにクラス情報を次の表のように設定することで，単一クラスに所属する端末と複数クラスに所属する端末の混在が可能になります。

表 5-24　端末ごとのクラス情報の設定の例

端末	クラス情報（（ ）は 2 進数表記の値）	フィルタ検出の動作
クラス A に所属する端末	1（000001）	クラス A のフィルタにヒットし，ネットワーク X にアクセス可能
クラス B に所属する端末	2（000010）	クラス B のフィルタにヒットし，ネットワーク X と Y にアクセス可能
クラス C に所属する端末	4（000100）	クラス C のフィルタにヒットし，ネットワーク X と Z にアクセス可能
クラス D に所属する端末	8（001000）	クラス D のフィルタにヒットし，ネットワーク S にアクセス可能
クラス B と C と D に所属する端末	14（001110）	クラス B と C と D のフィルタにそれぞれヒットし，ネットワーク X と Y と Z と S にアクセス可能

5.3.9 RADIUS 認証方式のダイナミック VLAN モードにおける認証後 VLAN の決定

RADIUS 認証方式のダイナミック VLAN モードでは，RADIUS 属性 Tunnel-Type，Tunnel-Medium-Type，および Tunnel-Private-Group-ID の値により，認証端末の認証後 VLAN を決定します。一般的な使い方としては，Tunnel-Type と Tunnel-Medium-Type は固定値を指定し，Tunnel-Private-Group-ID に任意の認証後 VLAN（どれかの MAC VLAN）の値を指定しますが，認証成功後も意図的に端末をネイティブ VLAN に収容することもできます。RADIUS 属性に指定する値の組み合わせと認証結果を次の表に示します。

なお，各 RADIUS 属性の説明は，「6　IEEE802.1X の解説」，「8　Web 認証の解説」，「10　MAC 認証の解説」を参照してください。

表 5-25　Access-Accept 受信時の RADIUS 属性の組合せによる認証動作

RADIUS 属性			認証結果	
Tunnel-Type	Tunnel-Medium-Type	Tunnel-Private-Group-ID	認証成功/失敗	認証後 VLAN
無し	無し	無し	認証成功	ネイティブ VLAN
VLAN(13)	IEEE-802(6)	無しまたは空	認証成功	ネイティブ VLAN
		switchport mac dot1q vlan と同じ VLAN	認証失敗	－
		ネイティブ VLAN	認証成功※	ネイティブ VLAN

RADIUS 属性			認証結果	
Tunnel-Type	Tunnel-Medium-Type	Tunnel-Private-Group-ID	認証成功/失敗	認証後 VLAN
		任意の MAC VLAN	認証成功	Tunnel-Private-Group-ID に指定した MAC VLAN
		上記以外	認証失敗	－
上記以外の組み合わせ			認証失敗	－

（凡例）　－：認証失敗のため無し

注※

コンフィグレーションコマンド authentication native vlan を設定していないときは認証失敗となります。

5.4 レイヤ 2 認証使用時の注意事項

5.4.1 本装置の設定および状態変更時の注意

(1) 本装置の時刻が変更された場合の注意

認証接続時間を装置の時刻を用いて管理しているので，本装置の時刻が変更された場合，認証接続時間に影響が出ます。

例えば，運用コマンド set clock で 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

IEEE802.1X，Web 認証，または MAC 認証が有効な状態のポートでコンフィグレーションコマンド switchport mode の設定変更により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，運用コマンド clear dot1x auth-state，clear web-authentication auth-state，または clear mac-authentication auth-state で端末の認証状態を解除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 dot1x，restart web-authentication，または restart mac-authentication を実行して，IEEE802.1X プログラム，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。その後，運用コマンド restart vlan mac-manager で L2MAC 管理プログラムを再起動してください。

(3) 認証プログラムを停止する場合の注意

コンフィグレーションコマンド dot1x system-auth-control，web-authentication system-auth-control，または mac-authentication system-auth-control の設定を削除して認証プログラムを停止する場合は，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，運用コマンド clear dot1x auth-state，clear web-authentication auth-state，または clear mac-authentication auth-state で端末の認証状態を解除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プログラムを停止してください。認証プログラムを停止したあと，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プログラムを停止した場合は，その後，運用コマンド restart vlan mac-manager で L2MAC 管理プログラムを再起動してください。

(4) 認証プログラムを再起動する場合の注意

認証端末が接続されている状態で運用コマンド restart dot1x，restart web-authentication，または restart mac-authentication を実行して認証プログラムを再起動したときは，運用コマンド restart vlan mac-manager で L2MAC 管理プログラムを再起動してください。

(5) 認証ポートと MAC VLAN の設定での注意

IEEE802.1X（ダイナミック VLAN モード），Web 認証（ダイナミック VLAN モード），および MAC 認証（ダイナミック VLAN モード）で設定されている認証ポート数と，コンフィグレーションコマンド vlan <vlan id list> mac-based の設定数との積が約 1600 を超えている場合，次に示す操作をすると，L2MAC 管理プログラムの初期設定時間に伴って，認証が開始されるまでおよび認証済み端末の通信が回復するまでに時間が掛かります。

- 装置の起動
- 運用コマンド reload の実行

- 運用コマンド restart vlan mac-manager の実行

5.4.2 RADIUS サーバ使用時の注意

(1) RADIUS サーバを設定する場合の注意事項

レイヤ 2 認証では，レイヤ 2 認証用の RADIUS サーバを次に示すコンフィグレーションで設定できるため，使用するレイヤ 2 認証ごとに RADIUS サーバを設定してください。

- IEEE802.1X：dot1x radius-server host コマンド
- Web 認証：web-authentication radius-server host コマンド
- MAC 認証：mac-authentication radius-server host コマンド

なお，本装置へのログイン認証に使用する RADIUS サーバをレイヤ 2 認証で使用することもできますが，使用したい場合は，該当するレイヤ 2 認証用の RADIUS サーバの設定を削除してください。

(2) 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。

(3) 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 dot1x 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 dot1x radius-server host で指定されたタイムアウト時間および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 dot1x 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 dot1x 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。

(4) IPv6 アドレスの RADIUS サーバ指定の注意事項

IPv6 アドレスの RADIUS サーバを使用する場合，リンクローカルアドレスの RADIUS サーバは使用しないでください。レイヤ 2 認証では，リンクローカルアドレスの RADIUS サーバと通信できません。

(5)　RADIUS サーバ通信の dead interval 設定時の注意事項

dead-interval タイマは 1 分ごとに動作するため，コンフィグレーションコマンド authentication radius-server dead-interval で設定された時間より，実際の時間が最大 1 分短くなる場合があります。このため 1 を設定した場合，dead-interval の時間がほぼなくなることがあります。

(6)　IEEE802.1X の RADIUS サーバタイムアウトと強制認証の注意事項

コンフィグレーションコマンド dot1x radius-server host によって，すべての RADIUS サーバが無応答を検出したタイミングよりも，コンフィグレーションコマンド dot1x timeout server-timeout によって，IEEE802.1X が先に認証サーバ応答待ちタイムアウトで認証失敗を検出した場合は，強制認証による認証成功にはなりません。

IEEE802.1X の強制認証を使用する場合は，コンフィグレーションコマンド dot1x radius-server host で指定するタイムアウト時間と再送回数によって決定されるすべての RADIUS サーバ無応答となる時間の合計より，コンフィグレーションコマンド dot1x timeout server-timeout のタイムアウト時間が長くなるように設定してください。

5.5 レイヤ 2 認証共通のコマンドガイド

5.5.1 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 5-26　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 arp-relay	認証前状態の端末からの ARP パケットを本装置の外部に転送したい場合に指定します。	○	○	○
authentication auto-logout strayer	認証ポート以外に移動した端末の認証を自動的に解除します。	－	○	○
authentication force-authorized enable	強制認証を設定します。	○	○	○
authentication force-authorized vlan	ダイナミック VLAN モードの強制認証時に切り替える VLAN ID を指定します。	○	○	○
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。	○	○	○
authentication logout linkdown	リンクダウンによる認証解除を抑止します。	○	○	○
authentication mac 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 MAC アクセスリストで指定します。	○	○	○
authentication max-user (global)	装置単位の認証数制限値を設定します。	○	○	○
authentication max-user (interface)	ポート単位の認証数制限値を設定します。	○	○	○
authentication native vlan	ダイナミック VLAN モードで，RADIUS 属性（Tunnel-Private-Group-ID）にネイティブ VLAN を指定したときに，端末の認証を許可します。	○	○	○
authentication radius-server dead-interval	RADIUS サーバ無応答時に再度，最優先 RADIUS サーバへアクセスするまでの待ち時間を設定します。	○	○	○

（凡例）　○：動作できる　－：動作できない

レイヤ 2 認証の運用コマンド一覧を次の表に示します。

表 5-27　レイヤ 2 認証の運用コマンド一覧

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
show authentication fail-list	レイヤ 2 認証に失敗した端末情報を MAC アドレスの昇順に表示します。	○	○	○
clear authentication fail-list	レイヤ 2 認証に失敗した端末情報をクリアします。	○	○	○

（凡例）　○：動作できる　－：動作できない

5.5.2 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) 認証前状態端末からの ARP パケットを本装置外部に転送する設定

［設定のポイント］

認証前状態の端末から送信された ARP パケットを本装置外部に転送する設定をします。

［コマンドによる設定］

1.
```
(config)# interface gigabitethernet 1/0/10
(config-if)# web-authentication port
(config-if)# mac-authentication port
(config-if)# authentication arp-relay
(config-if)# exit
```
Web 認証と MAC 認証の認証対象ポート 1/0/10 に ARP パケットを転送するよう設定します。

(2) 認証専用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アクセスリストを設定します（authentication ip access-group コマンドの例で説明します）。

［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)# permit ip any host 10.0.0.1
(config-ext-nacl)# exit
(config)# interface gigabitethernet 1/0/10
(config-if)# web-authentication port
(config-if)# mac-authentication port
(config-if)# authentication ip access-group 100
(config-if)# exit
```
認証前の端末から DHCP パケットと IP アドレス 10.0.0.1（DNS サーバ）へのアクセスを許可する認証専用 IPv4 アクセスリストを設定します。

(3) 強制認証の設定

［設定のポイント］

RADIUS サーバが応答しない場合，または Web 認証では内蔵 Web 認証 DB が，MAC 認証では内蔵 MAC 認証 DB が登録されていない場合に強制認証する設定をします。

［コマンドによる設定］

1. (config)# authentication force-authorized enable
   強制認証を設定します。

(4) 強制認証時に切り替える VLAN ID の設定

［設定のポイント］

ダイナミック VLAN モードで強制認証となった場合に切り替える VLAN ID を設定します。

［コマンドによる設定］

1. (config)# interface gigabitethernet 1/0/5
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac vlan 100,200
   (config-if)# web-authentication port
   (config-if)# mac-authentication port
   (config-if)# authentication force-authorized vlan 100
   (config-if)# exit
   Web 認証と MAC 認証のダイナミック VLAN モードで指定された認証対象ポート 1/0/5 に，強制認証時に切り替える VLAN ID 100 を設定します。

(5) 装置単位の認証数制限値の設定

［設定のポイント］

レイヤ 2 認証の装置単位の認証数制限を設定します。

［コマンドによる設定］

1. (config)# authentication max-user 512
   レイヤ 2 認証の装置単位の認証数制限を 512 に設定します。

(6) ポート単位の認証数制限値の設定

［設定のポイント］

レイヤ 2 認証のポート単位の認証数制限を設定します。

［コマンドによる設定］

1. (config)# interface gigabitethernet 1/0/5
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   (config-if)# mac-authentication port
   (config-if)# authentication max-user 64
   (config-if)# exit
   認証対象ポート 1/0/5 の認証数制限を 64 に設定します。

(7) RADIUS サーバへアクセス時の dead interval 時間の設定

［設定のポイント］

最優先 RADIUS サーバが無応答になったあと，ほかの RADIUS サーバで認証を始めてから，再度最優先 RADIUS サーバへアクセスを試みるまでの待ち時間(dead interval 時間)を設定します。

［コマンドによる設定］

1. (config)# authentication radius-server dead-interval 20
   RADIUS サーバの dead interval 時間を 20 分に設定します。

(8) 認証対象外ポートへ移動時の認証解除の設定

［設定のポイント］

認証対象外ポートへ移動を検知したときに認証状態を解除する設定をします。

［コマンドによる設定］

1. (config)# authentication auto-logout strayer
   認証状態を解除する設定をします。

(9)　リンクダウン時の認証解除の抑止の設定

［設定のポイント］

ポートのリンクダウン時に認証状態を解除しない設定をします。

［コマンドによる設定］

1. (config)# interface gigabitethernet 1/0/5
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   (config-if)# mac-authentication port
   (config-if)# no authentication logout linkdown
   (config-if)# exit
   認証対象ポート 1/0/5 でポートのリンクダウン時に認証状態を解除しない設定をします。

(10) ダイナミック ACL/QoS の設定

［設定のポイント］

ダイナミック ACL/QoS の設定では，フィルタ/QoS のコンフィグレーションコマンドを使用します。ここでは，認証済み端末が所属するクラスが 10 または 30 のとき，クラス 10 と 30 を対象とするフィルタを設定します。なお，この設定例では，あらかじめフロー検出モードを layer2-2 に設定しておく必要があります。

［コマンドによる設定］

1. (config)# ip access-list extended authen-classes
   (config-ext-nacl)# permit ip any 192.168.10.0 0.0.0.255 class 10
   (config-ext-nacl)# permit ip any 192.168.30.0 0.0.0.255 class 30
   (config-ext-nacl)# exit
   アクセスリスト authen-classes に，アクセス条件，ネットワーク条件，およびユーザクラスを設定します。
2. (config)# interface gigabitethernet 1/0/5
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   (config-if)# mac-authentication port
   (config-if)# ip access-group authen-classes in
   (config-if)# exit
   認証対象ポート 1/0/5 に受信側フィルタとして authen-classes を設定します（ユーザクラスを検出条件に設定している場合，in 以外は指定できません）。

6 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。

6.1 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。

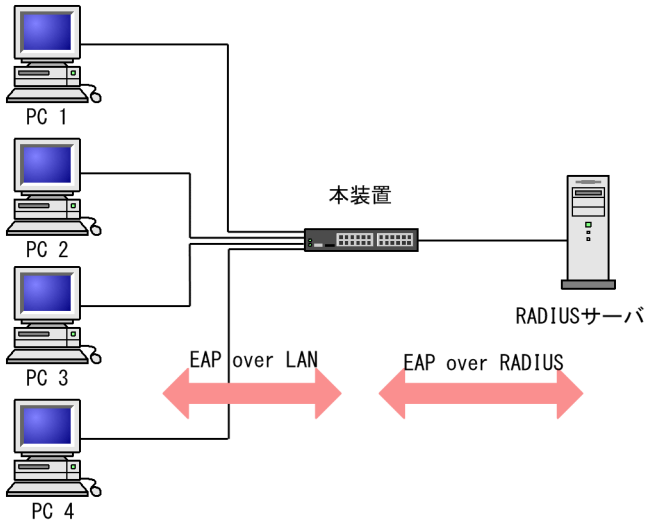
IEEE802.1X の構成要素と動作概略を次の表に示します。

表 6-1　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。

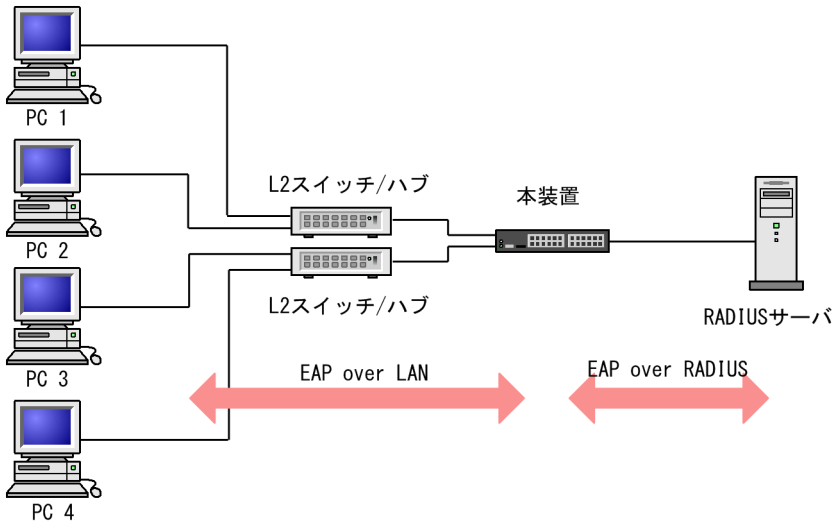
標準的な IEEE802.1X の構成では，本装置のポートに直接端末を接続して運用します。本装置を使った IEEE802.1X 基本構成を次の図に示します。

図 6-1　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 6-2　端末との間に L2 スイッチを配置した IEEE802.1X 構成



6.1.1 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 6-2　認証で使用する属性名（その 1　Access-Request)」から「表 6-5　認証で使用する属性名（その 4　Access-Reject)」に示します。

表 6-2　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（"CONNECT Ethernet"） チャネルグループ（"CONNECT Port-Channel"）
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（"Port x/0/y"） チャネルグループ（"ChGr 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。

表 6-3 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 6-4 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。
Filter-Id	11	Supplicant のセッションに適用されるフィルタ・リストの名前。 端末認証モードで意味を持つ。ただし，適用可能なフィルタが認証専用アクセスリスト固定であるため，"0"以外の値が設定されていた場合に有効（ただし，ダイナミック ACL/QoS とマルチステップ認証で使用する文字列を除く）。
Reply-Message	18	ユーザに表示されるメッセージ。
Session-Timeout	27	Supplicant の再認証タイマ値。※
Termination-Action	29	Radius サーバからの再認証タイマ満了時のアクション指示。※
Tunnel-Type	64	トンネル・タイプ。ダイナミック VLAN モードでだけ意味を持つ。 VLAN(13)固定。
Tunnel-Medium-Type	65	トンネルを作成する際のプロトコル。ダイナミック VLAN モードでだけ意味を持つ。

属性名	Type 値	説明
		IEEE802(6)固定。
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。
Tunnel-Private-Group-ID	85	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。ダイナミック VLAN モードだけ意味を持つ。 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 (3)コンフィグレーションコマンド name で指定した VLAN 名称を示す文字列 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" (3)の場合　"business-office"
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 6-5　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 6-6　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。

認証アルゴリズム	概要
	次に示す 2 種類の認証方式に対応。 ・PEAP-MS-CHAP V2：パスワードベースの資格情報を使用した認証方式 ・PEAP-TLS：証明証発行機構を使用した認証方式
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ティング情報を送信し，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ティング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 6-7　RADIUS Accounting がサポートする属性

属性名	Type 値	解説	アカウンティング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（認証成功，認証解除に関しては同じ値）。	○	○	○
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。	－	○	○

属性名	Type 値	解説	アカウンティング要求種別による送信の有無		
			start	stop	Interim-Update
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 6-8　Acct-Terminate-Cause での切断要因」を参照。	－	○	－
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。	○	○	○
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（"Port x/0/y"） チャネルグループ（"ChGr 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。	○	○	○

(凡例)　○：送信する　－：送信しない

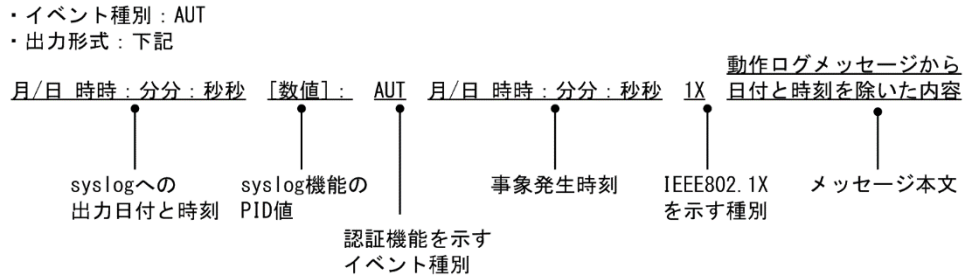
表 6-8　Acct-Terminate-Cause での切断要因

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
Idle Timeout	4	認証端末の通信がなくなったため切断した。 ・無通信監視時間が超過した場合
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
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 ・VLAN を削除または Disable にした場合 ・コンフィグレーションコマンド switchport mode を変更した場合 ・運用コマンド clear dot1x auth-state を実行した場合 ・マルチステップ認証のユーザ認証成功により切断した場合

(5)　syslog サーバへの動作ログ記録

IEEE802.1X の動作ログメッセージを syslog サーバに出力（または E-mail 送信）できます。メッセージ出力の際，IEEE802.1X を示す種別を付加するため，該当部分の出力形式を次の図に示します（E-mail 送信の場合，syslog 機能の PID 値は出力しません）。

図 6-3　syslog サーバへの出力形式



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 aut（E-mail 送信の場合，logging email-event-kind aut）によって，出力を開始および停止できます。

6.2 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。

6.2.1 認証モード

本装置の IEEE802.1X では，二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 6-9　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
固定 VLAN モード	シングルモード	－
	マルチモード	－
	端末認証モード	認証端末数制限オプション
ダイナミック VLAN モード	シングルモード	－
	端末認証モード	認証端末数制限オプション

(凡例)　－：該当なし

(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) 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。固定 VLAN モードでは，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 で通信できます。
- 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 で通信できます。

(b) 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。ダイナミック VLAN モードでは，認証ポートとして次のポートを設定できます。

- MAC ポート

(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，そのほかの端末のパケット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 6-10 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
固定 VLAN モード ダイナミック VLAN モード	1024	1	1024

6.2.2 端末検出動作切り替えオプション

本装置では，認証済み端末が存在しない場合，認証前端末を検出するために 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，認証済み端末と認証前端末が混在するため，認証済み端末が存在していても端末を検出する必要があります。しかし，EAP-Request/Identity をマルチキャスト送信すると認証済み端末も受信するため，認証済み端末の再認証が発生するなどの問題があります。

本装置では，端末認証モードの場合だけ，端末検出動作を 4 方式から選択できます。各方式の特徴を理解して，適切な端末検出動作を選択してください。端末検出動作は dot1x supplicant-detection コマンドで指定できます。指定しない場合は，shortcut で動作します。なお，本装置が送信する Request/Identity のマルチキャストは，Untagged フレームです。トランクポートを認証ポートに使用する場合，ネイティブ VLAN 以外の VLAN に所属する認証端末宛てには Request/Identity のマルチキャストを送信できません。そのため，dot1x supplicant-detection コマンドで auto を設定してください。

各方式の動作について，次で説明します。

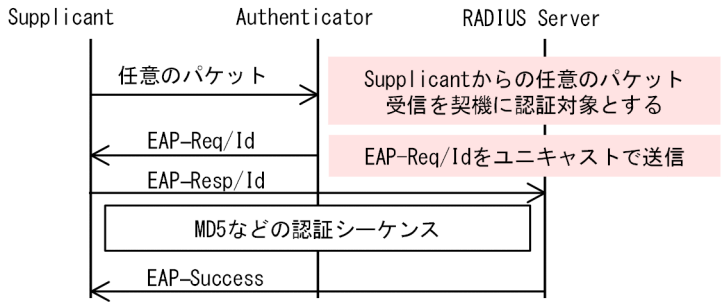
(1) auto

EAP-Request/Identity をマルチキャスト送信しません。認証前端末が送信した任意のフレームを受信することで認証前端末を検出し，認証を開始します。

この方式では，認証済み端末には EAP-Request/Identity が到達しないため，認証済み端末の再認証による負荷はありません。検出にも負荷にも問題がないため，この方式での運用をお勧めします。

auto 指定時の EAP-Request/Identity のシーケンスを次の図に示します。

図 6-4　auto 指定時の EAP-Request/Identity のシーケンス



(2)　disable

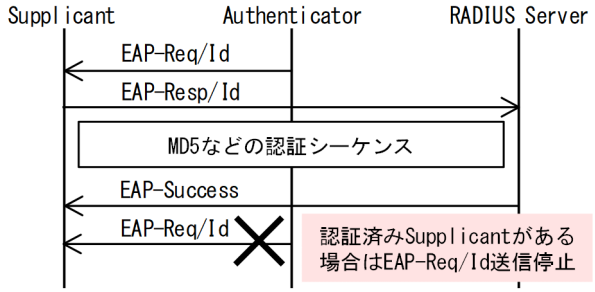
認証済み端末が存在する場合は，EAP-Request/Identity をマルチキャスト送信しません。認証前端末が送信した EAPOL-Start を受信することで認証前端末を検出し，認証を開始します。

このため，自発的に EAPOL-Start を送信しない Supplicant ソフトウェアを使用すると，認証前端末を検出できません。このような場合は，Supplicant に EAPOL-Start を送信するように設定するか，本装置の端末検出動作に auto を指定してください。

この方式では，認証済み端末に EAP-Request/Identity が到達しないため，認証済み端末の再認証による負荷はありません。

disable 指定時の EAP-Request/Identity のシーケンスを次の図に示します。

図 6-5　disable 指定時の EAP-Request/Identity のシーケンス



(3)　full

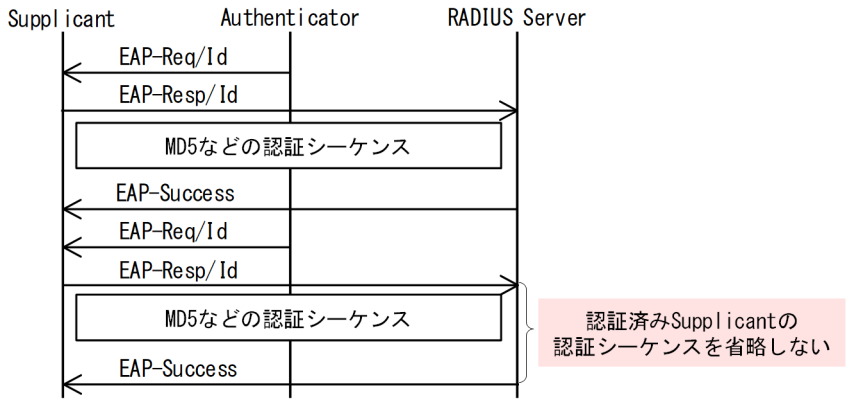
認証済み端末が存在する場合でも，EAP-Request/Identity をマルチキャスト送信します。認証前端末がこのフレームを受信し応答することで，認証を開始します。

認証済み端末もこのフレームを受信することで再認証を開始します。この方式では，認証済み端末が再認証を開始した場合，認証シーケンスを省略しないで実施します。

認証済み端末が定期的に再認証するため，端末台数に比例した負荷が掛かります。負荷の影響を避けるため，認証単位当たりの端末台数を 20 台以下にしてください。

full 指定時の EAP-Request/Identity のシーケンスを次の図に示します。

図 6-6　full 指定時の EAP-Request/Identity のシーケンス



(4)　shortcut

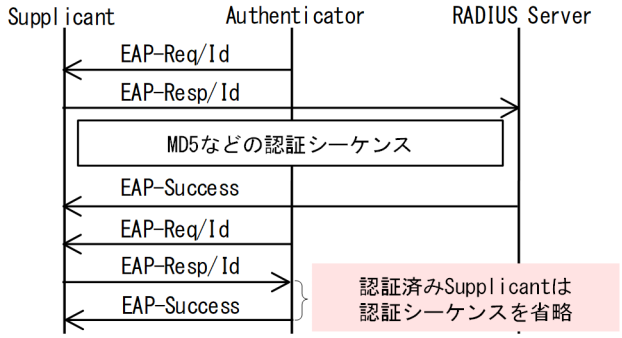
認証済み端末が存在する場合でも，EAP-Request/Identity をマルチキャスト送信します。認証前端末がこのフレームを受信し応答することで，認証を開始します。

認証済み端末もこのフレームを受信することで再認証を開始します。この方式では，認証済み端末が再認証を開始した場合，認証シーケンスを省略してすぐに EAP-Success を送信することで負荷を軽減します。

しかし，一部の Supplicant ソフトウェアでは，EAP-Success をすぐに送信する動作を認証失敗と見なします。この結果，認証後すぐに通信が途切れたり，認証後数分から数十分で通信が途切れたり，再認証を繰り返して負荷が上がったりすることがあります。

shortcut 指定時の EAP-Request/Identity のシーケンスを次の図に示します。

図 6-7　shortcut 指定時の EAP-Request/Identity のシーケンス（デフォルト）



6.2.3 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。

6.2.4 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 IP アドレスまたはホスト名を指定できますが，IEEE802.1X では IP アドレスの指定を推奨します。ホスト名を指定する場合は，「5.4.2

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，「コンフィグレーションガイド Vol.1」　「13.1　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) 端末認証モードで認証端末にフィルタを適用するときの設定

本装置でサポートする端末認証モードで認証端末に対してフィルタの適用を実施する場合，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 6-4　認証で使用する属性名（その 3　Access-Accept)」を参照してください。

- Filter-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。

6.2.5 EAPOL フォワーディング機能

本装置で IEEE802.1X を動作させない場合に，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，「コンフィグレーションガイド Vol.1」　「27.6　L2 プロトコルフレーム透過機能のコマンドガイド」を参照してください。

6.2.6 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 6-11　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
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	○	○
認証済み端末の無通信監視による認証解除	○	○

認証解除方式	固定 VLAN モード	ダイナミック VLAN モード
VLAN 設定変更による認証解除	○	○
認証モードの切り替えによる認証解除	○	○
IEEE802.1X の停止による認証解除	○	○
動的に登録された VLAN の削除によるログアウト	－	○

（凡例） ○：サポート －：該当なし

(1) 運用コマンドによる認証解除

運用コマンド clear dot1x auth-state でポートまたは 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。

(2) 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。

(3) 認証済み端末の無通信監視による認証解除

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することで，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，強制的に認証状態を解除します。

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，端末からのアクセスがなくなってから約 10 分間（60 秒周期で監視），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。

スタック構成では，無通信監視の時間が最大 3 分間（180 秒）追加されます。

なお，この機能はコンフィグレーションコマンド no dot1x 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認証状態を解除しない設定が可能）。

(4) 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

(5) 認証モードの切り替えによる認証解除

コンフィグレーションコマンドで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。

(6) IEEE802.1X 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 IEEE802.1X の定義が削除されて IEEE802.1X が停止した場合，すべての端末の認証を解除します。

(7) 動的に登録された VLAN の削除によるログアウト

動的に VLAN が作成された認証ポートにコンフィグレーションコマンド switchport mac vlan が設定された場合，該当ポートに動的に作成された VLAN ID は削除されて，VLAN に所属していた端末の認証を解除し

ます。

6.2.7 認証数制限

装置単位およびポート単位に認証数の制限が設定できます。詳細については，「5.3　レイヤ 2 認証共通の機能」を参照してください。

6.2.8 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の取扱いについては，「5.3　レイヤ 2 認証共通の機能」を参照してください。

6.2.9 認証端末の疎通制限

端末認証モードでは，認証に成功してもフィルタを適用することで疎通制限ができます。設定方法については，「6.2.4　RADIUS サーバ接続機能」を参照してください。

ただし，ダイナミック ACL/QoS，またはマルチステップ認証を使用する端末では，疎通制限ができません。

なお，疎通制限された端末は，認証数制限の対象外になります。認証数制限については，「5.3.2　認証数制限」を参照してください。

6.3 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，「5.2　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

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 IEEE802.1X 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)　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 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。

7.1 コマンドガイド

7.1.1 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 7-1　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 サーバでアカウンティング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。
dot1x 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。
dot1x 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 の動作ログメッセージを，syslog サーバ宛てまたはメールアドレス宛て（E-Mail 使用）に送信します。
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	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	認証単位の最大認証端末数を設定します。
dot1x multiple-hosts dot1x multiple-authentication	IEEE802.1X の認証サブモードを設定します。
dot1x port-control	指定インタフェースに対して，IEEE802.1X 認証を有効にします。
dot1x radius-server host	IEEE802.1X 専用に RADIUS サーバの IP アドレスなどを指定します。
dot1x 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	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	認証サブモード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，そのインタフェース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	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	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	認証サーバからの応答待ち時間を設定します。
dot1x 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	定期的な EAP-Request/Identity の送信間隔を設定します。

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 7-2　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 dead-interval-timer	dead interval 機能による 2 台目以降の RADIUS サーバへのアクセスから，1 台目の RADIUS サーバへのアクセスに戻します。
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。

7.1.2 IEEE802.1X を有効にする設定

IEEE802.1X の基本認証モード設定について説明します。

［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。

7.1.3 固定 VLAN モードの設定

特定のインタフェースに対して，認証モードを固定 VLAN モードに設定します。

［設定のポイント］

アクセスポートを設定し，そのポートで IEEE802.1X 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 1/0/1
   (config-if)# switchport mode access
   ポート 1/0/1 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
   IEEE802.1X 認証を有効にします。

7.1.4 ダイナミック VLAN モードの設定

特定のインタフェースに対して，認証モードをダイナミック VLAN モードに設定します。

［設定のポイント］

ダイナミック VLAN モードで，認証後 VLAN を設定します。MAC ポートを設定し，認証前 VLAN（ネイティブ VLAN）を設定したうえで，そのポートで IEEE802.1X 認証を有効にします。次に，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。ダイナミック VLAN モードでは，認証サブモードにマルチモードは設定できません。

［コマンドによる設定］

1. (config)# vlan 100 mac-based
   (config-vlan)# state active
   (config-vlan)# exit
   認証後 VLAN として，VLAN100 に MAC VLAN を設定します。
2. (config)# interface gigabitethernet 1/0/1
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac native vlan 10
   ポート 1/0/1 に mac-vlan モードを設定し，ネイティブ VLAN を設定します。
3. (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。
4. (config-if)# dot1x port-control auto
   IEEE802.1X 認証を有効にします。

7.1.5 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。IEEE802.1X 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］

1. (config)# interface gigabitethernet 1/0/1
   (config-if)# dot1x multiple-authentication
   (config-if)# dot1x port-control auto
   (config-if)# dot1x max-supplicant 50
   ポート 1/0/1 で認証を許可する最大端末数を 50 に設定します。

(2)　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。full は，認証処理を省略することができない Supplicant を使用している場合に設定します。full モードを指定した場合は，装置の負荷が高くなるので注意が必要です。auto は，EAP-Request/Identity をマルチキャスト送信しません。端末から送信された任意のパケットの受信を契機に，端末ごとに EAP-Request/Identity を送信します。

［コマンドによる設定］

1. (config)# interface gigabitethernet 1/0/1
   (config-if)# dot1x multiple-authentication

```
(config-if)# dot1x port-control auto
(config-if)# dot1x supplicant-detection disable
```

ポート 1/0/1 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。

7.1.6 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］

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# dot1x reauthentication
(config-if)# dot1x timeout reauth-period 360
```
ポート 1/0/1 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。

(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］

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# dot1x timeout supp-timeout 60
```
ポート 1/0/1 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 1/0/1 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］

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# dot1x reauthentication
(config-if)# dot1x ignore-eapol-start
```
ポート 1/0/1 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，設定時間には注意してください。

［コマンドによる設定］

1. (config)# interface gigabitethernet 1/0/1
   (config-if)# dot1x timeout quiet-period 300
   IEEE802.1X 認証を設定しているポート 1/0/1 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。

reauth-period ＞ tx-period ≧ (装置で認証を行う総端末数÷20)×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］

1. (config)# interface gigabitethernet 1/0/1
   (config-if)# dot1x timeout tx-period 300
   IEEE802.1X 認証を設定しているポート 1/0/1 に EAP-Request/Identity フレーム送信の時間間隔を 300 秒に設定します。

(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。dot1x radius-server host 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］

dot1x radius-server host 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］

1. (config)# interface gigabitethernet 1/0/1
   (config-if)# dot1x timeout server-timeout 300
   IEEE802.1X 認証を設定しているポート 1/0/1 に認証サーバからの応答待ち時間を 300 秒に設定します。

(7)　複数端末からの認証要求時の通信遮断時間の設定

IEEE802.1X 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 1/0/1
   (config-if)# dot1x timeout keep-unauth 1800
   IEEE802.1X 認証を設定しているポート 1/0/1 に通信遮断状態の時間を 1800 秒に設定します。

7.1.7 RADIUS サーバ関連の設定

(1)　RADIUS サーバの設定

［設定のポイント］

ユーザ認証を RADIUS サーバで行うために，IP アドレス，タイムアウト時間，再送回数，および RADIUS 鍵を設定します。なお，タイムアウト時間と再送回数を設定する場合は，dot1x timeout server-timeout コマンドの設定値に注意してください。

［コマンドによる設定］

1. (config)# dot1x radius-server host 10.0.0.200 timeout 1 retransmit 4 key "dot1xauth"
   RADIUS サーバの IP アドレス，タイムアウト時間，再送回数，および RADIUS 鍵を設定します。

(2)　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。

(3)　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。

7.1.8 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，端末の MAC アドレスのどちらかを指定できます。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 7-1　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，端末の MAC アドレスのどちらかを指定できます。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 7-2　装置内すべての IEEE802.1X 認証ポートで再認証する実行例

```
> reauthenticate dot1x
Reauthenticate all 802.1X ports and vlans. Are you sure? (y/n) :y
```

8 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。

8.1 概要

Web 認証は，Microsoft Edge 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 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。
- 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。

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 モードおよびダイナミック 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 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。

8.2 システム構成例

ここでは，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。

8.2.1 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。

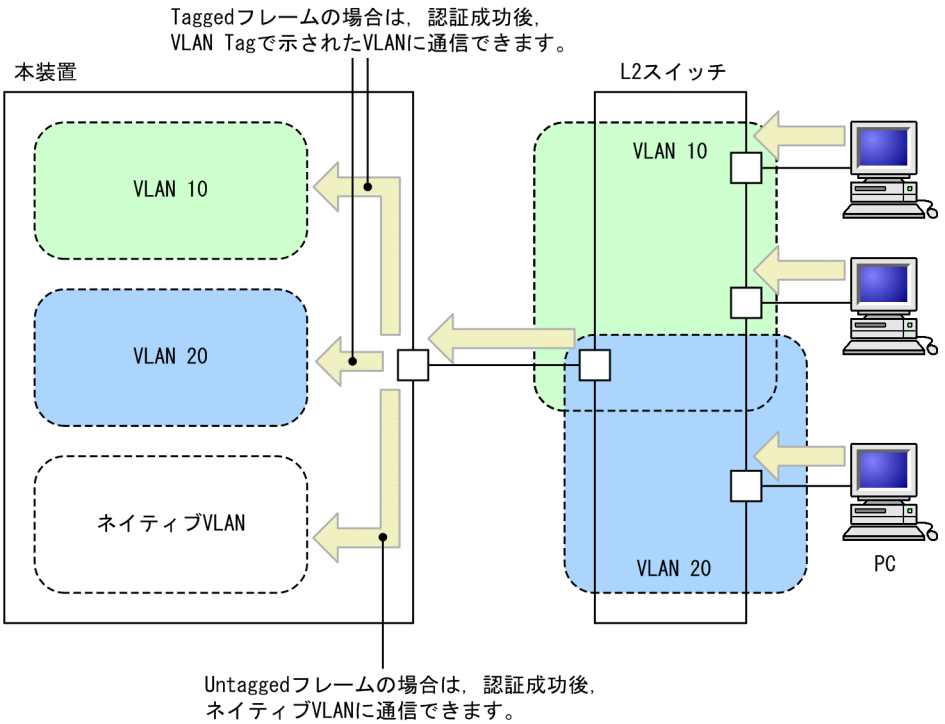
本装置では認証ポートとして次のポートを設定できます。

- アクセスポート
- トランクポート

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。

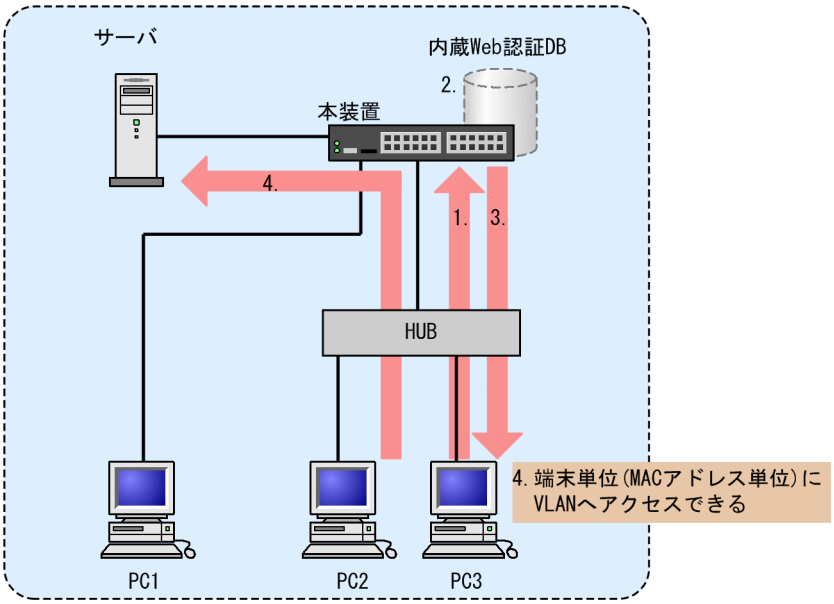
図 8-1　トランクポートの扱い



(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 8-2　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。

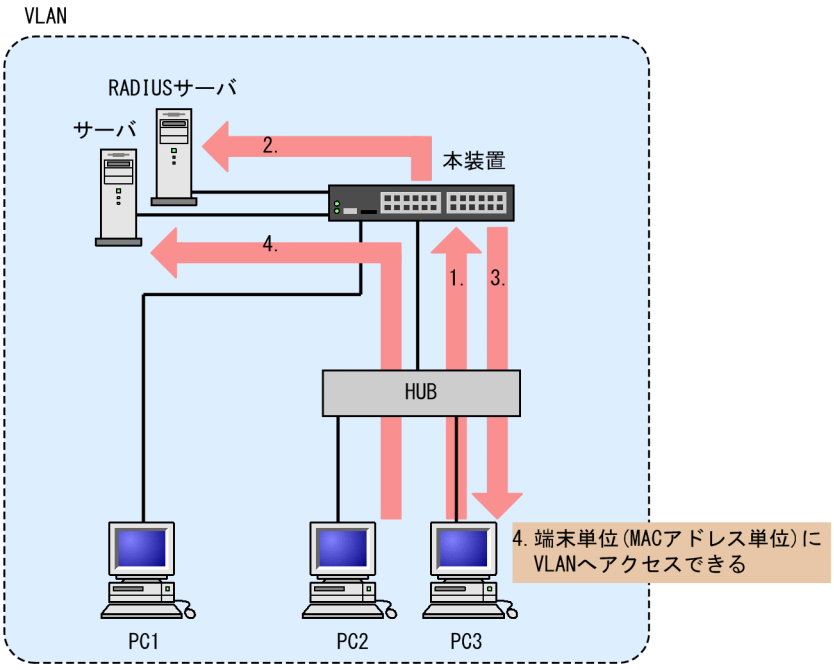
3.　認証が成功であれば，認証成功画面を PC に表示します。

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 8-3　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。

8.2.2 ダイナミック VLAN モード

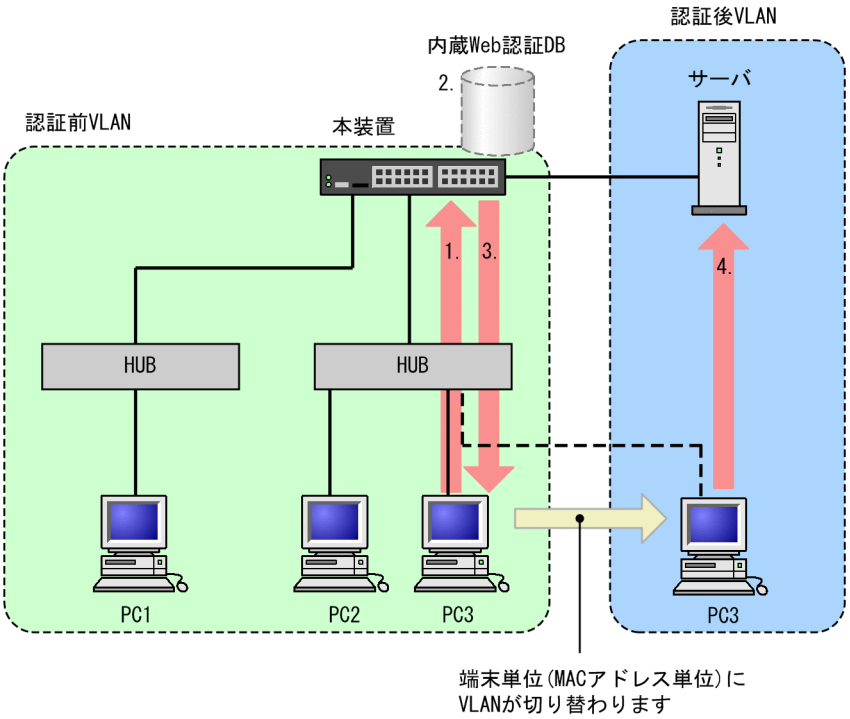
ダイナミック VLAN モードでは，認証前 VLAN に収容されていた端末を，認証成功後，内蔵 Web 認証 DB または RADIUS に登録されている VLAN ID を使用して，MAC VLAN と MAC アドレステーブルに登録して認証後 VLAN への通信を許可します。このため，次に示す設定が必要になります。

- MAC VLAN が設定されているポートを認証ポートとして設定

(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 8-4　ダイナミック VLAN モードのローカル認証方式の構成

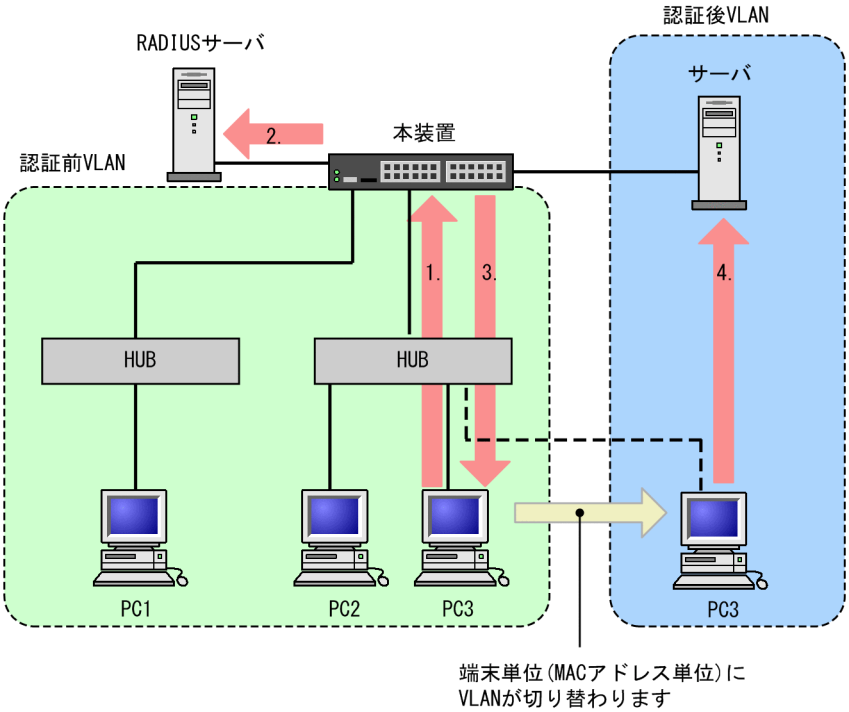


1. HUB 経由で接続された PC から Web ブラウザを起動し，本装置にアクセスします。
2. 本装置の内蔵 Web 認証 DB に登録されたユーザ情報と，PC から入力されたユーザ ID およびパスワードとの一致を確認する認証を行います。
3. 認証が成功であれば，認証成功画面を PC に表示し，認証後 VLAN へ切り替わります。
4. 認証済みの PC は，認証後 VLAN のサーバに接続できるようになります。

(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 8-5　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。

8.2.3 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にシステム構成例を示します。

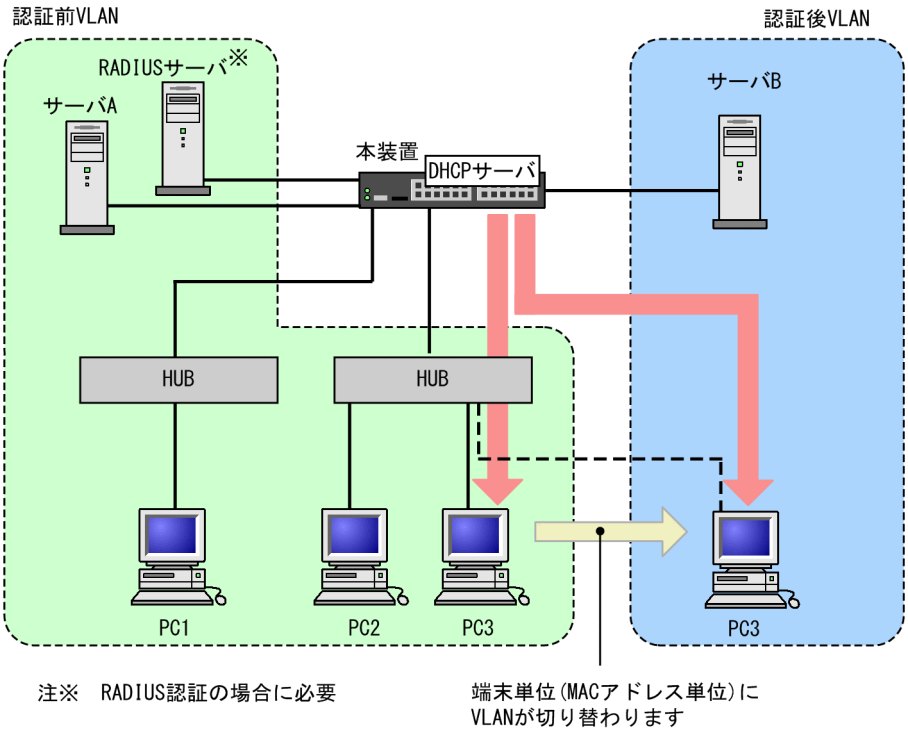
(1)　本装置内蔵の DHCP サーバ機能で IP アドレスを配布する場合

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 8-6　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。

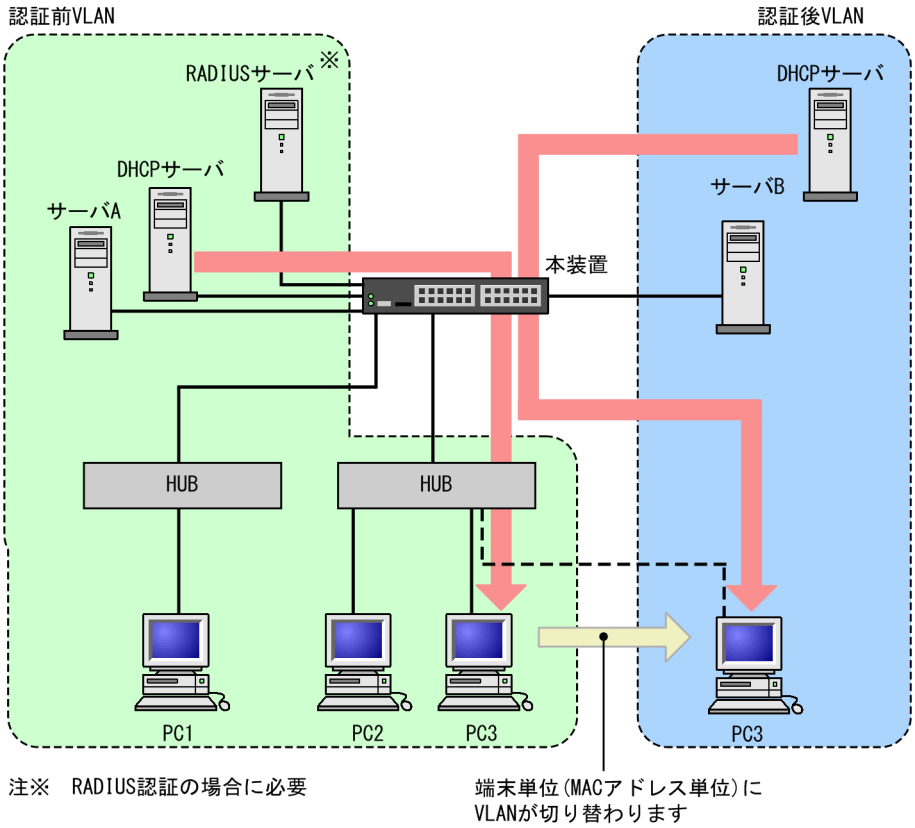
(2)　外部 DHCP サーバを使用する場合

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 8-7　Web 認証システム構成図（外部 DHCP サーバ）



注意

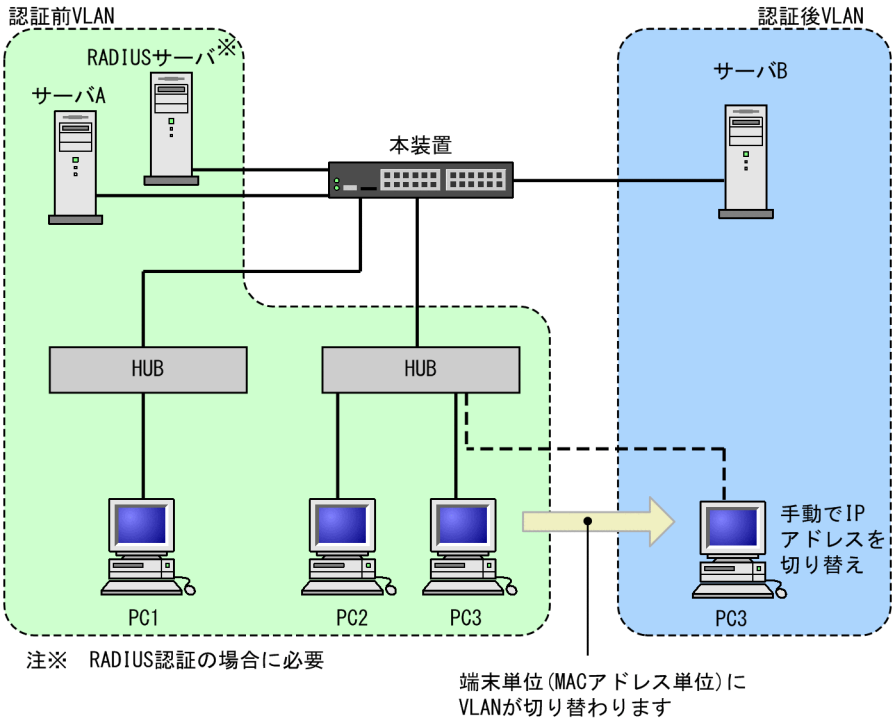
- 外部 DHCP サーバに，デフォルトゲートウェイアドレスを端末に配布するための設定が必要です。

(3)　手動で端末の 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，認証完了後に手動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，認証後に手動で 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 8-8　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。

8.3 認証機能

8.3.1 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アクセスリストの設定が必要です。認証専用アクセスリストについては「5.3　レイヤ 2 認証共通の機能」を参照してください。

8.3.2 認証ネットワークへのログイン

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

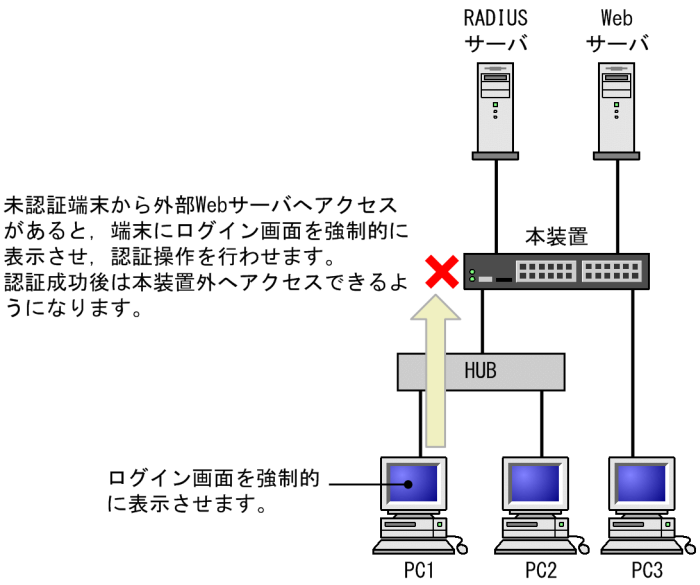
- Web 認証専用 IP アドレスを使用する場合,コンフィグレーションコマンド authentication arp-relay を設定する必要があります。設定されていない場合は，端末のデフォルトゲートウェイの設定で本装置のインタフェースの IP アドレスを指定してください。

(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 サーバ宛ての 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。

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 8-9　URL リダイレクト機能



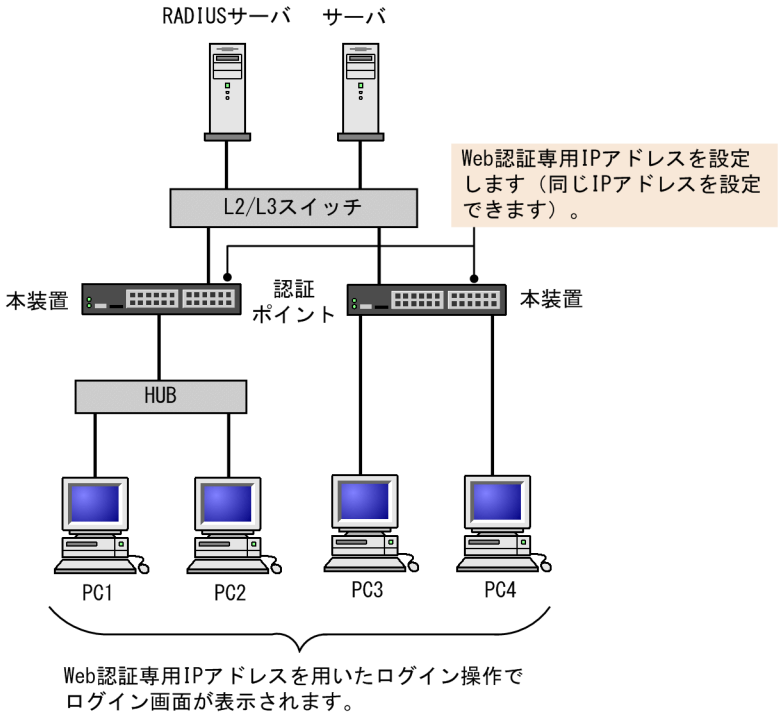
注意

端末の Web ブラウザにプロキシサーバを設定して，https で URL アクセスを実施した場合は，多くの Web ブラウザで本機能が利用できません。

(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 8-10　Web 認証専用 IP アドレスによるログイン操作



注意

端末の Web ブラウザにプロキシサーバを設定している場合は，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。

8.3.3 ユーザ切り替えオプション

ユーザ切り替えオプションは，ある端末で Web 認証のログイン済みのユーザ ID（旧ユーザ）がいる状態で，旧ユーザをログアウトしなくても，同一端末から別のユーザ ID（新ユーザ）でログインができるようにする機能です。

本オプションでユーザを切り替える（新ユーザでのログイン）ときに，新ユーザが接続した認証ポートや認証後 VLAN が旧ユーザから変わった場合，装置内の管理情報も更新されます。

なお，本オプションは，1 台の端末で，ログアウトの操作をしなくても別のユーザ（ユーザ ID）へ切り替える機能であり，同時に複数ユーザがログインできる機能ではありません。

注意

- ユーザ切り替えのとき，新ユーザのログインに失敗した場合は，旧ユーザのログイン状態を維持します。
- 新ユーザによる Web 認証のログインが成功すると，旧ユーザをログアウトした上で新ユーザをログイン状態へ移行します。
  最大端末数が認証状態（新規端末の認証ができない状態）のとき，新ユーザのログインを行う場合，旧

ユーザのログアウト直後（一時的に最大端末数の認証状態から変化する）に，別端末の新規認証が割り込むと，収容条件の超過により新ユーザのログインは失敗し，旧ユーザでの通信もできなくなります。収容条件の超過により，ユーザ切り替えが失敗した場合は，ほかの端末の認証状態を解除して，認証端末数が収容条件以内であることを確認してから，新ユーザで再認証してください。

- 旧ユーザが使用している認証ポートに対して，同じ VLAN 設定の認証ポートで新ユーザの認証が成功した場合と，異なる VLAN 設定の認証ポートで新ユーザの認証が成功した場合で，旧ユーザのログアウトの要因が異なります。
- マルチステップ認証ポート（ユーザ認証許可オプション）では，旧ユーザと新ユーザの Radius 属性 ID（Filter-ID）が異なると，新ユーザのログインに成功しても，ユーザの切り替えができないことがあります。マルチステップ認証ポートを使用して，本オプションを使用する場合は，RADIUS サーバの Filter-ID 設定に注意してください。

8.3.4 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 8-1 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
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	○	－
認証済み端末の無通信監視によるログアウト	－	○
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	○	○
Web 認証の停止によるログアウト	○	○
動的に登録された VLAN の削除によるログアウト	－	○
認証対象外ポートへの移動によるログアウト	○	○

（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) 認証済み端末の無通信監視によるログアウト

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することで，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。

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，端末からのアクセスがなくなってから約 10 分間（60 秒周期で監視），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。

スタック構成では，無通信監視の時間が最大 3 分間（180 秒）追加されます。

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）。

(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 アドレス宛てに送出された 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) 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。

(11) 動的に登録された VLAN の削除によるログアウト

動的に VLAN が作成された認証ポートにコンフィグレーションコマンド switchport mac vlan が設定された場合，該当ポートに動的に作成された VLAN ID は削除されて，VLAN に所属していた端末の認証を解除します。

(12) 認証対象外ポートへの移動によるログアウト

コンフィグレーションコマンド authentication auto-logout strayer が設定されているとき，認証された MAC アドレスを送信元 MAC アドレスとするパケットを認証対象外ポートで受信した場合，認証を解除します。

8.3.5 認証数制限

装置単位およびポート単位に認証数の制限が設定できます。詳細は，「5.3　レイヤ 2 認証共通の機能」を参照してください。

8.3.6 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ついては，「5.3　レイヤ 2 認証共通の機能」を参照してください。

8.3.7 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 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 8-2 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） ○：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）

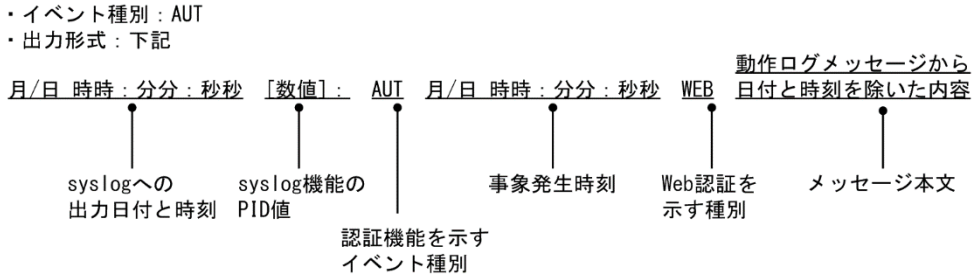
RADIUS 認証方式の場合は，RADIUS サーバが持っている機能によって，ログイン成功／失敗が記録されます。ただし，使用する RADIUS サーバによって記録される情報が異なる場合がありますので，詳細は RADIUS サーバの説明書を参照してください。

(4) syslog サーバへの動作ログ記録

Web 認証の動作ログメッセージを syslog サーバに出力（または E-mail 送信）できます。また，動作ログメ

ッセージは Web 認証のアカウントログを含みます。メッセージ出力の際，Web 認証を示す種別を付加するため，該当部分の出力形式を次の図に示します（E-mail 送信の場合，syslog 機能の PID 値は出力しません）。

図 8-11　syslog サーバへの出力形式



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（E-mail 送信の場合は，logging email-event-kind aut）によって，出力を開始および停止できます。

8.4 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 ブラウザは Microsoft Edge などの一般的な Web ブラウザを使用します。

(1)　Web 認証のログイン画面表示

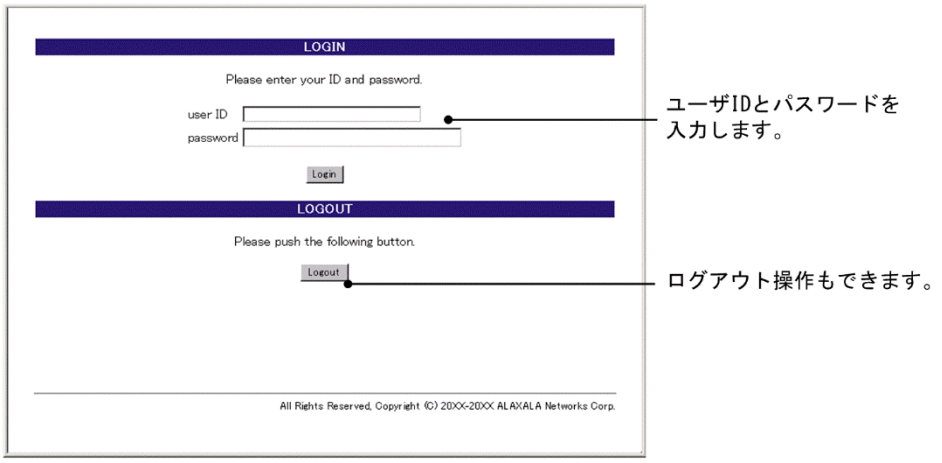
端末の Web ブラウザにログイン画面を表示して，ユーザ ID とパスワードを入力してください。

URL リダイレクト機能を使用する場合は，端末の Web ブラウザで本装置を経由する任意の Web サーバへアクセスすると，URL リダイレクト機能によって本装置の Web 認証のログイン画面が表示されます。

URL リダイレクト機能を使用しない場合は，端末の Web ブラウザで次に示すログイン URL を指定して Web 認証のログイン画面にアクセスしてください。固定 VLAN モードとダイナミック VLAN モードでは，ログイン URL の Web サーバ部分に Web 認証専用 IP アドレスを指定してください。

- HTTP 使用時：http://Web 認証専用 IP アドレス/login.html
- HTTPS 使用時：https://Web 認証専用 IP アドレス/login.html

図 8-12　ログイン画面（ブラウザ表示例）



(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

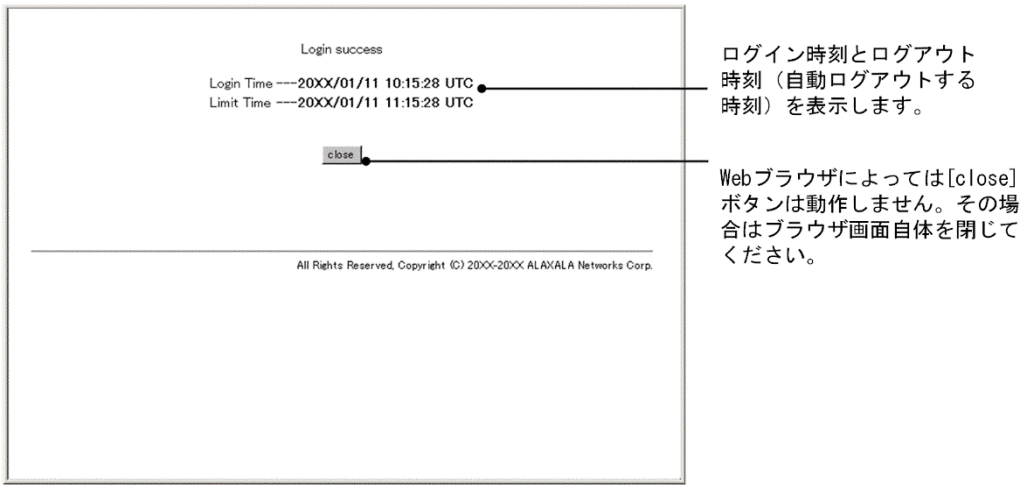
入力されたユーザ ID とパスワードを基に，ローカル認証方式の場合は内蔵 Web 認証 DB に登録されているユーザ情報と一致しているかチェックします。また，RADIUS 認証方式の場合は RADIUS サーバに問い合わせを行い，認証可否のチェックをします。

(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 8-13　ログイン成功画面（ブラウザ表示例）

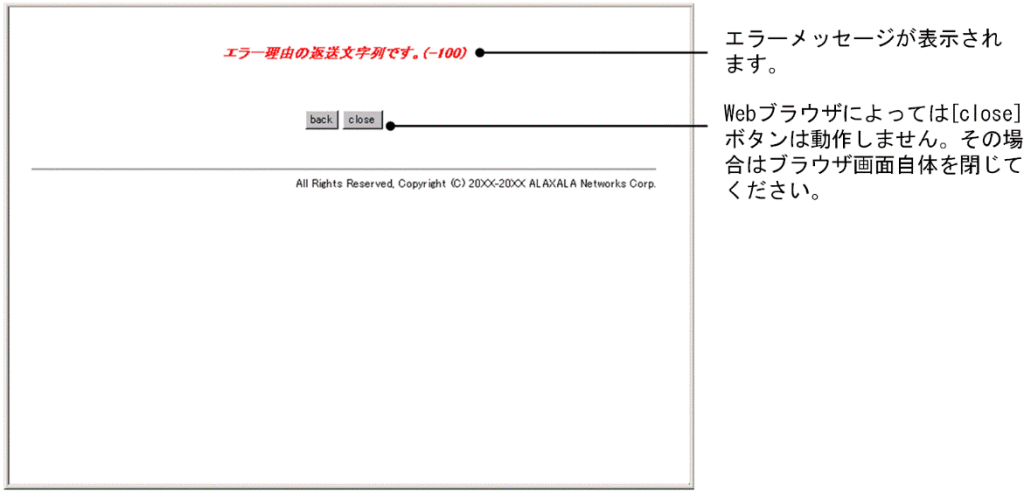


(4)　認証失敗時の画面表示

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，「8.6　認証エラーメッセージ」に示します。

図 8-14　ログイン失敗画面（ブラウザ表示例）



(5)　Web 認証からのログアウト画面表示

認証済み端末の Web ブラウザでログアウト URL を指定してアクセスし，ログアウト画面を表示します。ログアウト画面で［Logout］ボタンを押すと，Web 認証は端末の認証を解除します。認証が解除されると，ログアウト完了画面を表示します。

ログアウト URL では，URL の Web サーバ部分に Web 認証専用 IP アドレスを指定してください。

- HTTP 使用時：http://Web 認証専用 IP アドレス/logout.html
- HTTPS 使用時：https://Web 認証専用 IP アドレス/logout.html

また，ログイン画面からでもログアウトできます。ログイン画面にある［Logout］ボタンを押してください。

- HTTP 使用時：http://Web 認証専用 IP アドレス/login.html

- HTTPS 使用時：https://Web 認証専用 IP アドレス/login.html

図 8-15　ログアウト画面（ブラウザ表示例）

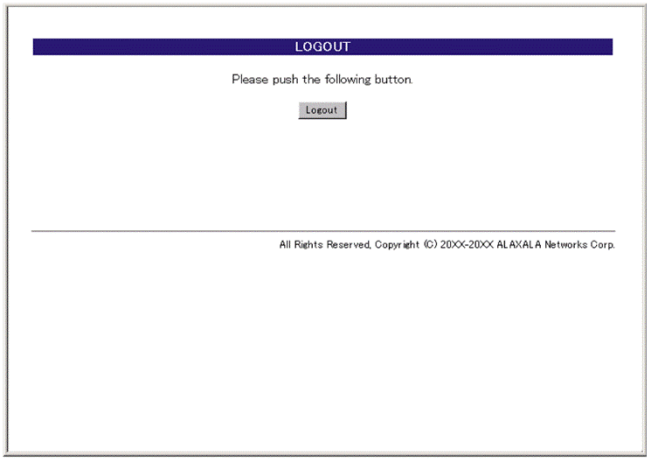
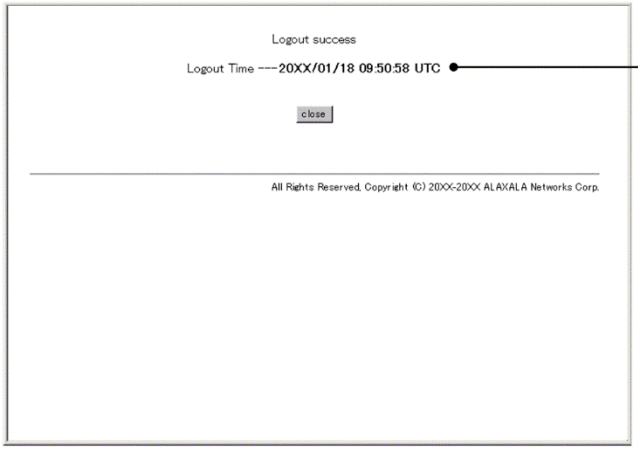


図 8-16 ログアウト完了画面（ブラウザ表示例）



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。

8.5 内蔵 Web 認証 DB および RADIUS サーバの準備

8.5.1 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。

8.5.2 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。

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
   - コンフィグレーションコマンド name で設定した VLAN 名称を設定

ユーザ ID とパスワードには文字数 1～32 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 8-3 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，指定されていなければ 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。
NAS-Port	5	認証している認証単位の IfIndex を格納します。
Service-Type	6	Framed(2)を設定します。
State	24	該当する認証に対して，直前に RADIUS サーバから Access-Challenge で送られてきた State 値を設定します。 なお，State 値がない場合は設定しません。
Called-Station-Id	30	ブリッジやアクセスポイントの MAC アドレスです。本装置の MAC アドレス（ASCII，"-"区切り）を格納します。
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。
Connect-Info	77	コネクションの特徴を示す文字列を格納します。 ポート（"CONNECT Ethernet"） チャネルグループ（"CONNECT Port-Channel"）
NAS-Port-Id	87	認証ポートを識別するための文字列を格納します。 ポート（"Port x/0/y"） チャネルグループ（"ChGr x"） （x，y には数字が入る）
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，指定されていなければ 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。

表 8-4 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。

属性名	Type 値	説明
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 を表しているので，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。 また，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 name で設定された VLAN 名称が指定された場合，VLAN 名称に対応する VLAN ID を使用します。 固定 VLAN モード時は使用しません。

表 8-5 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。
NAS-Port	5	認証している認証単位の IfIndex 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-Input-Octets	42	Accounting 情報（受信オクテット数）を格納します（(0)固定）。
Acct-Output-Octets	43	Accounting 情報（送信オクテット数）を格納します（(0)固定）。
Acct-Session-Id	44	Accounting 情報を識別する ID（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。

属性名	Type 値	説明
Acct-Input-Packets	47	Accounting 情報（受信パケット数）を格納します（(0)固定）。
Acct-Output-Packets	48	Accounting 情報（送信パケット数）を格納します（(0)固定）。
Acct-Terminate-Cause	49	Accounting 情報（セッション終了要因）を格納します。 詳細は，「表 8-6 Acct-Terminate-Cause での切断要因」を参照。
NAS-Port-Type	61	Virtual(5)を設定します。
NAS-Port-Id	87	認証するポートを識別するための文字列を格納します。 ポート（"Port x/0/y"） チャネルグループ（"ChGr x"） （x，y には数字が入る）
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。

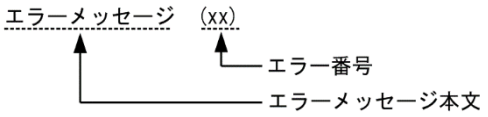
表 8-6 Acct-Terminate-Cause での切断要因

切断要因	値	解説
User Request	1	認証端末の動作により切断した。 ・認証端末が Web 画面でログアウトした場合 ・認証端末のポート移動を検出した場合
Idle Timeout	4	認証端末の通信がなくなったため切断した。 ・無通信監視時間が超過した場合 ・接続監視機能でログアウトを検出した場合
Session Timeout	5	最大接続時間の超過により切断した。
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 ・運用コマンド clear web-authentication auth-state を実行した場合
Port-Preempted	13	ユーザを切り替えるため,ログイン中ユーザのセッションを切断した。 （コンフィグレーションコマンド web-authentication user replacement 設定時）
Service Unavailable	15	認証端末のポート移動を検知したが，移動先のポートで最大認証端末数を超過したために切断した。
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 ・VLAN を削除または Disable にした場合 ・コンフィグレーションコマンド switchport mode を変更した場合

8.6 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 8-17 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 8-7 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 128 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 340 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 モードもしくはダイナミック 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 状態となっています。 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 モードもしくはダイナミック 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
	83	ログイン端末の MAC 認証に失敗したため，マルチステップ認証ができませんでした
	90	マルチステップ認証ユーザ認証許可オプション設定時，Web 認証が許可されていなかったため認証できませんでした
	92	マルチステップ認証のユーザ認証として Web 認証の認証中に，端末認証の認証状態が解除されたため，認証できませんでした
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

エラーメッセージ内容	エラー番号	エラー発生理由
		きませんでした
	48	認証対象ポートの認証制限数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)
	85	ログイン端末の端末認証の認証状態取得に失敗したためマルチステップ認証ができませんでした
	91	マルチステップ認証の認証中に強制ログアウトされたため認証できませんでした
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)
	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，83，90：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。
- 51：端末の IP アドレスを見直して，再度ログイン操作を行ってください。
- 52～54，85，91：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。
- 80～82：再度ログアウト操作を行ってください。
- 92：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，端末認証のコンフィグレーションを見直してください。

8.7 Web 認証画面入れ替え機能

8.7.1 Web 認証画面ファイルセット

Web 認証の際，認証端末の Web ブラウザに表示するログイン画面やログアウト画面などの画面情報（以降，Web 認証画面と呼びます）は，本装置に予め設定しているファイルの一式（以降，Web 認証画面ファイルセットと呼びます）を使用します。

Web 認証画面ファイルセットには，基本 Web 認証画面ファイルセットと個別 Web 認証画面ファイルセットの 2 種類があり，運用コマンド set web-authentication html-files を実行することで，ファイルセットのすべてのファイル，または一部のファイルを入れ替えることができます。

Web 認証画面ファイルセットの説明を次の表に示します。

表 8-8　Web 認証画面ファイルセット

Web 認証画面 ファイルセット	説明
基本 Web 認証画面 ファイルセット	Web 認証をする場合，認証端末のブラウザに表示する Web 認証画面のファイル一式です。運用コマンド set web-authentication html-files を実行しない場合は，デフォルトの Web 認証画面が認証端末のブラウザに表示されます。 また，運用コマンドで一部の Web 認証画面を入れ替えた場合は，入れ替えた Web 認証画面が認証端末のブラウザ表示に反映されます。
個別 Web 認証画面 ファイルセット	コンフィグレーションコマンド web-authentication html-fileset を設定した Web 認証ポートで Web 認証をする場合，認証端末のブラウザに表示する Web 認証画面のファイル一式です。 また，個別 Web 認証画面ファイルセットに一部の Web 認証画面を設定している場合，設定している Web 認証画面が認証端末のブラウザ表示に反映されます。個別 Web 認証画面ファイルセットに設定していない Web 認証画面については，基本 Web 認証画面ファイルセットの Web 認証画面を代用します。

8.7.2 Web 認証画面入れ替え機能

Web 認証画面ファイルセットの入れ替えは，運用コマンド set web-authentication html-files 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。

また，「表 8-7　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，「9.2　Web 認証画面作成手引き」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，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ますが，登録した画面が認証端末のブラウザ表示に反映されません。

- 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。

8.8 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，「5.2　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。

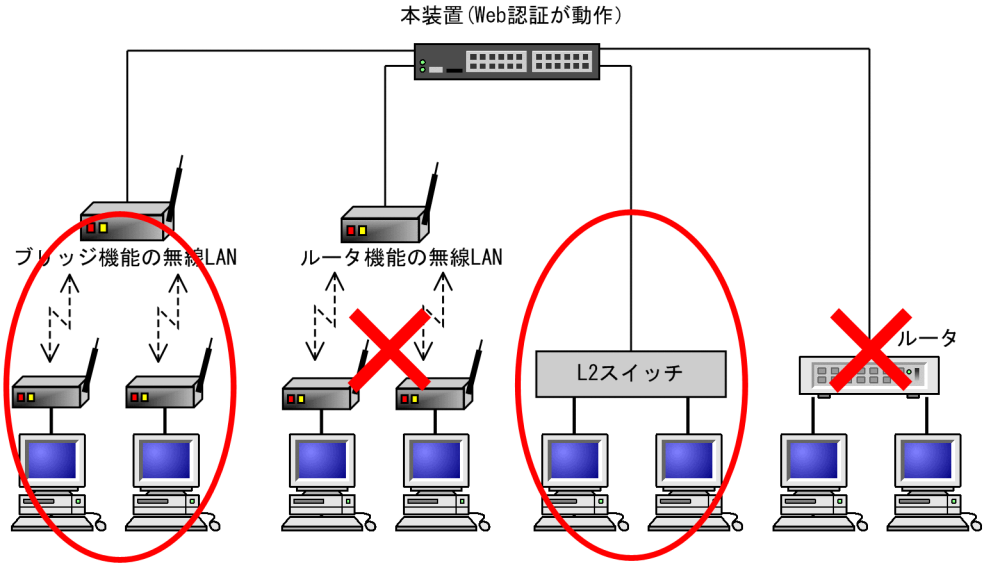
(2)　本装置と認証対象の端末間に接続する装置について

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 アドレスを認証対処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ない 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 8-18　本装置と端末間の接続



(3)　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。

(4)　DHCP サーバの IP アドレスリース時間設定について

認証対象端末に認証前 IP アドレスを DHCP サーバから配布する場合，DHCP サーバの IP アドレスリース時間をできるだけ短く設定してください。

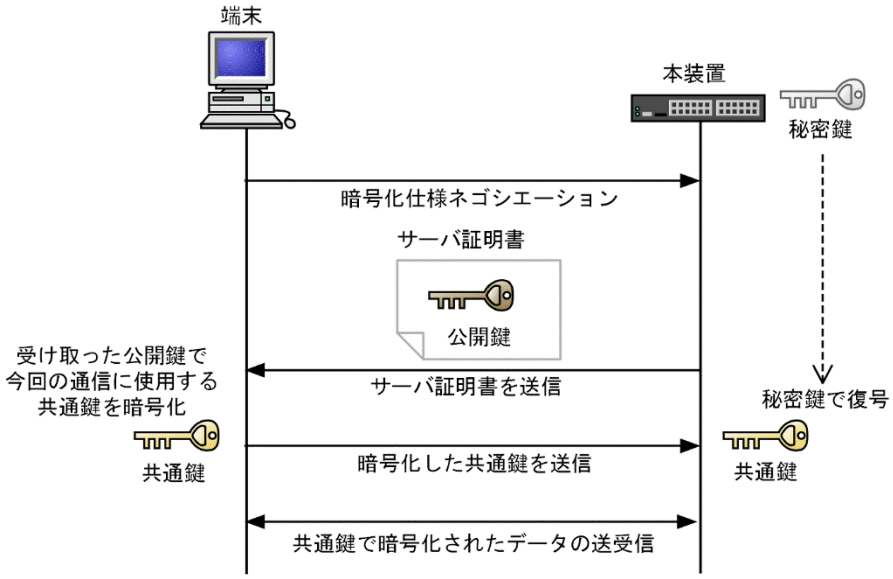
なお，内蔵 DHCP サーバに関しては，10 秒から指定できますが，小さい値を設定し，しかも，認証ユーザ数が多い場合には装置に負荷が掛かりますので，必要に応じてリース時間の設定を変更してください。

8.9 SSL 証明書の運用

8.9.1 HTTPS によるログイン・ログアウト

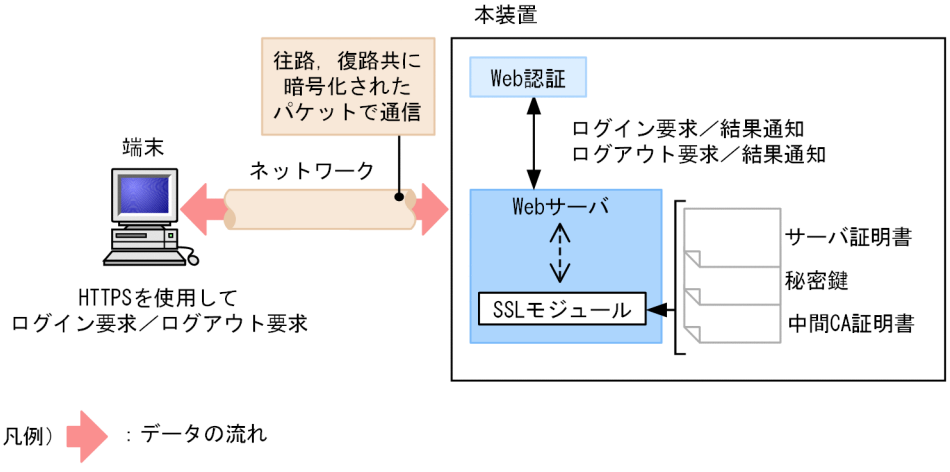
Web 認証のログイン操作およびログアウト操作の通信を他者から守るために，HTTPS が使用できます。Web 認証では，本装置をサーバに見立てた片方向の認証方式を使用して，本装置に実装された SSL モジュールによってサーバ証明書と鍵を使用して通信を暗号化します。なお，以下 SSL と表記されていた場合，TLS も含みます。SSL の動作を次の図に示します。

図 8-19　SSL の動作



ログイン操作やログアウト操作に HTTPS を使用すると，ネットワークを通過するパケットが暗号化されます。HTTPS を使用した本装置と端末間の Web 認証の通信を次の図に示します。

図 8-20　HTTPS を使用した本装置と端末間の Web 認証の通信



SSL を使用するに当たっては，本装置にサーバ証明書，秘密鍵，および中間 CA 証明書を登録する必要があります。なお，工場出荷時は，デフォルトのサーバ証明書と秘密鍵が登録されていますが，実際の運用に当たっては，利用環境に沿ったサーバ証明書，秘密鍵，および中間 CA 証明書を必ず作成して本装置に登録してください（中間 CA 証明書は，工場出荷時には登録されていません）。

8.9.2 サポート仕様

本装置がサポートする SSL の仕様を次の表に示します。

表 8-9　SSL サポート仕様

分類	内容	サポート
SSL/TLS バージョン	TLS 1.0	○
	TLS 1.1	○
	TLS 1.2	○
暗号スイート	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	○
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	○
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	○
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	○
	TLS_RSA_WITH_AES_256_GCM_SHA384	×
	TLS_RSA_WITH_AES_128_GCM_SHA256	×
	TLS_RSA_WITH_AES_256_CBC_SHA	○
	TLS_RSA_WITH_AES_128_CBC_SHA	○
	TLS_RSA_WITH_3DES_EDE_CBC_SHA	×
	TLS_RSA_WITH_RC4_128_SHA	×
認証方法	RSA（2048～4096 ビット），ECDSA（256 ビット）	○
メッセージ認証コード	SHA-256，SHA-384，SHA-512，SHA-1	○

（凡例）　○：サポートする　×：サポートしない

なお，認証方法は RSA 2048 ビットを，メッセージ認証コードは SHA-256 を推奨します。

8.9.3 運用フロー

HTTPS（SSL 通信）を使用するに当たっては，次の手順に従って作業してください。

1. PC でサーバ証明書と鍵を作成する。
2. MC を使用，または運用コマンド sftp，scp によって，サーバ証明書と鍵を本装置に転送する。
3. サーバ証明書と鍵を本装置に登録する。
4. Web 認証を再起動する。

9 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説明します。

9.1 コマンドガイド

9.1.1 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 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 web-authentication default start-stop group radius	アカウンティング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 html-fileset	ポートごとで使用する個別 Web 認証画面ファイルセット名を設定します。
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	認証成功後，端末からアクセスする URL を指定します。
web-authentication logging enable	Web 認証の動作ログメッセージを，syslog サーバ宛てまたはメールアドレス宛て（E-Mail 使用）に送信します。
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 radius-server host	Web 認証専用に RADIUS サーバの IP アドレスなどを指定します。
web-authentication redirect enable	URL リダイレクト機能を有効にします。
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 ssl connection-timeout	SSL セッション成立のタイムアウト値を設定します。
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 user replacement	ユーザ切り替えオプションを有効にします。
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。

Web 認証の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

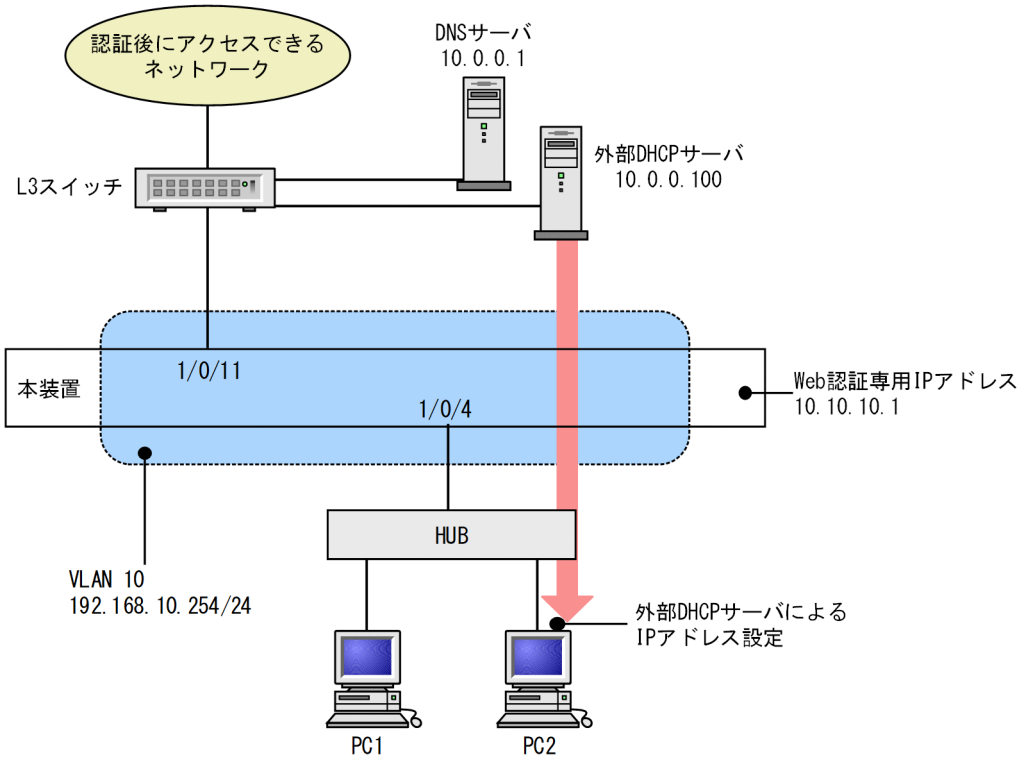
コマンド名	説明
set web-authentication user	Web 認証で使用するユーザ ID を追加します。
set web-authentication passwd	登録したユーザのパスワードを変更します。
set web-authentication vlan	登録したユーザの VLAN ID を変更します。
remove web-authentication user	登録したユーザ ID を削除します。
commit web-authentication	追加，変更した内容を内蔵 Web 認証 DB に反映します。
store web-authentication	内蔵 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 認証のコンフィグ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。
clear web-authentication dead-interval-timer	dead interval 機能による 2 台目以降の RADIUS サーバへのアクセスから，1 台目の RADIUS サーバへのアクセスに戻します。
set web-authentication ssl-crt	SSL 通信用のサーバ証明書および秘密鍵を登録します。
clear web-authentication ssl-crt	登録した SSL 証明書と秘密鍵を削除します。
show web-authentication ssl-crt	登録した SSL 証明書と秘密鍵を表示します。
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。

9.1.2 固定 VLAN モードの設定

(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 9-1　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 1/0/4
(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 1/0/11
(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) 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)# permit udp any any eq domain
   (config-ext-nacl)# exit
   (config)# interface gigabitethernet 1/0/4
   (config-if)# authentication ip access-group 100
   (config-if)# authentication arp-relay
   (config-if)# exit
   認証前の端末から DHCP パケットと DNS サーバへのアクセスを許可する認証専用 IPv4 アクセスリストを設定します。さらに，ARP パケットを本装置の外部に転送させるように設定します。

(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。

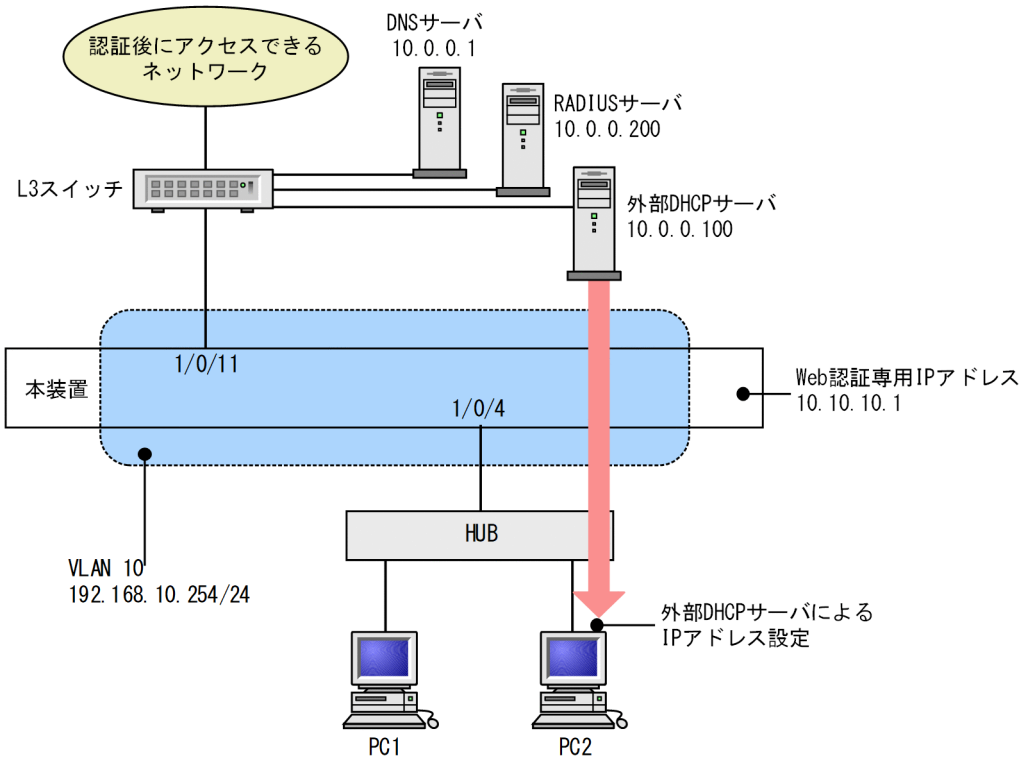
［コマンドによる設定］

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 9-2　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 1/0/4
(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 1/0/11
(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) 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)# permit udp any any eq domain
   (config-ext-nacl)# exit
   (config)# interface gigabitethernet 1/0/4
   (config-if)# authentication ip access-group 100
   (config-if)# authentication arp-relay
   (config-if)# exit
   認証前の端末から DHCP パケットと DNS サーバへのアクセスを許可する認証専用 IPv4 アクセスリストを設定します。さらに，ARP パケットを本装置の外部に転送させるように設定します。

(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。

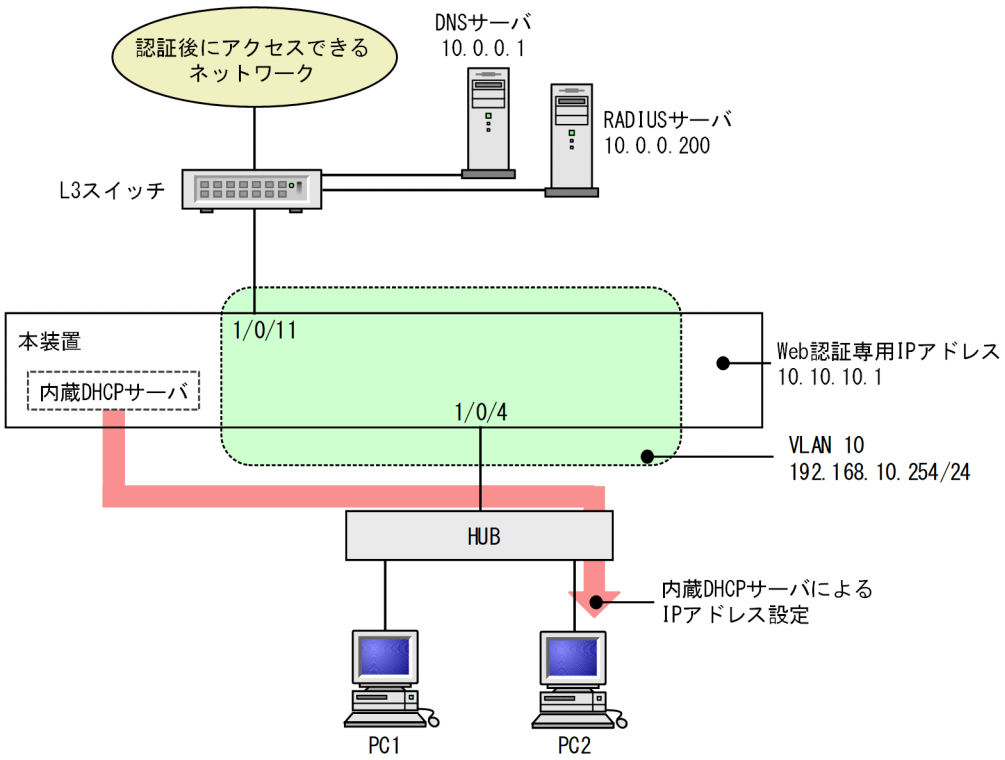
［コマンドによる設定］

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)# web-authentication 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。

(3) RADIUS 認証方式＋内蔵 DHCP サーバ使用時の設定

RADIUS 認証方式と本装置内 DHCP サーバを使用する上での基本的な構成を次の図に示します。

図 9-3　固定 VLAN モードの RADIUS 認証方式＋内蔵 DHCP サーバの基本構成



(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)# interface gigabitethernet 1/0/4
(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。

2.
```
(config)# interface gigabitethernet 1/0/11
(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) 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 host 0.0.0.0 host 192.168.10.254 eq bootps
   (config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
   (config-ext-nacl)# permit udp any any eq domain
   (config-ext-nacl)# exit
   (config)# interface gigabitethernet 1/0/4
   (config-if)# authentication ip access-group 100
   (config-if)# authentication arp-relay
   (config-if)# exit
   認証前の端末から本装置内 DHCP サーバ向けの DHCP パケットと DNS サーバへのアクセスを許可する認証専用 IPv4 アクセスリストを設定します。さらに，ARP パケットを本装置の外部に転送させるよう設定します。

(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)# web-authentication 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。

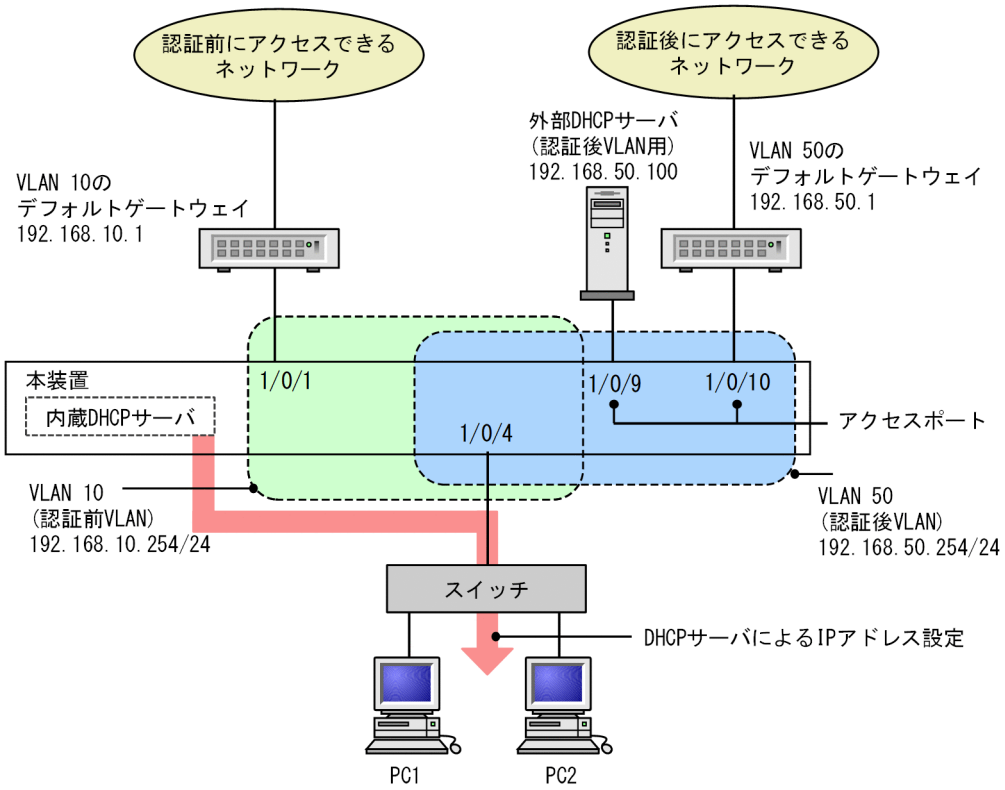
9.1.3 ダイナミック VLAN モードの設定

(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 9-4　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］

1.
```
(config)# interface gigabitethernet 1/0/4
(config-if)# switchport mode mac-vlan
(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。

2.
```
(config)# interface range gigabitethernet 1/0/9-10
(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) 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 host 0.0.0.0 host 192.168.10.254 eq bootps
(config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit ip host 192.168.10.0 host 192.168.10.1
(config-ext-nacl)# exit
(config)# interface gigabitethernet 1/0/4
(config-if)# authentication ip access-group 100
(config-if)# authentication arp-relay
(config-if)# exit
```

認証前の端末から本装置内 DHCP サーバ向けの DHCP パケットと VLAN10 のデフォルトゲートウェイ（IP アドレス 192.168.10.1）へのアクセスを許可する認証専用 IPv4 アクセスリストを設定します。さらに，ARP パケットを本装置の外部に転送させるよう設定します。

(d) VLAN 間の通信を禁止する

［設定のポイント］

認証前 VLAN と認証後 VLAN 間の通信を禁止する設定をします。

［コマンドによる設定］

1.
```
(config)# ip access-list extended 110
(config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.10.254 eq bootps
(config-ext-nacl)# permit udp host 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 110 in
(config-if)# exit
```

2.
```
(config)# ip access-list extended 150
(config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.50.100 eq bootps
(config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit udp host 192.168.50.100 any eq bootpc
(config-ext-nacl)# permit ip 192.168.50.0 0.0.0.255 192.168.50.0 0.0.0.255
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface vlan 50
(config-if)# ip access-group 150 in
(config-if)# exit
```

認証前 VLAN と認証後 VLAN 間で通信させないように設定します。

(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］

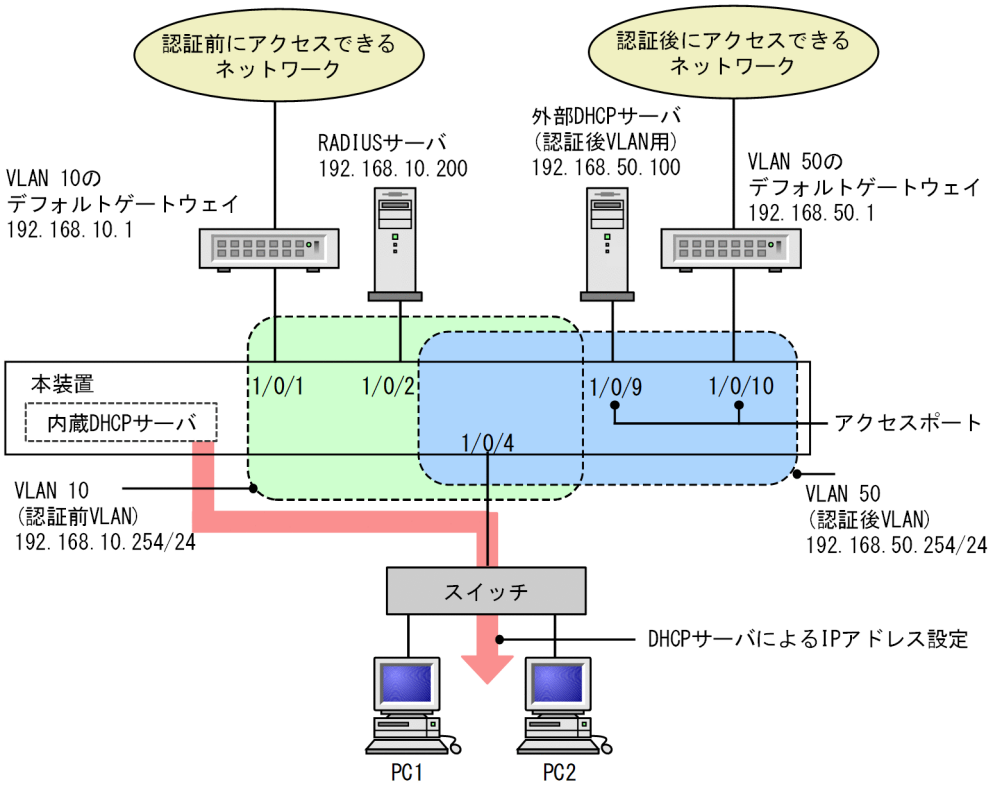
1. (config)# web-authentication ip address 10.10.10.1
   Web 認証専用の IP アドレス（IPv4 アドレス）を設定します。
2. (config)# web-authentication system-auth-control
   Web 認証を起動します。

(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。

図 9-5　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］

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 1/0/4
   (config-if)# switchport mode mac-vlan
   (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。

2.
```
(config)# interface range gigabitethernet 1/0/9-10
(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) 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 host 0.0.0.0 host 192.168.10.254 eq bootps
(config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit ip host 192.168.10.0 host 192.168.10.1
(config-ext-nacl)# exit
(config)# interface gigabitethernet 1/0/4
(config-if)# authentication ip access-group 100
(config-if)# authentication arp-relay
(config-if)# exit
```
認証前の端末から本装置内 DHCP サーバ向けの DHCP パケットと VLAN 10 のデフォルトゲートウェイ（IP アドレス 192.168.10.1）へのアクセスを許可する認証専用 IPv4 アクセスリストを設定します。さらに，ARP パケットを本装置の外部に転送させるよう設定します。

(d) VLAN 間の通信を禁止する

［設定のポイント］

認証前 VLAN と認証後 VLAN 間の通信を禁止する設定をします。

［コマンドによる設定］

1.
```
(config)# ip access-list extended 110
(config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.10.254 eq bootps
(config-ext-nacl)# permit udp host 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 110 in
(config-if)# exit
```

2.
```
(config)# ip access-list extended 150
(config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.50.100 eq bootps
(config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit udp host 192.168.50.100 any eq bootpc
(config-ext-nacl)# permit ip 192.168.50.0 0.0.0.255 192.168.50.0 0.0.0.255
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface vlan 50
(config-if)# ip access-group 150 in
(config-if)# exit
```
認証前 VLAN と認証後 VLAN 間で通信させないように設定します。

(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 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)# web-authentication 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。

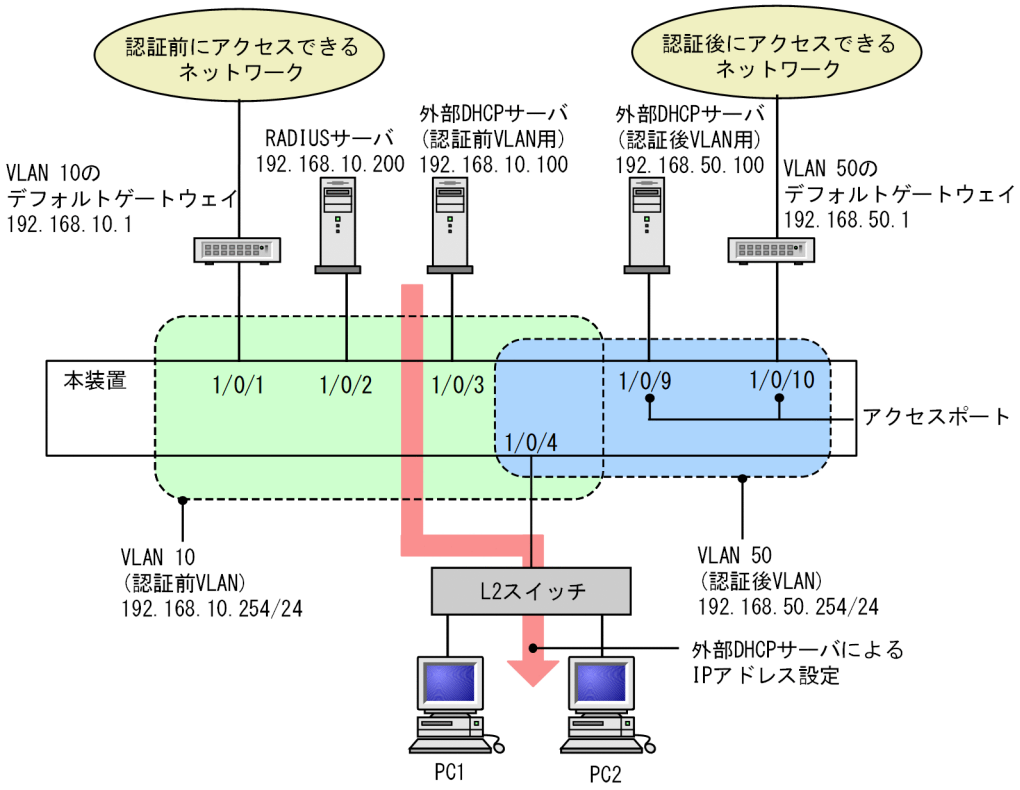
3.
```
(config)# web-authentication system-auth-control
```
Web 認証を起動します。

(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 9-6　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］

1.
```
(config)# interface gigabitethernet 1/0/4
(config-if)# switchport mode mac-vlan
(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。

2.
```
(config)# interface range gigabitethernet 1/0/9-10
(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) 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 host 0.0.0.0 host 192.168.10.100 eq bootps
(config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit ip host 192.168.10.0 host 192.168.10.1
(config-ext-nacl)# exit
(config)# interface gigabitethernet 1/0/4
(config-if)# authentication ip access-group 100
(config-if)# authentication arp-relay
(config-if)# exit
```

認証前の端末から外部 DHCP サーバ向けの DHCP パケットと VLAN 10 のデフォルトゲートウェイ（IP アドレス 192.168.10.1）へのアクセスを許可する認証専用 IPv4 アクセスリストを設定します。さらに，ARP パケットを本装置の外部に転送させるよう設定します。

(d) VLAN 間の通信を禁止する

［設定のポイント］

認証前 VLAN と認証後 VLAN 間の通信を禁止する設定をします。

［コマンドによる設定］

1.
```
(config)# ip access-list extended 110
(config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.10.254 eq bootps
(config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit udp host 192.168.10.100 any eq bootpc
(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 110 in
(config-if)# exit
```

2.
```
(config)# ip access-list extended 150
(config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.50.100 eq bootps
(config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit udp host 192.168.50.100 any eq bootpc
(config-ext-nacl)# permit ip 192.168.50.0 0.0.0.255 192.168.50.0 0.0.0.255
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface vlan 50
(config-if)# ip access-group 150 in
(config-if)# exit
```

認証前 VLAN と認証後 VLAN 間で通信させないように設定します。

(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 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)# web-authentication 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。

9.1.4 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）

［設定のポイント］

Web 認証のダイナミック 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 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 web-authentication radius-server host 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。

(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］

Web 認証を使用中に設定を変更した場合は，直ちに，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。なお，認証途中のユーザは再度ログイン操作が必要です。

(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］

Web 認証を使用中に設定を変更した場合は，直ちに，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。なお，認証途中のユーザは再度ログイン操作が必要です。

(8) URL リダイレクト機能の無効設定（固定 VLAN モード，ダイナミック VLAN モード）

［設定のポイント］

Web 認証の URL リダイレクト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 redirect enable
   Web 認証の URL リダイレクト機能を無効にします。

［注意事項］

Web 認証を使用中に設定を変更した場合は，直ちに，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。なお，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（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］

Web 認証を使用中に設定を変更した場合は，直ちに，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。なお，認証途中のユーザは再度ログイン操作が必要です。

(10) 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。

(11) 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。

(12) 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）。なお，49152 番以降は，Web 認証以外で使用することがあります。サービスポート番号を他機能が使用すると Web 認証が動作しないため，サービスポート番号は 49152 番より前の番号を設定してください。

［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］

Web 認証を使用中に設定を変更した場合は，直ちに，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。なお，認証途中のユーザは再度ログイン操作が必要です。

(13) 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。

(14) ユーザ切り替えオプションの設定

［設定のポイント］

ユーザ切り替えオプションを使用する場合，オプション有効の設定をします。

［コマンドによる設定］

1. (config)# web-authentication user replacement
   ユーザ切り替えオプション有効の設定をします。

9.1.5 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 1/0/4
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   (config-if)# web-authentication port
   (config-if)# exit
   (config)# interface gigabitethernet 1/0/10
   (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 1/0/4 は認証対象ポートとして設定します。また，ポート 1/0/10 には認証しないで通信を許可する設定をします。

(2) 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 1/0/10
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 50
   (config-if)# exit
   MAC VLAN ID 50 のポート 1/0/10 に対して，認証しないで通信を許可する設定をします。

9.1.6 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グ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（PPPP4321）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
```

9.1.7 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 store web-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 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 load web-authentication コマンドで内蔵 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
#
```

9.1.8 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 9-7　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。

9.1.9 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 9-8　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.
#
```

9.1.10 dead interval 機能による RADIUS サーバアクセスを 1 台目の RADIUS サーバに戻す

1 台目の RADIUS サーバが無応答になり，dead interval 機能によって，2 台目以降の RADIUS サーバへのアクセスに切り替わった場合，コンフィグレーションコマンド authentication radius-server dead-interval で設定された時間を待たないで最初の RADIUS サーバへのアクセスに戻すには，clear web-authentication dead-interval-timer コマンドを実行します。

図 9-9　1 台目の RADIUS サーバへの切り替え

```
# clear web-authentication dead-interval-timer
#
```

9.2 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，および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。ログイン画面については「9.2.1　ログイン画面（login.html）」を，ログアウト画面については「9.2.2　ログアウト画面（logout.html）」を参照してください。

また，「表 8-7　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，「9.2.3 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。

9.2.1 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 9-3　ログイン画面に必要な設定

記述内容	意味
<form name="Login" method="post" action="/cgi-bin/Login.cgi"></form>	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。
<input type="text" name="uid" size="40" maxlength="32" autocomplete="OFF" />	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<form></form>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。
<input type="password" name="pwd" size="40" maxlength="32" autocomplete="OFF" />	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<form></form>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
<input type="submit" value="Login" />	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<form></form>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）　< img src="/image_file.gif" >

(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。

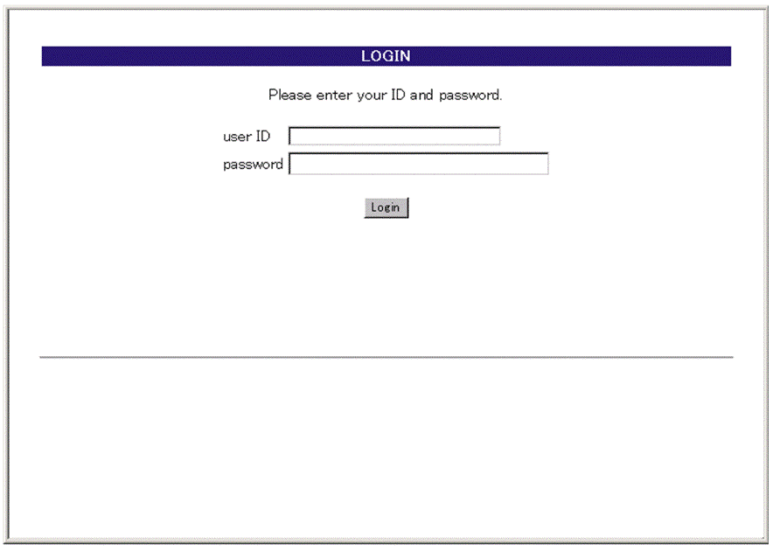
図 9-10　ログイン画面（login.html）のソース例

```
<?xml version="1.0" encoding="utf-8"?>
<!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="en" lang="en">
<head>
<title> </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>                                    ログイン操作をWeb認証に指示するための記述
 <td>user ID</td>
 <td>

<input type="text" name="uid" size="40" maxlength="32" autocomplete="OFF" />
                                                ユーザID指定のための記述
</td>
</tr><tr>
 <td>password</td>
 <td>

<input type="password" name="pwd" size="40" maxlength="32"
autocomplete="OFF" />
                                                パスワード指定のための記述
</td></tr>
</table>
<br />
<input type="submit" value="Login" />
                                        Web認証にログイン要求を行うための記述
</form>
<br /><br /><br /><br /><br />
</center>
<!-- ===== Footer ===== -->
<hr>
</body>
</html>
```

(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 9-11　ログイン画面（ブラウザ表示例）



9.2.2 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 9-4　ログアウト画面に必要な設定

記述内容	意味
<form name="Logout" method="post" action="/cgi-bin/Logout.cgi"></form>	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。
<input type="submit" value="Logout" />	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<form></form>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）　< img src="/image_file.gif" >

(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 9-12　ログアウト画面（logout.html）のソース例

```
<?xml version="1.0" encoding="utf-8"?>
<!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="en" lang="en">
<head>
<title> </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 />
</center>
<!-- ===== Footer ===== -->
<hr>
</body>
</html>
```

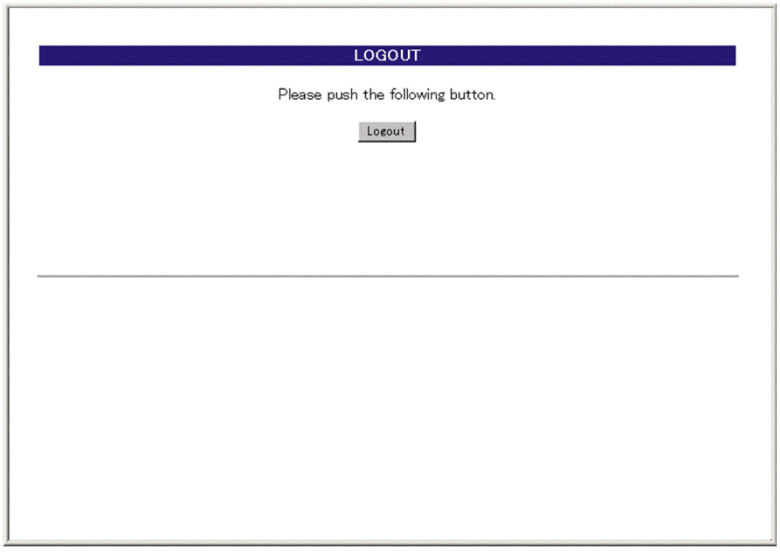
ログアウト操作をWeb認証に指示するための記述

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 9-13　ログアウト画面（ブラウザ表示例）



9.2.3 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 9-5　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”
”も含みます。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 9-14　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>システム管理者に問い合わせてください。
システムの設定に誤りがあります<BR>システム管理者に問い合わせてください。
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>システム管理者に問い合わせてください。
システム障害発生（critical）<BR>システム管理者に問い合わせてください。
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 9-15　ログイン失敗画面（ブラウザ表示例）

9.2.4 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 9-6　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	―	―	○	―	―	―

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
<!-- 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	―	―	―
<!-- Session_Code -->	なし	―	―	―	―	―	―

（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，「9.2.5　その他の画面サンプル」を参照してください。

9.2.5 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 9-16　ログイン成功画面のソース例（loginOK.html）

```
<?xml version="1.0" encoding="utf-8"?>
<!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="en" lang="en">
<head>
<title> </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）　＜img src="/image_file.gif" ＞

なお，ダイナミック VLAN モードでは，認証成功により該当の端末が所属する VLAN が切り替わるため，loginOK.html のサイズが大きい場合にログイン成功画面が最後まで表示されないことがあります。また，loginOK.html ファイルにほかのファイルを関連付けしたときに，関連付けしたファイルが正常に表示されないことがあります。

図 9-17　ログイン成功画面（ブラウザ表示例）

(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 9-18　ログアウト完了画面のソース例（logoutOK.html）

```
<?xml version="1.0" encoding="utf-8"?>
<!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="en" lang="en">
<head>
<title> </title>
</head>
<body oncontextmenu=¥"return false;¥">
<!-- ===== Body ===== -->
<center>
Logout success
<br /><br />
Logout Time --- <b><!-- Logout_Time --></b>
<br /><br /><br />
<form>
<input type="button" value="close" onClick="window.close()" />
</form>
<br /><br />
</center>
<!-- ===== Footer ===== -->
<hr>
</body>
</html>
```

ログアウト時刻表示タグ

注意

logoutOK.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）　< img src="/image_file.gif" >

図 9-19　ログアウト完了画面（ブラウザ表示例）

(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 9-20　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="utf-8"?>
<!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="en" lang="en">
<head>
<title> </title>
</head>
<body oncontextmenu=¥"return false;¥">
<!-- ===== Body ===== -->
<center>                                    エラーメッセージ表示タグ
<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>
```

注意

loginNG.html，logoutNG.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）　< img src="/image_file.gif" >

図 9-21　ログイン／ログアウト失敗画面（ブラウザ表示例）

9.3 SSL 証明書の準備

9.3.1 サーバ証明書と鍵を作成する環境

SSL 用サーバ証明書と鍵を作成するには，openssl が動く環境が必要です。openssl が動作する OS を次に示します。

- UNIX 系 OS
- Windows 系 OS（cygwin が動作必須）

openssl を実行して，サーバ証明書と鍵を作成します。openssl 1.0.2 以降のバージョンを使用してください。また，openssl の構築に関しては，オープンソースである openssl のドキュメントを参照してください。

9.3.2 サーバ証明書と鍵の作成

サーバ証明書と鍵の作成に当たって，openssl に入力する情報を次の表に示します。

表 9-7　openssl に入力する情報

名称	内容・意味
pass phrase for server.key	サーバ用パスワード
Country Name	国コード
State or Province Name	都道府県名
Locality Name	市町村名
Organization Name	団体名または会社名
Organizational Unit Name	部署名
Common Name	FQDN または本装置の IP アドレス
Email Address	管理者の電子メールアドレス
challenge password	－
optional company name	－

（凡例）－：入力不要

SSL 用サーバ証明書と鍵は，openssl が動作する環境で作成します。次に手順を示します。また，実行例では次に示すファイル名を使用します。

- 秘密鍵のファイル名：server.key
- 署名要求書のファイル名：server.pem
- 作成するサーバ証明書のファイル名：server.crt
- 生成する秘密鍵のファイル名：serverinstall.key

なお，openssl 動作環境のプロンプトを「unix#」とします。

(1)　乱数シードファイルを準備する

数百バイト程度のファイル（rand.dat）を準備します。内容およびコードは問いません。

(2)　SSL 通信で使用する鍵を作成する

鍵長を 2048 ビットとした鍵（server.key）を作成する例を次の図に示します。

図 9-22　鍵の作成

```
unix# openssl genrsa -out server.key -aes256 -rand rand.dat 2048
```

```
241 semi-random bytes loaded
Generating RSA private key, 2048 bit long modulus
.....................................................................+++
.............+++
e is 65537 (0x10001)
Enter pass phrase for server.key: *******                              <-1
Verifying - Enter pass phrase for server.key: *******                  <-2
```

1. サーバ用のパスワードを入力します。
2. サーバ用のパスワードを再入力します。

(3) 署名要求書を作成する

SHA256 を使用して，秘密鍵（server.key）から署名要求書（server.pem）を作成する例を次の図に示します。なお，この図で入力する情報は，操作を示すために使用したものです。実際には，CA 局が発行する CA 証明書，および中間 CA 証明書との照合に必要な情報を入力してください。

図 9-23 署名要求書の作成

```
unix# openssl req -new -sha256 -key server.key -out server.pem
Enter pass phrase for server.key: *******                              <-1
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:JP                                   <-2
State or Province Name (full name) [Some-State]:KANAGAWA               <-3

Locality Name (eg, city) []:KAWASAKI                                   <-4
Organization Name (eg, company) [Internet Widgits Pty Ltd]:AlaxalA     <-5
Organizational Unit Name (eg, section) []:AX                           <-6

Common Name (e.g. server FQDN or YOUR name) []:www.example.com         <-7
Email Address []:admin@example.com                                     <-8
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:                                               <-9
An optional company name []:                                           <-9
```

1. サーバ用のパスワードを入力します。
2. 国コードを入力します。
3. 都道府県名を入力します。
4. 地域を入力します。
5. 会社名を入力します。
6. 任意の名称を入力します。
7. FQDN または本装置の IP アドレスを入力します。
8. メールアドレスを入力します。

9.　何も入力しません。

(4)　サーバ証明書を作成する

-days オプションを使用して，有効期限を 365 日と設定したサーバ証明書（server.crt）を作成する例を次の図に示します。

図 9-24　サーバ証明書の作成

```
unix# openssl x509 -in server.pem -out server.crt -req -signkey server.key -days 365
Signature ok
subject=/C=JP/ST=KANAGAWA/L=KAWASAKI/O=AlaxalA/OU=AX/CN=www.example.com/emailAddress=admin@exam
ple.com
Getting Private key
Enter pass phrase for server.key: *******                              <-1
```

1.　サーバ用のパスワードを入力します。

(5)　装置にインストールするための秘密鍵を生成する

装置にインストールするための秘密鍵（serverinstall.key）を生成する例を次の図に示します。

図 9-25　秘密鍵の生成

```
unix# openssl rsa -in server.key -out serverinstall.key
Enter pass phrase for server.key: *******                              <-1
writing RSA key
```

1.　サーバ用のパスワードを入力します。

9.3.3 サーバ証明書と鍵の登録

運用コマンド set web-authentication ssl-crt で，サーバ証明書と秘密鍵を本装置に登録します。また，中間 CA 証明書がある場合，サーバ証明書および秘密鍵と同時に登録します。次に手順を示します。

(1)　サーバ証明書と鍵を本装置に転送する

MC を使用するか，運用コマンド sftp，scp などによって，作成したサーバ証明書と秘密鍵を本装置に転送します。また，中間 CA 証明書がある場合は，同様に本装置に転送します。

(2)　中間 CA 証明書を準備する

中間 CA 証明書がある場合は，登録する中間 CA 証明書のファイルを準備します。また，複数の中間 CA 証明書（次の実行例では二つのファイル root.crt と next.crt）がある場合は，ファイルをマージして一つのファイル（ca.crt）を作成します。

図 9-26　中間 CA 証明書の準備

```
# cp root.crt ca.crt
# cat next.crt >> ca.crt
#
```

(3)　サーバ証明書と鍵を本装置に登録する

装置管理者モードでログインして，カレントディレクトリにサーバ証明書（server.crt）と秘密鍵（serverinstall.key）を置きます。また，中間 CA 証明書（ca.crt）がある場合は，カレントディレクトリに中間 CA 証明書を置きます。

ファイルを置いた状態で，運用コマンド set web-authentication ssl-crt を実行して本装置に登録します。

図 9-27 サーバ証明書と鍵の登録

```
# set web-authentication ssl-crt
Set path to the key: serverinstall.key                          <-1
Set path to the certificate: server.crt                         <-2
Set path to the intermediate CA certificate: ca.crt             <-3
Would you wish to install SSL key and certificate? (y/n):y      <-4
Install complete.
Please restart web-authentication daemon or web-server daemon.
#
```

1. 秘密鍵のファイル名を指定します。
2. サーバ証明書のファイル名を指定します。
3. 中間 CA 証明書のファイル名を指定します。中間 CA 証明書がない場合は，［Enter］キーだけを入力します。
4. 入力した内容が正しければ，y を入力します。

なお，登録時には，サーバ証明書，秘密鍵，および中間 CA 証明書の内容や正当性のチェックをしません。そのため，正しい組み合わせのサーバ証明書，秘密鍵，および中間 CA 証明書を登録しなかった場合は，HTTPS を使用してのログイン操作やログアウト操作ができなくなります。このようなときは，登録した証明書と秘密鍵をいったん削除したあと，再度正しい組み合わせのサーバ証明書，秘密鍵，および中間 CA 証明書を登録してください。

(4) 登録を確認する

運用コマンド show web-authentication ssl-crt を実行して，サーバ証明書，秘密鍵，および中間 CA 証明書が登録されていることを確認します。

図 9-28 サーバ証明書と鍵の登録確認

```
# show web-authentication ssl-crt
Date 20XX/04/15 10:07:04 UTC
                              DATE
SSL key                :  20XX/03/30 14:05
SSL certificate        :  20XX/03/30 14:05
SSL intermediate cert:  20XX/03/30 14:05
```

(5) Web サーバを再起動する

運用コマンド restart web-authentication web-server を実行して，Web サーバを再起動します。

図 9-29 Web サーバの再起動

```
# restart web-authentication web-server
```

(6) Web サーバの起動を確認する

ps コマンドを使用して，Web サーバ（httpd）が起動していることを確認します。

図 9-30 Web サーバの起動確認

```
# ps -auwx |grep httpd
root       471  0.0  0.1   212    672 ??  S     6:19PM  0:00.52 /usr/local/sbin/httpd -DS_WA -
DSSL -DWA_SSL
operator 11070  0.0  0.1   164    556 00  S+    6:20PM  0:00.01 sh -c ps -auwx | grep httpd
operator 11421  0.0  0.0    32     36 00  R+    6:20PM  0:00.00 grep httpd
```

9.3.4 サーバ証明書と鍵の削除

運用コマンド clear web-authentication ssl-crt で，本装置に登録したサーバ証明書，秘密鍵，および中間 CA 証明書を削除します。次に手順を示します。

(1) サーバ証明書と鍵を削除する

装置管理者モードでログインして，運用コマンド clear web-authentication ssl-crt を実行して登録したサーバ証明書，秘密鍵，および中間 CA 証明書を削除します。

図 9-31　サーバ証明書と鍵の削除

```
# clear web-authentication ssl-crt
Would you wish to clear SSL key and certificate? (y/n):y                <-1
Please restart web-authentication daemon or web-server daemon.
#
```

1.　y を入力すると，登録したサーバ証明書，秘密鍵，および中間 CA 証明書を削除します。

(2) 削除を確認する

運用コマンド show web-authentication ssl-crt を実行して，サーバ証明書，秘密鍵，および中間 CA 証明書が削除されていることを確認します。

図 9-32　サーバ証明書と鍵の削除確認

```
# show web-authentication ssl-crt
Date 20XX/04/15 10:07:04 UTC
                              DATE
SSL key                :  default now
SSL certificate        :  default now
SSL intermediate cert:  -
```

(3) Web サーバを再起動する

運用コマンド restart web-authentication web-server を実行して，Web サーバを再起動します。

図 9-33　Web サーバの再起動

```
# restart web-authentication web-server
```

(4) Web サーバの起動を確認する

ps コマンドを使用して，Web サーバ（httpd）が起動していることを確認します。

図 9-34　Web サーバの起動確認

```
# ps -auwx | grep httpd
root       471  0.0  0.1   212    672 ??  S     6:19PM  0:00.52 /usr/local/sbin/httpd -DS_WA -
DSSL -DWA_SSL
operator 11070  0.0  0.1   164    556 00  S+    6:20PM  0:00.01 sh -c ps -auwx | grep httpd
operator 11421  0.0  0.0    32     36 00  R+    6:20PM  0:00.00 grep httpd
```

10 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。

10.1 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 認証よりも先に DHCP snooping の対象となるため，DHCP snooping で許可されたパケットだけが MAC 認証の対象となります。

(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。

10.2 システム構成例

ここでは，固定 VLAN モードおよびダイナミック VLAN 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。

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。

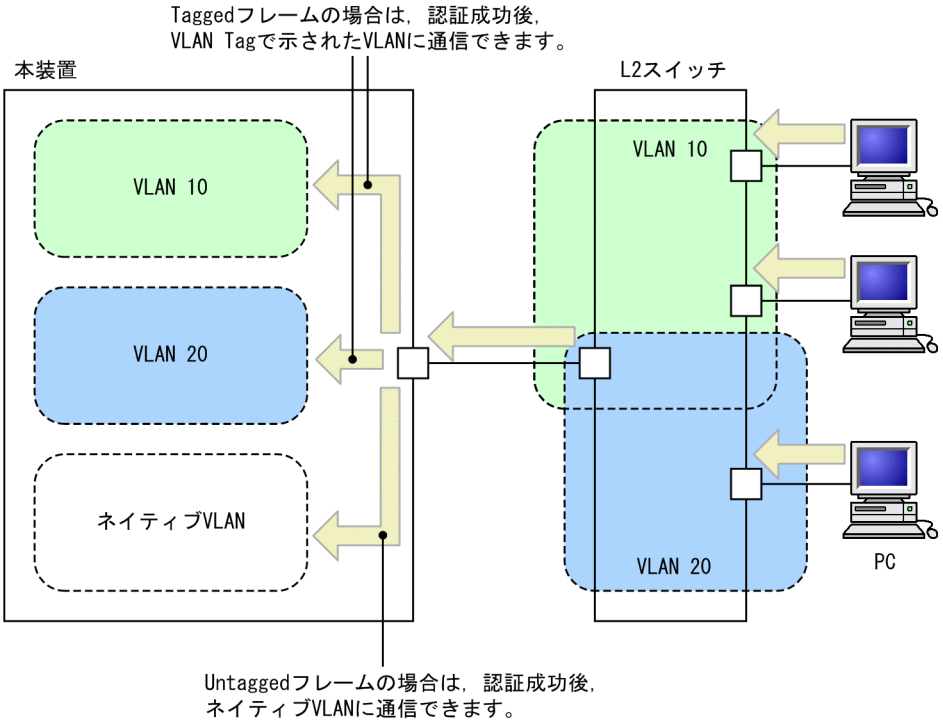
本装置では，認証ポートとして次のポートを設定できます。

- アクセスポート
- トランクポート

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 10-1　Tagged フレームおよび Untagged フレームの扱い

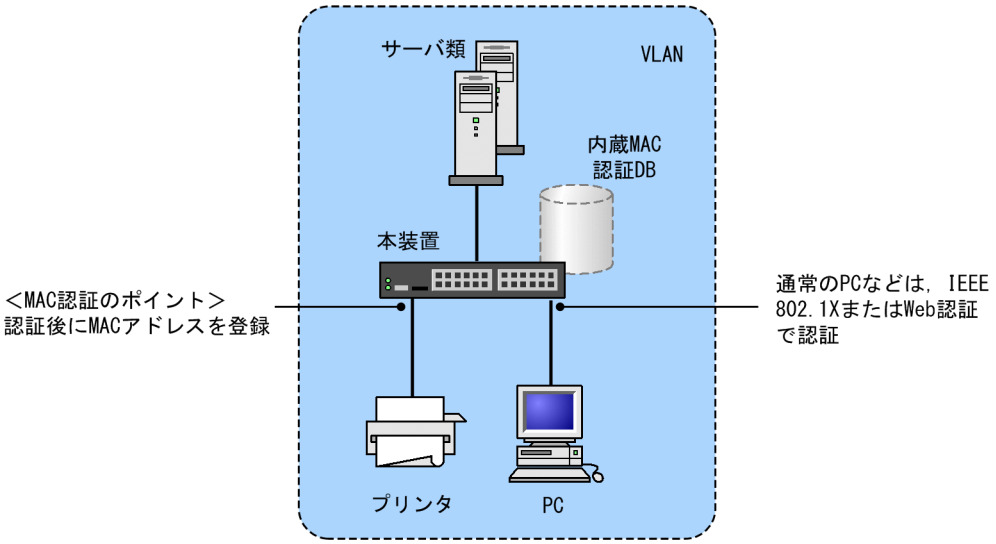


また，認証前 VLAN 内で通信したい場合は，認証専用 IPv4 アクセスリストで通信に必要なフィルタ条件を設定する必要があります。

(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通信を許可する方式です。

図 10-2　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。

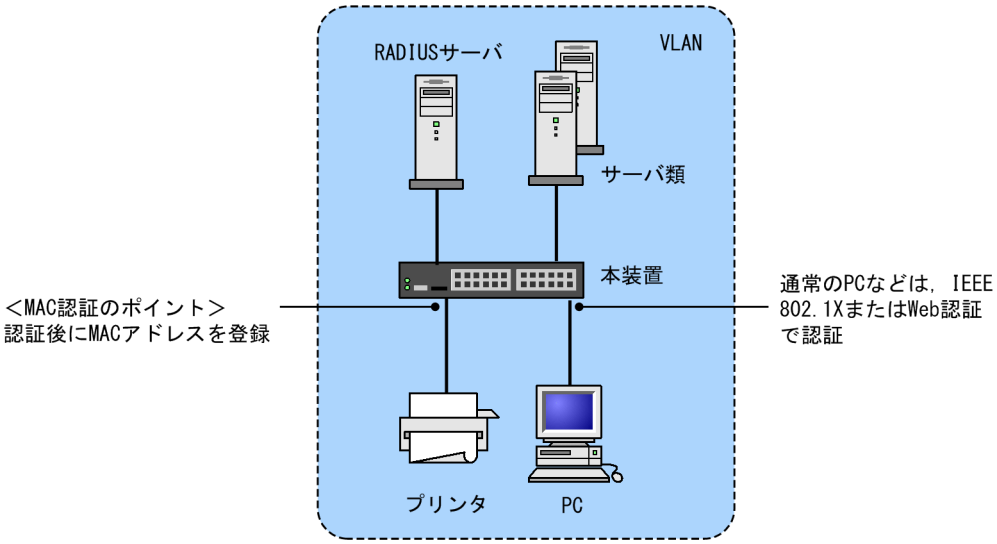
表 10-1　固定 VLAN モードのローカル認証方式の VLAN ID 照合

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 10-3　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 10-2　固定 VLAN モードの RADIUS 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	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，コンフィグ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，認証を行う MAC アドレスをパスワードとして用います。

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。

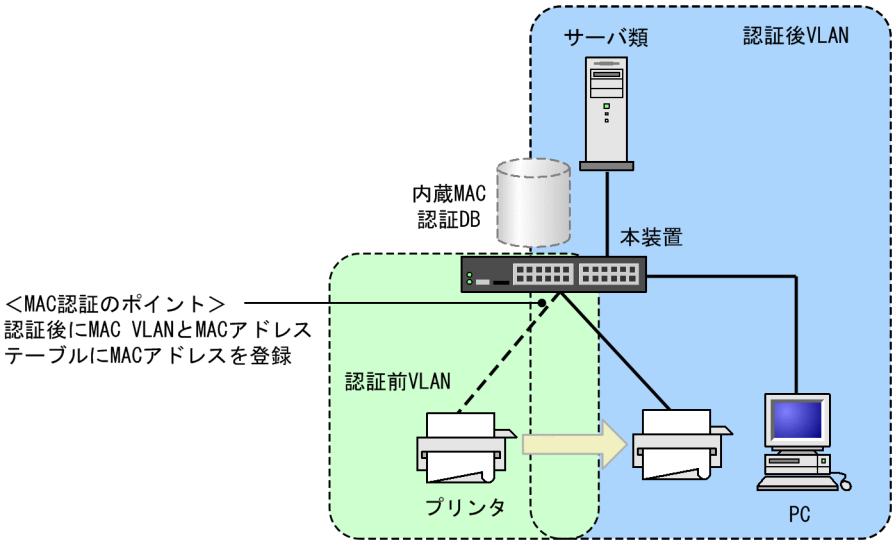
- MAC VLAN が設定されている MAC ポートを認証ポートとして設定

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 10-4　ダイナミック VLAN モードのローカル認証方式の構成

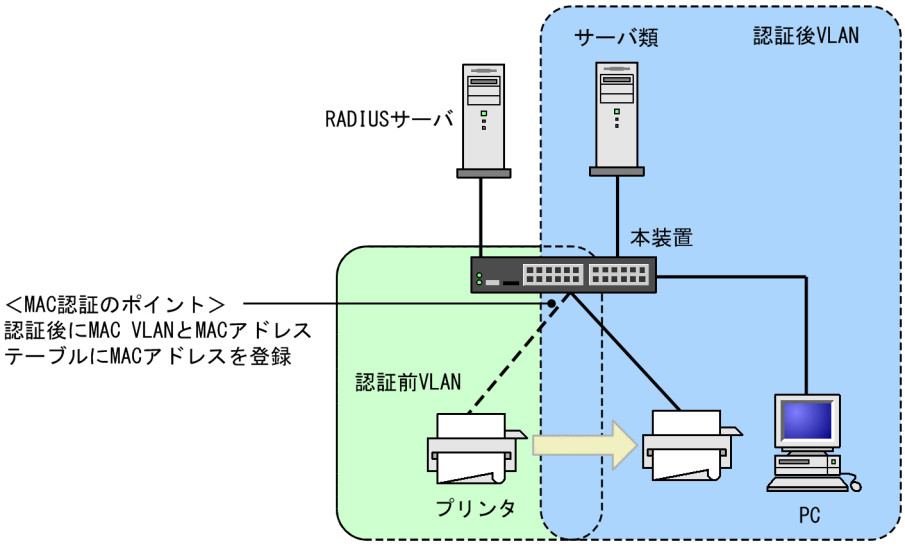


(2)　RADIUS 認証方式

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 10-5　ダイナミック VLAN モードの RADIUS 認証方式の構成



10.2.3 MAC ポートに dot1q 設定時の動作

MAC ポートに dot1q が設定された場合の動作については，「5.3　レイヤ 2 認証共通の機能」を参照してください。

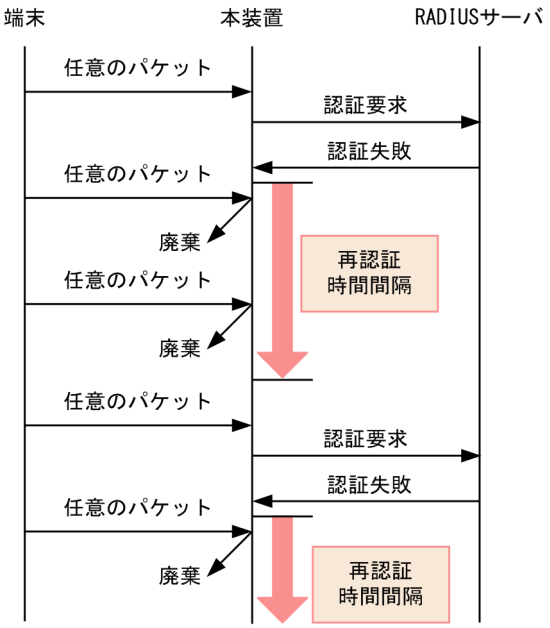
10.3 認証機能

10.3.1 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。複数の端末で認証失敗処理が行われた場合，同時に再認証時間間隔を監視する端末数は 1024 台です。

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 秒以内に改めて認証処理を行います。

図 10-6　認証失敗後の動作シーケンス



10.3.2 定期的再認証要求

認証成功後，RADIUS サーバの設定情報を反映させるために，認証成功から一定周期で RADIUS サーバへ再認証要求処理を実施します。

定期的再認証要求の結果，認証成功であれば MAC 認証状態は継続されますが，認証失敗の場合は強制的に該当端末の MAC 認証状態を解除します。

再認証を行う周期はコンフィグレーションコマンド mac-authentication timeout reauth-period で設定できます。

なお，端末が認証状態のとき，RADIUS サーバの設定情報で該当端末の認証後 VLAN の値だけを変更する場合は，運用コマンド clear mac-authentication auth-state で端末の認証状態を解除してください。

10.3.3 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 10-3　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	○	○

認証解除方式	固定 VLAN モード	ダイナミック VLAN モード
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	○	○
認証済み端末の無通信監視による認証解除	○	○
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	○	○
動的に登録された VLAN の削除による認証解除	－	○
認証対象外ポートへの移動による認証解除	○	○
定期的再認証要求で認証失敗による認証解除	○	○

（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) 認証済み端末の無通信監視による認証解除

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することで，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，端末からのアクセスがなくなってから約 60 分間（60 秒周期で監視），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。なお，この時間はコンフィグレーションコマンド mac-authentication auto-logout で 1 秒単位の時間を設定できますが，設定した時間を満たす回数を 60 秒周期で監視する動作となります。

スタック構成では，無通信監視の時間が最大 3 分間（180 秒）追加されます。

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

なお，ダイナミック VLAN モードで VLAN を suspend して認証解除する場合は，認証後 VLAN を suspend する必要があります。

(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

コンフィグレーションコマンドで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。

(9)　動的に登録された VLAN の削除による認証解除

動的に VLAN が作成された認証ポートにコンフィグレーションコマンド switchport mac vlan が設定された場合，該当ポートに動的に作成された VLAN ID は削除されて，VLAN に所属していた端末の認証を解除します。

(10) 認証対象外ポートへの移動による認証解除

コンフィグレーションコマンド authentication auto-logout strayer が設定されているとき，認証された MAC アドレスを送信元 MAC アドレスとするパケットを認証対象外ポートで受信した場合，認証を解除します。

(11) 定期的再認証で認証失敗による認証解除

RADIUS サーバへ認証済み端末の定期的再認証要求をして，再認証に失敗した場合は，該当端末の認証を解除します。

10.3.4 認証数制限

装置単位およびポート単位に認証数の制限が設定できます。詳細は，「5.3　レイヤ 2 認証共通の機能」を参照してください。

10.3.5 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，「5.3　レイヤ 2 認証共通の機能」を参照してください。

10.3.6 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 10-4　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

注※

記録される内容については，「表 10-7　RADIUS Accounting で使用する属性名」の NAS-Identifier の項目を参照してください。

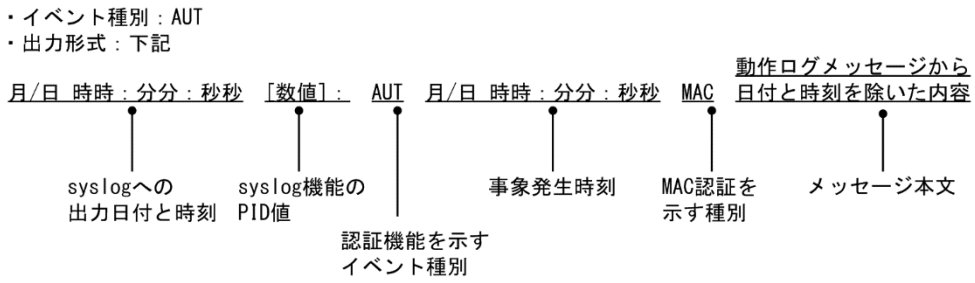
(3) RADIUS サーバへの認証情報記録

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 認証の動作ログメッセージを syslog サーバに出力（または E-mail 送信）できます。また，動作ログメッセージは MAC 認証のアカウントログを含みます。メッセージ出力の際，MAC 認証を示す種別を付加するため，該当部分の出力形式を次の図に示します（E-mail 送信の場合，syslog 機能の PID 値は出力しません）。

図 10-7　syslog サーバ出力形式



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（E-mail 送信の場合は，logging email-event-kind aut）によって，出力の開始および停止ができます。

10.4 内蔵 MAC 認証 DB および RADIUS サーバの準備

10.4.1 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。

10.4.2 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。

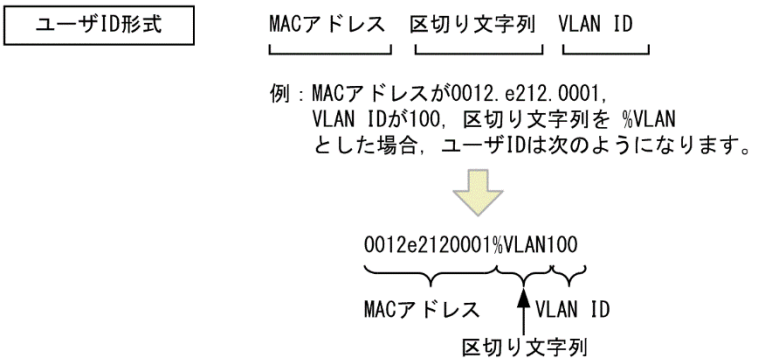
(1)　ユーザ ID の登録

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 10-8　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
   - コンフィグレーションコマンド name で設定した VLAN 名称を設定

(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 10-5　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 10-8　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，またはコンフィグ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。
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，指定されていなければ 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。
NAS-Port	5	認証している認証単位の IfIndex を格納します。
Service-Type	6	Framed(2)を設定します。

属性名	Type 値	説明
Called-Station-Id	30	ブリッジやアクセスポイントの MAC アドレスです。本装置の MAC アドレス（ASCII，"-"区切り）を格納します。
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。
Connect-Info	77	コネクションの特徴を示す文字列を格納します。 ポート（"CONNECT Ethernet"） チャネルグループ（"CONNECT Port-Channel"）
NAS-Port-Id	87	認証ポートを識別するための文字列を格納します。 ポート（"Port x/0/y"） チャネルグループ（"ChGr x"） （x，y には数字が入る）
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，指定されていなければ 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。

表 10-6　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 を表しているので，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。 また，コンフィグレーションコマンド name で設定された VLAN 名称が指定された場合は，VLAN 名称に対応する VLAN ID を使用します。 固定 VLAN モード時は使用しません。

表 10-7　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 10-8　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。
NAS-Port	5	認証している認証単位の IfIndex 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-e2-01-23-45
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。ただし，0 秒の場合は格納されません。
Acct-Input-Octets	42	Accounting 情報（受信オクテット数）を格納します（(0)固定）。
Acct-Output-Octets	43	Accounting 情報（送信オクテット数）を格納します（(0)固定）。
Acct-Session-Id	44	Accounting 情報を識別する ID（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。
Acct-Input-Packets	47	Accounting 情報（受信パケット数）を格納します（(0)固定）。
Acct-Output-Packets	48	Accounting 情報（送信パケット数）を格納します（(0)固定）。
Acct-Terminate-Cause	49	Accounting 情報（セッション終了要因）を格納します。 詳細は，「表 10-8　Acct-Terminate-Cause での切断要因」を参照。
NAS-Port-Type	61	Virtual(5)を設定します。
NAS-Port-Id	87	認証するポートを識別するための文字列を格納します。 ポート（"Port x/0/y"） チャネルグループ（"ChGr x"） （x，y には数字が入る）
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，これ以外は，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。

表 10-8　Acct-Terminate-Cause での切断要因

切断要因	値	解説
User Request	1	認証端末の動作により切断した。 ・認証端末のポート移動を検出した場合
Idle Timeout	4	認証端末の通信がなくなったため切断した。 ・無通信監視時間が超過した場合
Session Timeout	5	最大接続時間の超過により切断した。
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 ・運用コマンド clear mac-authentication auth-state を実行した場合
NAS Request	10	マルチステップ認証のユーザ認証成功により切断した。
Service Unavailable	15	認証端末のポート移動を検知したが，移動先のポートで最大認証端末数を超過したために切断した。
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 ・VLAN を削除または Disable にした場合 ・コンフィグレーションコマンド switchport mode を変更した場合

10.5 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，「5.2　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。

11 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。

11.1 コマンドガイド

11.1.1 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 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 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 認証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 dot1q-vlan force-authorized	MAC ポートに switchport mac dot1q vlan 設定がある場合に，Tagged フレームを認証除外に設定します。
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 id-format	RADIUS 認証方式を使用している場合に，RADIUS サーバへ認証要求するときの MAC アドレス形式を設定します。
mac-authentication logging enable	MAC 認証の動作ログメッセージを，syslog サーバ宛てまたはメールアドレス宛て（E-Mail 使用）に送信します。
mac-authentication login-failed-logging disable	MAC 認証で認証失敗時の認証ログの出力を抑止します。
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 認証専用に 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 timeout reauth-period	RADIUS サーバへ定期的再認証要求をする周期を設定します。
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。

MAC 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
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。

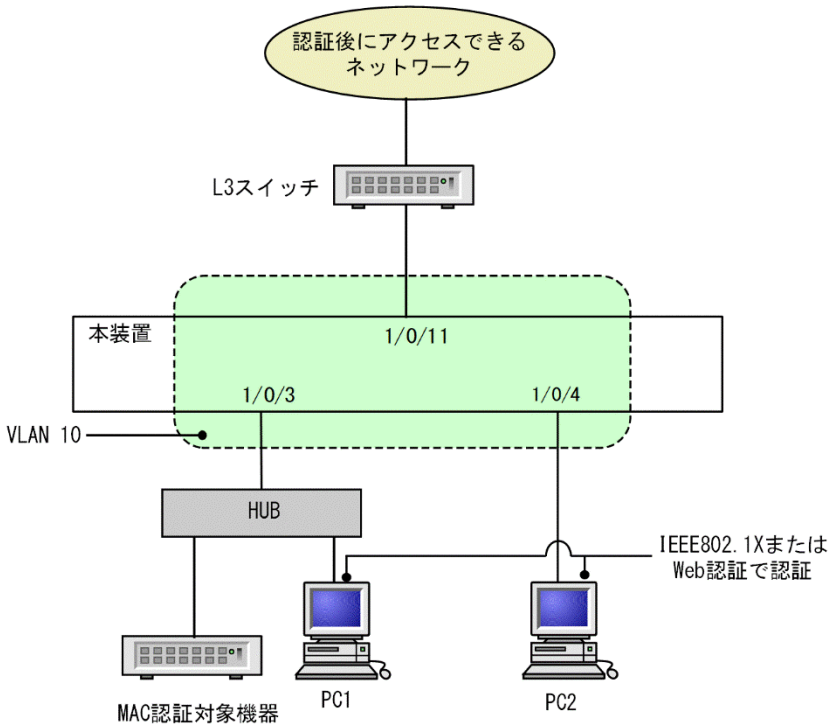
コマンド名	説明
show mac-authentication statistics	統計情報を表示します。
clear mac-authentication auth-state mac-address	認証済み端末を強制的に認証解除します。
clear mac-authentication logging	動作ログ情報をクリアします。
clear mac-authentication statistics	統計情報をクリアします。
set mac-authentication mac-address	内蔵 MAC 認証 DB へ MAC アドレスを登録します。
remove mac-authentication	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。
clear mac-authentication dead-interval-timer	dead interval 機能による 2 台目以降の RADIUS サーバへのアクセスから，1 台目の RADIUS サーバへのアクセスに戻します。
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。

11.1.2 固定 VLAN モードの設定

(1)　ローカル認証方式の基本的な設定

固定 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 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］

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 1/0/3
   (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 認証のコンフィグレーションコマンドを設定して MAC 認証を有効にします。

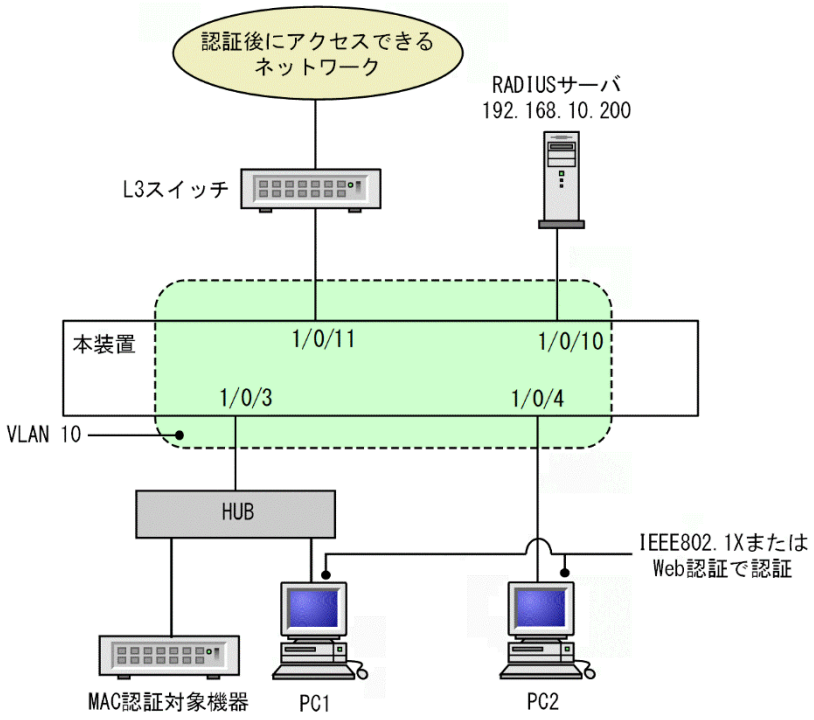
［コマンドによる設定］

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

固定 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 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］

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 1/0/3
   (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 認証のコンフィグ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。

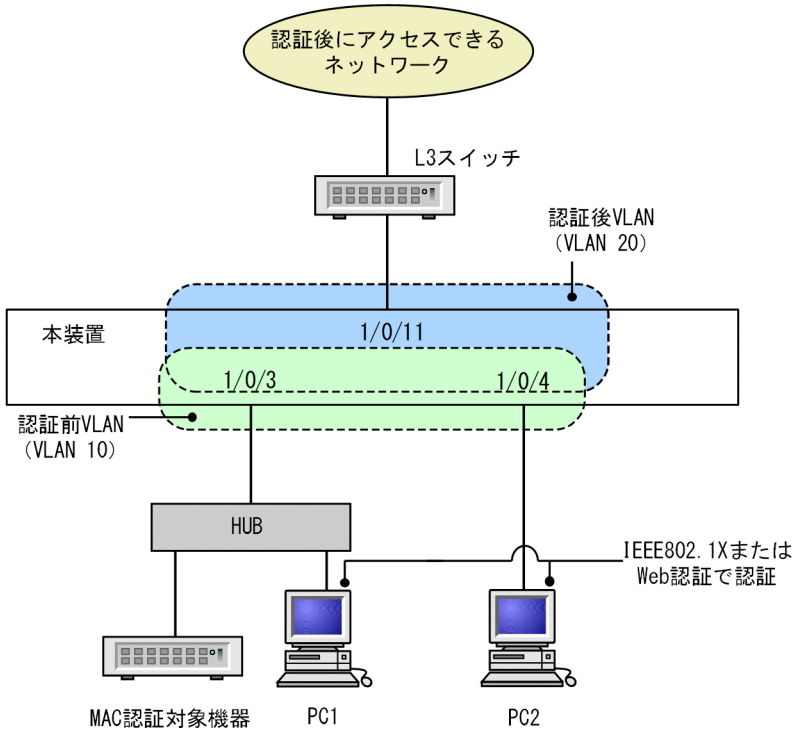
2.
```
(config)# mac-authentication system-auth-control
```
MAC 認証を起動します。

11.1.3 ダイナミック VLAN モードの設定

(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，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 11-3　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 1/0/3-4
```

```
(config-if-range)# switchport mode mac-vlan
(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 認証のコンフィグレーションコマンドを設定して MAC 認証を有効にします。

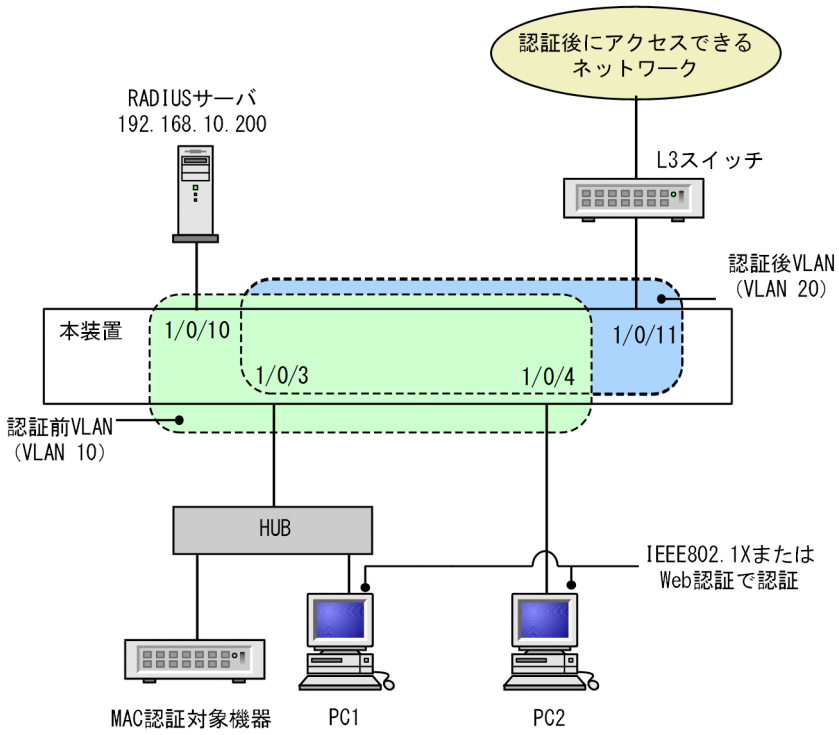
［コマンドによる設定］

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 11-4　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 1/0/3-4
(config-if-range)# switchport mode mac-vlan
(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 認証のコンフィグ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。

11.1.4 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 サーバにアカウンティング集計をするように設定します。

(5) 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。

(6) 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。

(7) 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。

(8) 定期的再認証要求の周期を設定

［設定のポイント］

認証済みの端末について，RADIUS サーバへ定期的再認証要求をする周期を設定します。

［コマンドによる設定］

1. (config)# mac-authentication timeout reauth-period 7200
   定期的再認証要求をする周期を 7200 秒に設定します。なお，定期的再認証をしない場合は，mac-authentication timeout reauth-period 0 を設定してください。

(9) 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。

(10) 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。

11.1.5 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 1/0/4
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   (config-if)# mac-authentication port
   (config-if)# exit
   (config)# interface gigabitethernet 1/0/10
   (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 1/0/4 には認証ポートを設定します。また，ポート 1/0/10 には認証しないで通信を許可する設定をします。

(2) 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 10
   (config-vlan)# state active
   (config-vlan)# exit
   (config)# interface gigabitethernet 1/0/4
   (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 1/0/10
   (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 1/0/4 には認証ポートを設定し

ます。また，ポート 1/0/10 には認証しないで通信を許可する設定をします。

(3) dot1q 設定 MAC ポートの認証除外設定

［設定のポイント］

dot1q 設定がされた MAC ポートの Tagged フレームを認証除外に設定します。

［コマンドによる設定］

1.
```
(config)# interface gigabitethernet 1/0/20
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 20
(config-if)# switchport mac native vlan 10
(config-if)# switchport mac dot1q vlan 100
(config-if)# mac-authentication port
(config-if)# mac-authentication dot1q-vlan force-authorized
(config-if)# exit
```
MAC 認証の認証対象ポート 1/0/20 に受信した，VLAN ID 100 を持つ Tagged フレームを認証除外にする設定をします。

11.1.6 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
```

11.1.7 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
#
```

11.1.8 dead interval 機能による RADIUS サーバアクセスを 1 台目の RADIUS サーバに戻す

1 台目の RADIUS サーバが無応答になり，dead interval 機能によって，2 台目以降の RADIUS サーバへのアクセスに切り替わった場合，コンフィグレーションコマンド authentication radius-server dead-interval で設定された時間を待たないで最初の RADIUS サーバへのアクセスに戻すには，clear mac-authentication dead-interval-timer コマンドを実行します。

図 11-5　1 台目の RADIUS サーバへの切り替え

```
# clear mac-authentication dead-interval-timer
#
```

12 マルチステップ認証

本装置では，端末認証とユーザ認証を 2 段階で実施するマルチステップ認証をサポートしています。この章では，マルチステップ認証について解説します。

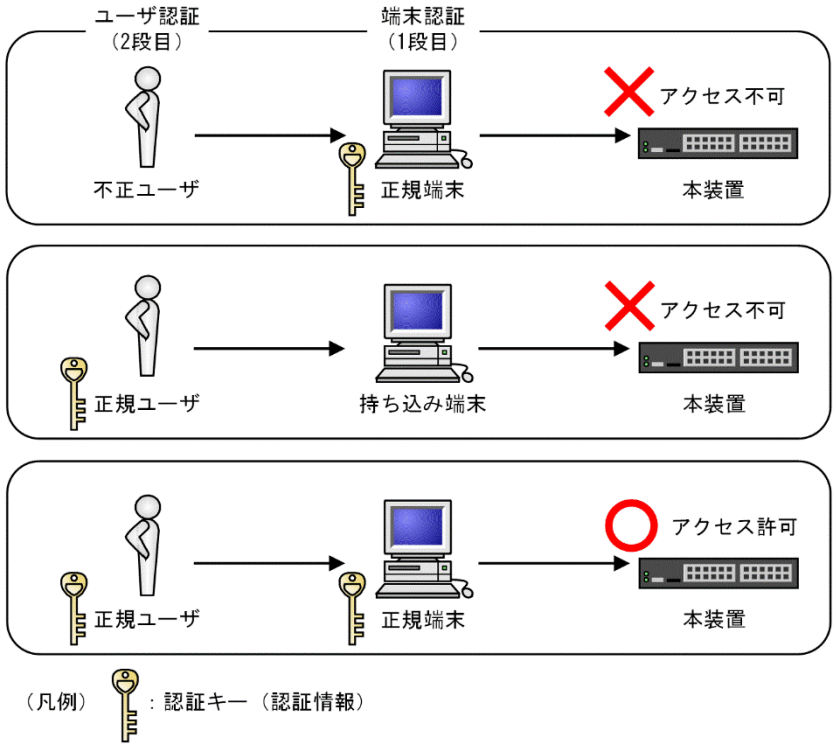
12.1 解説

12.1.1 概要

マルチステップ認証は，レイヤ 2 認証を組み合わせて端末認証（1 段目の認証）とユーザ認証（2 段目の認証）の 2 段階認証をすることで，正規端末を使用する正規ユーザだけにアクセスを許可します。これによって，不正ユーザや外部からの不正な持ち込み端末によるアクセスを排除できます。

マルチステップ認証の概要を次の図に示します。

図 12-1　マルチステップ認証の概要



12.1.2 サポート機能

(1)　マルチステップ認証が動作するレイヤ 2 認証の組み合わせと認証モード

IEEE802.1X，Web 認証，MAC 認証のうち 2 つを組み合わせて使用します。レイヤ 2 認証の組み合わせと認証モードについては，「5.1.1　レイヤ 2 認証種別」を参照してください。

(2)　マルチステップ認証のオプション

マルチステップ認証には，オプション設定なしの基本マルチステップ認証，およびオプション設定があり，コンフィグレーションコマンド authentication multi-step で設定します。マルチステップ認証のオプションについて次の表に示します。

表 12-1　マルチステップ認証のオプション

端末認証	ユーザ認証	オプション種別 （コンフィグレーション※）	動作概要
MAC 認証	IEEE802.1X ま	基本マルチステップ認証	端末認証成功時だけ，ユーザ認

端末認証	ユーザ認証	オプション種別（コンフィグレーション※）	動作概要
	たは Web 認証	（パラメータなし）	証ができます。
		ユーザ認証許可オプション（permissive パラメータ）	端末認証に失敗しても，ユーザ認証ができます。
IEEE802.1X または MAC 認証	Web 認証	端末認証 dot1x オプション（dot1x パラメータ）	端末認証成功時だけ，ユーザ認証ができます。

注※

ポート単位に指定できます。

(3) 認証方式

マルチステップ認証では，RADIUS 認証方式だけをサポートしています。端末認証では，RADIUS サーバから Access-Accept 受信時に，RADIUS 属性 Filter-Id または Tunnel-Private-Group-ID の文字列で認証動作を決定します。マルチステップ認証で使用する属性名に設定するテキスト文字列と対応する認証動作を次の表に示します。

表 12-2　RADIUS サーバで使用する属性名

属性名（Type 値）	RADIUS サーバの種類	文字列	認証動作
Filter-Id（11）	端末認証用 RADIUS サーバ	@@1X-Auth@@ または/1X-Auth	IEEE802.1X でユーザ認証をします。
		@@Web-Auth@@ または/Web-Auth	Web 認証でユーザ認証をします。
		@@MultiStep@@ または/MultiStep	Web 認証または IEEE802.1X でユーザ認証をします。
		/Class=xx（xx は 0～63 までの数字）	端末認証だけ（シングル認証）で認証成功とします。同時に，クラス情報を設定します。
		空白（Filter-Id 未設定）またはその他の文字列※1	端末認証だけ（シングル認証）で認証成功とします。クラス情報は設定しません。
	ユーザ認証用 RADIUS サーバ	/Class=xx（xx は 0～63 までの数字）	ユーザ認証（マルチステップ認証）で認証成功とします。同時に，クラス情報を設定します。
			端末認証が失敗した端末でも，ユーザ認証（シングル認証）を許可します。同時にユーザ認証が成功した端末に，クラス情報を設定します。※2
		/MAC-Auth/Class=xx（xx は 0～63 までの数字）	端末認証が失敗した端末では，ユーザ認証を許可しません。同時にユーザ認証（マルチステップ認証）が成功した端末に，クラス情報を設定します。※2
		@@MAC-Auth@@ または/MAC-Auth	端末認証が失敗した端末に，ユーザ認証を許可しません。また，ユーザ認証（マルチステップ認証）が成功した端末に，クラス情報は

属性名（Type値）	RADIUS サーバの種類	文字列	認証動作
			設定しません。※2
		空白（Filter-Id 未設定）またはその他の文字列※1	端末認証が失敗した端末でも，ユーザ認証（シングル認証）を許可します。また，ユーザ認証が成功した端末に，クラス情報は設定しません。※2
Tunnel-Private-Group-ID（81）	端末認証用 RADIUS サーバ	VLAN を識別する文字列※3	ダイナミック VLAN モードで使用します。端末認証に成功した端末が所属する VLAN を指定します。
	ユーザ認証用 RADIUS サーバ	VLAN を識別する文字列※3	ダイナミック VLAN モードで使用します。ユーザ認証に成功した端末が所属する VLAN を指定します。

注※1

その他の文字列を使用する場合は，マルチステップ認証およびダイナミック ACL/QoS のクラス情報で使用する文字列（「@@1X-Auth@@」など）は含めないでください。本装置がその他の文字列として認識しません。

注※2

ユーザ認証許可オプションを設定したときに該当します。

注※3

文字列に指定する内容は，IEEE802.1X，Web 認証，および MAC 認証の解説にある，認証で使用する属性名（Tunnel-Private-Group-ID）を参照してください。

12.1.3 認証動作

(1) 基本マルチステップ認証ポートの動作

端末認証では，端末認証成功時に RADIUS 属性 Filter-Id の文字列に従ってユーザ認証をするか，またはシングル認証で認証成功となります。ユーザ認証では，RADIUS 属性 Filter-Id の値に関係なく，ユーザ認証によって認証成功となります。

(2) ユーザ認証許可オプションポートの認証動作

ユーザ認証許可オプションポートでは，大きく二つのケースで認証成功となります。

- 一つ目のケースは，端末認証とユーザ認証を経て認証成功とするケースです。このとき，端末認証とユーザ認証の動作は基本マルチステップ認証と同じです。なお，ユーザ認証許可オプションポートでマルチステップ認証を必須とする場合は，ユーザ認証の RADIUS 属性 Filter-Id の値を@@MAC-Auth@@としてください。これによって，端末認証に失敗したときはユーザ認証を許可しません。
- 二つ目のケースは，端末認証が失敗しても，ユーザ認証を許可するケースです。なお，ユーザ認証の RADIUS 属性 Filter-Id の設定は不要です。このときのユーザ認証は，端末認証の失敗状態（保留エントリ）が存在する時間（MAC 認証失敗時の再認証時間間隔）の間だけ実施します。MAC 認証失敗時の再認証時間間隔は，コンフィグレーションコマンド mac-authentication auth-interval-timer で設定します。

(3) 端末認証 dot1x オプションポートの認証動作

端末認証では，端末認証成功時に RADIUS 属性 Filter-Id の文字列に従ってユーザ認証をするか，またはシングル認証で認証成功となりますが，端末認証に MAC 認証と IEEE802.1X を使用できます。ユーザ認証では，RADIUS 属性 Filter-Id の値に関係なく，ユーザ認証によって認証成功となります。

なお，端末認証に IEEE802.1X を使用する場合は，端末認証に使用する RADIUS サーバに該当端末を MAC 認証の対象として登録しないように，運用環境で対応する必要があります。

12.1.4 強制認証有効時の扱い

強制認証有効時に RADIUS サーバからの応答がないときは，その時点で認証成功となります。例えば，MAC 認証で端末認証をする場合に RADIUS サーバからの応答がないときは，シングル認証で認証成功となります。なお，強制認証が動作する認証モードについては，「5.3.3　強制認証」を参照してください。

12.1.5 認証端末の管理と認証解除

認証端末の管理は次のとおりです。

(1) マルチステップ認証端末の管理

マルチステップ認証端末の管理は，最終認証した機能で管理します。端末認証で認証許可となった端末がユーザ認証で許可されたときは，ユーザ認証の管理下となります。マルチステップ認証ポートでもシングル認証で認証完了したときは，該当するレイヤ 2 認証で端末を管理します。

(2) マルチステップ認証端末の認証解除

マルチステップ認証端末の認証解除は，ユーザ認証に使用されたレイヤ 2 認証の解除条件に従います。端末認証 dot1x オプションポートで EAPOL-Start フレームを受信した際は，端末認証が IEEE802.1X，MAC 認証どちらの場合でも，ユーザ認証（Web 認証）済の端末を認証解除します。ただし，該当ポートで IEEE802.1X のコンフィグレーションが設定されていない場合は，認証解除しません。なお，マルチステップ認証ポートのときにシングル認証で認証完了したときは，該当するレイヤ 2 認証の解除条件に従って認証解除します。

(3) マルチステップ認証端末の無通信監視

マルチステップ認証ポートでは，認証状態に応じて端末の無通信監視をします。端末の認証状態と無通信監視の方法の対応を次の表に示します。

表 12-3　端末の認証状態と無通信監視の方法の対応

端末の状態	認証状態	MAC 認証	IEEE802.1X	Web 認証
認証完了	マルチステップ認証完了（ユーザ認証完了）	－	認証済み端末の無通信監視	認証済み端末の無通信監視※1
	シングル認証完了	認証済み端末の無通信監視	認証済み端末の無通信監視	認証済み端末の無通信監視※1
保留（認証途中）	端末認証成功	認証済み端末の無通信監視※2	認証済み端末の無通信監視※2	－
認証失敗	認証失敗	MAC 認証失敗後に次の認証が実施されるまでの時間を監視※3	非認証状態保持時間を監視※4	即エントリ消去

（凡例）－：対象外

注※1

ダイナミック VLAN モードの場合です。

注※2

端末認証が成功し，ユーザ認証の要求を待っている状態です。この状態の該当端末の MAC アドレスは，ダイナミックエントリとして MAC アドレステーブルで管理します。ダイナミックエントリの無

通信監視時間は，各認証の無通信監視時間に MAC アドレスのエージングタイムアウトの時間が加算されます。

注※3

コンフィグレーションコマンド mac-authentication auth-interval-timer の設定値です。

注※4

コンフィグレーションコマンド dot1x timeout quiet-period の設定値です。

12.1.6 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ついては，「5.3　レイヤ 2 認証共通の機能」を参照してください。

12.1.7 認証状態およびアカウントログの表示

マルチステップ認証の認証状態，およびアカウントログは次の方法で表示します。

- マルチステップ認証の認証状態
  運用コマンド show authentication multi-step で，マルチステップ認証の認証経過を MAC アドレス単位で表示します。
- アカウントログ
  各認証の運用コマンドで，アカウントログを表示します。
  IEEE802.1X
  　show dot1x logging
  Web 認証
  　show web-authentication logging
  MAC 認証
  　show mac-authentication logging

12.1.8 マルチステップ認証使用時の注意事項

(1)　RADIUS 属性の Filter-Id の設定について

ユーザ認証用 RADIUS サーバの Filter-Id の設定では，次の点に注意してください。

Filter-Id 属性は，IEEE802.1X の認証端末の疎通制限でも使用します（詳細は「6.1　IEEE802.1X の概要」の「表 6-4　認証で使用する属性名（その 3　Access-Accept）」，および「6.2.9　認証端末の疎通制限」を参照してください）。IEEE802.1X で使用する RADIUS サーバで，マルチステップ認証で使用するテキスト文字列以外を Filter-Id 属性に設定した場合は，認証端末の疎通制限が動作します。

(2)　マルチステップ認証の認証数制限について

コンフィグレーションコマンド authentication max-user で設定した認証数制限は，ユーザ認証の認証数に対して適用します。

(3)　マルチステップ認証が有効な状態でマルチステップ認証の設定を変更または削除する場合の注意

マルチステップ認証が有効なポートで，コンフィグレーションコマンド authentication multi-step で dot1x を設定している状態で，authentication multi-step コマンドの設定を変更または削除する場合，該当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，運用コマンド clear dot1x auth-state，clear web-authentication auth-state，または clear mac-authentication auth-state で端末の認証状態を解除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コマンドを実行してください。その後，該当

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。

なお，認証端末が接続されている状態で authentication multi-step コマンドの設定を変更または削除した場合は，(4)の手順に従って，使用しているすべてのレイヤ 2 認証の認証プログラムと L2MAC 管理プログラムを再起動してください。

(4)　マルチステップ認証が有効な状態で認証プログラムを再起動する場合の注意

コンフィグレーションコマンド authentication multi-step が設定されているインタフェースが存在するときに認証プログラムを再起動する場合は，以下の順序で認証プログラムを再起動してください。なお，使用していない認証プログラムの再起動は不要ですが，L2MAC 管理プログラムは必ず再起動してください。

1. Web 認証プログラムを再起動（運用コマンド restart web-authentication を実行）
2. IEEE802.1X プログラムを再起動（運用コマンド restart dot1x を実行）
3. MAC 認証プログラムを再起動（運用コマンド restart mac-authentication を実行）
4. L2MAC 管理プログラムを再起動（運用コマンド restart vlan mac-manager を実行）

12.2 コマンドガイド

12.2.1 コマンド一覧

マルチステップ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 12-4　コンフィグレーションコマンド一覧

コマンド名	説明
authentication multi-step	ポートにマルチステップ認証を設定します。

マルチステップ認証の運用コマンド一覧を次の表に示します。

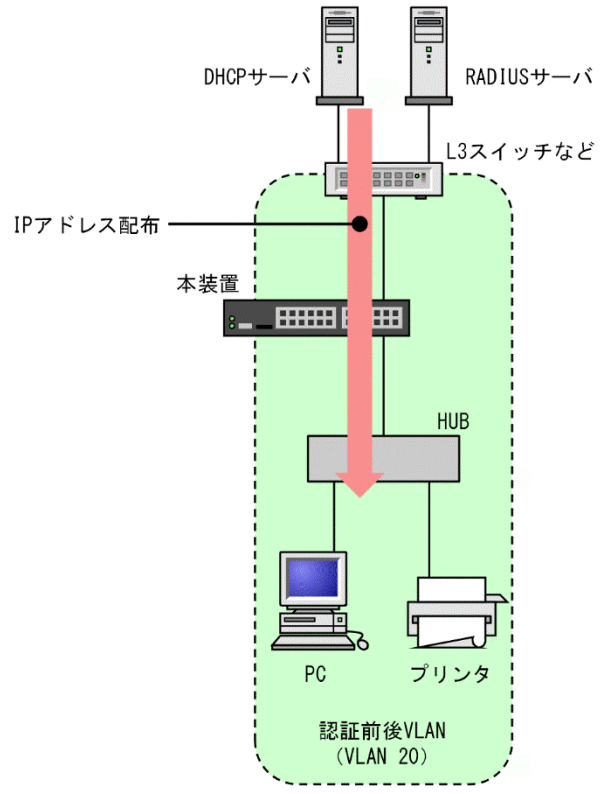
表 12-5　運用コマンド一覧

コマンド名	説明
show authentication multi-step	マルチステップ認証ポートの認証端末情報を，インタフェースごとに表示します。

12.2.2 固定 VLAN モードの設定

固定 VLAN モードによるマルチステップ認証の構成例を次の図に示します。

図 12-2　固定 VLAN モードによるマルチステップ認証の構成例



この例では，PC とプリンタを同一の基本マルチステップ認証ポートに接続し，PC はマルチステップ認証（MAC 認証と IEEE802.1X）を，プリンタはシングル認証（MAC 認証）をします。なお，PC とプリンタの IP アドレスは DHCP サーバから取得します。

［設定のポイント］

この例では，認証対象ポートに次に示す項目を設定します。

- VLAN の設定
- 認証方式の設定
- アクセスポートと VLAN の設定
- 端末認証（MAC 認証）の設定
- ユーザ認証（IEEE802.1X）の設定
- マルチステップ認証ポートの設定
- 認証専用 IPv4 アクセスリストの設定

その他，IEEE802.1X に必要な設定は「7　IEEE802.1X の設定と運用」を，MAC 認証に必要な設定は「11　MAC 認証の設定と運用」を参照してください。

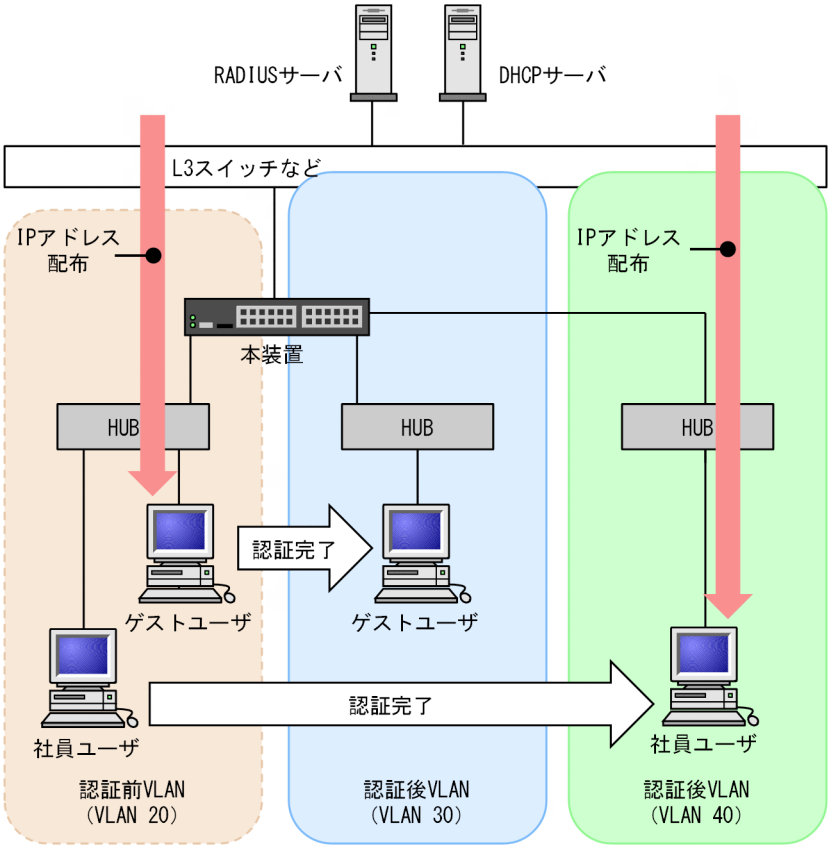
［コマンドによる設定］

1. (config)# vlan 20
   (config-vlan)# exit
   認証の前後で通信する VLAN 20 を設定します。
2. (config)# aaa authentication dot1x default group radius
   (config)# aaa authentication mac-authentication default group radius
   IEEE802.1X と MAC 認証の認証方式に，RADIUS 認証を設定します。
3. (config)# interface gigabitethernet 1/0/1
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 20
   ポート 1/0/1 をアクセスポートとして設定します。また，アクセスポートに VLAN 20 を設定します。
4. (config-if)# mac-authentication port
   (config-if)# dot1x port-control auto
   (config-if)# dot1x multiple-authentication
   (config-if)# dot1x supplicant-detection auto
   (config-if)# authentication multi-step
   ポート 1/0/1 に MAC 認証，IEEE802.1X，マルチステップ認証（ユーザ認証許可オプションなし）を設定します。
5. (config-if)# authentication ip access-group L2-AUTH
   (config-if)# authentication arp-relay
   (config-if)# exit
   ポート 1/0/1 に，認証前の PC とプリンタからのフレームに対する認証専用 IPv4 アクセスリストを設定します。また，認証前端末からの ARP フレーム中継を設定します。
6. (config)# ip access-list extended L2-AUTH
   (config-ext-nacl)# permit udp any any eq bootps
   (config-ext-nacl)# exit
   認証前に DHCP サーバから IP アドレスを取得するため，認証前の PC とプリンタからの DHCP フレーム（bootps）の中継を許可する認証専用 IPv4 アクセスリストを設定します。

12.2.3 ダイナミック VLAN モード設定

ダイナミック VLAN モードによるマルチステップ認証の構成例を次の図に示します。

図 12-3　ダイナミック VLAN モードによるマルチステップ認証の構成例



この例では，ゲストユーザ（PC）と社員ユーザ（PC）をユーザ認証許可オプションポートに接続します。ゲストユーザは，ユーザ認証許可オプションによる認証（MAC 認証（端末認証）に失敗後，Web 認証（ユーザ認証））を行い，認証成功で認証後 VLAN（VLAN 30）へ切り替えます。社員ユーザはマルチステップ認証（MAC 認証と Web 認証）で認証しますが，MAC 認証の認証成功で認証後 VLAN（VLAN 40）へ切り替えます。

なお，ゲストユーザは，MAC 認証の認証失敗後に Web 認証を試みるため，認証前 VLAN で DHCP サーバから IP アドレスを取得しますが，社員ユーザは MAC 認証の認証成功後に Web 認証を試みるため，認証後の VLAN で DHCP サーバから IP アドレスを取得します。

［設定のポイント］

この例では，認証対象ポートに次に示す項目を設定します。

- MAC VLAN を含む各 VLAN の設定
- 認証方式の設定
- MAC ポートとネイティブ VLAN の設定
- 端末認証（MAC 認証）の設定
- ユーザ認証（Web 認証）の設定
- マルチステップ認証ポートの設定（ユーザ認証許可オプション有）
- 認証専用 IPv4 アクセスリストの設定

その他，Web 認証に必要な設定は「9　Web 認証の設定と運用」，MAC 認証に必要な設定は「11　MAC 認証の設定と運用」を参照してください。

［コマンドによる設定］

1.　(config)# vlan 30 mac-based

```
(config-vlan)# exit
(config)# vlan 40 mac-based
(config-vlan)# exit
```

VLAN ID 30 と 40 に MAC VLAN を設定します。（RADIUS サーバから通知される認証後 VLAN と同じ VLAN ID を設定します。）

2.
```
(config)# vlan 20
(config-vlan)# exit
```
VLAN ID 20 を設定します。

3.
```
(config)# aaa authentication mac-authentication default group radius
(config)# aaa authentication web-authentication default group radius
```
MAC 認証と Web 認証の認証方式に RADIUS 認証を設定します。

4.
```
(config)# interface gigabitethernet 0/1
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac native vlan 20
```
ポート 0/1 を MAC ポートとして設定します。また，MAC ポートのネイティブ VLAN20（認証前 VLAN）を設定します。

5.
```
(config-if)# web-authentication port
(config-if)# mac-authentication port
(config-if)# authentication multi-step permissive
(config-if)# exit
```
ポート 0/1 に Web 認証，MAC 認証，マルチステップ認証（ユーザ認証許可オプション有）を設定します。

6.
```
(config-if)# authentication ip access-group L2-AUTH
(config-if)# authentication arp-relay
(config-if)# exit
```
ポート 0/1 に認証前端末からのフレームに対する認証専用 IPv4 アクセスリストを設定します。また，認証前端末からの ARP フレーム中継を設定します。

7.
```
(config)# ip access-list extended L2-AUTH
(config-ext-nacl)# permit udp any any eq bootps
(config-ext-nacl)# exit
```
認証前端末からの DHCP フレーム（bootps）の中継を許可する認証専用 IPv4 アクセスリストを設定します。

［注意事項］

RADIUS サーバから認証成功（Accept）受信で，RADIUS 属性に認証後 VLAN 情報がないときは，該当 MAC ポートのネイティブ VLAN に端末を収容します。このとき，端末は固定 VLAN モードの認証済み端末として扱います。

第4編　セキュリティ

13 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。

13.1 解説

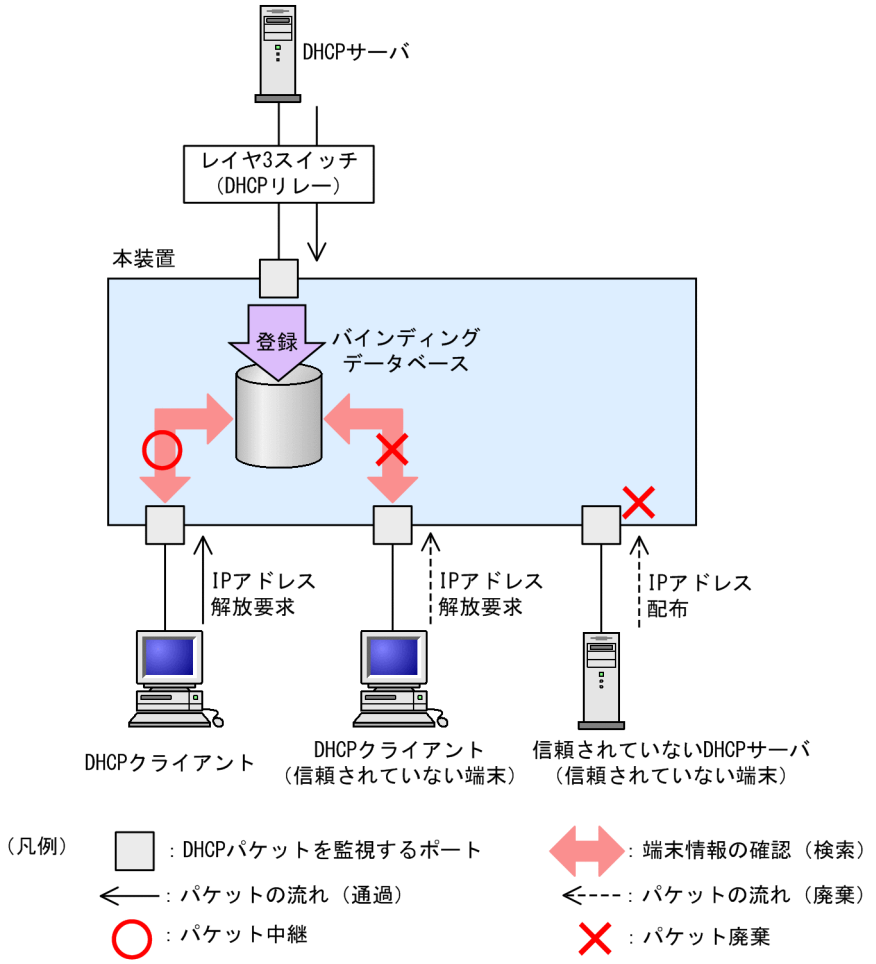
13.1.1 概要

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ダイナミック 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 13-1　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 13-1　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	・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

項目	機能の概要
固定 IP アドレスを持つ端末の登録	・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	・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	・信頼されていない DHCP サーバからの IP アドレス配布を抑止 ・信頼されていない DHCP クライアントからの IP アドレス解放を抑止 ・MAC アドレスの詐称を抑止 ・Option82 の詐称を抑止
DHCP パケットの受信レート制限	・設定した受信レートを超えた DHCP パケットを廃棄
端末フィルタ	・信頼されていない端末からの IPv4 パケットの中継を抑止
ARP パケットの検査	・信頼されていない端末からの ARP パケットの中継を抑止 ・MAC アドレスおよび IP アドレスの詐称を抑止
ARP パケットの受信レート制限	・設定した受信レートを超えた ARP パケットを廃棄

(1) スタック構成

マスタスイッチがバインディングデータベースを管理して，メンバスイッチと同期を行います。

マスタスイッチ以外のメンバスイッチでは，バインディングデータベースの保存と，端末フィルタだけを実施します。そのほかの機能はマスタスイッチで実施します。

13.1.2 DHCP パケットの監視

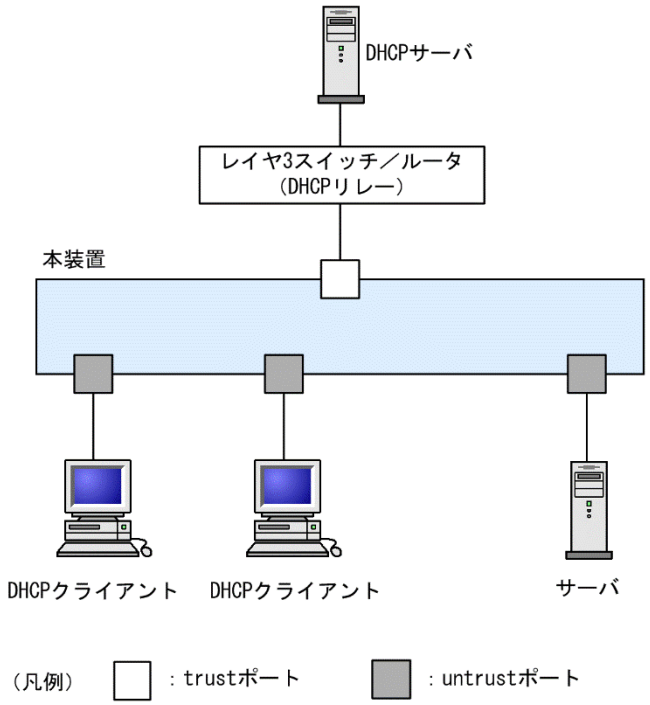
(1) ポートの種別

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 13-2　ポートの種別



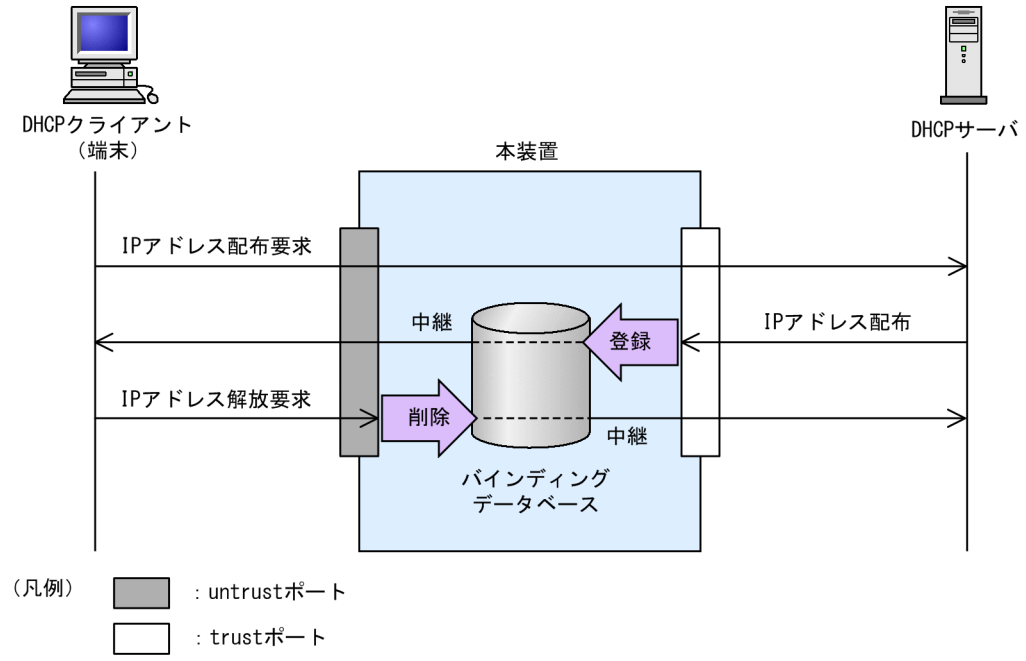
コンフィグレーションコマンド ip dhcp snooping で DHCP snooping を有効にすると，デフォルトですべてのポートが untrust ポートになります。DHCP サーバへ接続するポートを trust ポートとして設定してください。trust ポートはコンフィグレーションコマンド ip dhcp snooping trust で設定できます。

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 13-3　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。バインディングデータベースへの登録対象は，untrust ポートに接続した端末の端末情報です。

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 13-2 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 ・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ネルグループ番号	
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。

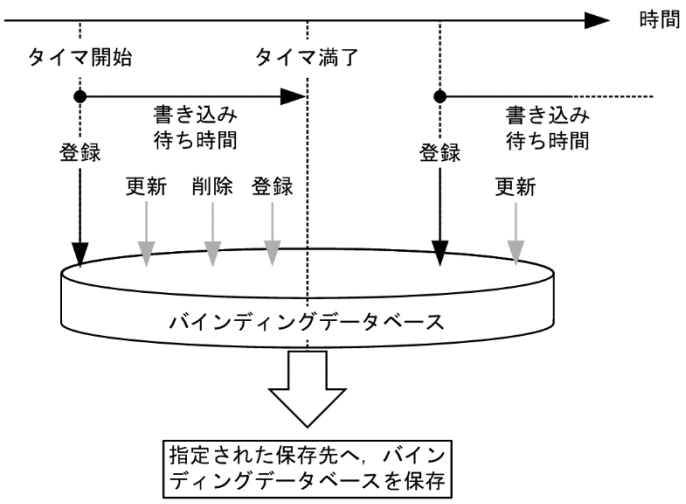
- ダイナミックのバインディングデータベースの登録，更新，または削除時
- コンフィグレーションコマンド ip dhcp snooping database url 設定時（保存先の変更を含む）
- 運用コマンド clear ip dhcp snooping binding 実行時

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始しません。

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 13-4　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

(e)　スタック構成

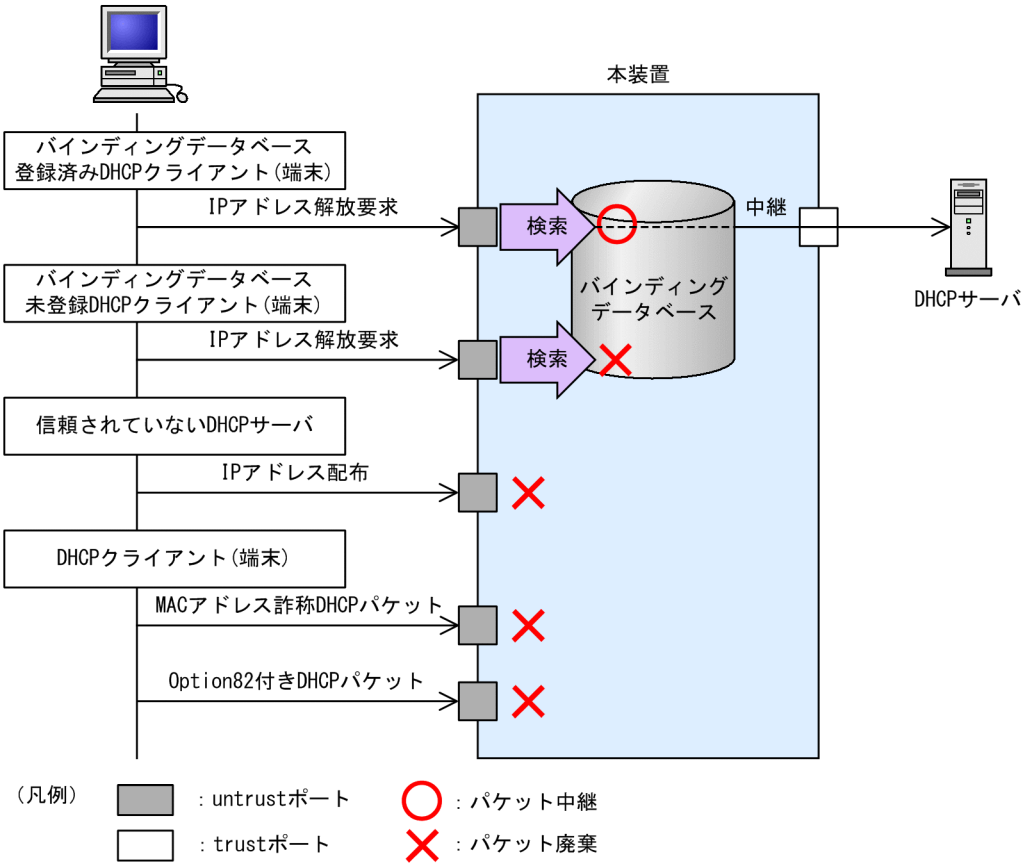
バインディングデータベースはメンバスイッチ間で同期され，前述の保存契機ですべてのメンバスイッチに保存されます。

復元はマスタスイッチの起動時だけ実施します。マスタスイッチに保存されたバインディングデータベースを復元します。

(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 13-5　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 アドレス配布を抑止
  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 アドレス配布を抑止します。
- 信頼されていない DHCP クライアントからの IP アドレス解放を抑止
  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，IP アドレス重複検出通知（DHCP DECLINE）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 アドレス解放を抑止します。
- MAC アドレスの詐称を抑止
  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止します。
- Option82 の詐称を抑止
  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 の詐称を抑止します。

13.1.3 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超えた 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。

受信レートを超えた DHCP パケットは廃棄し，運用ログ情報を採取します。ただし，SNMP 通知は送信しません。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。

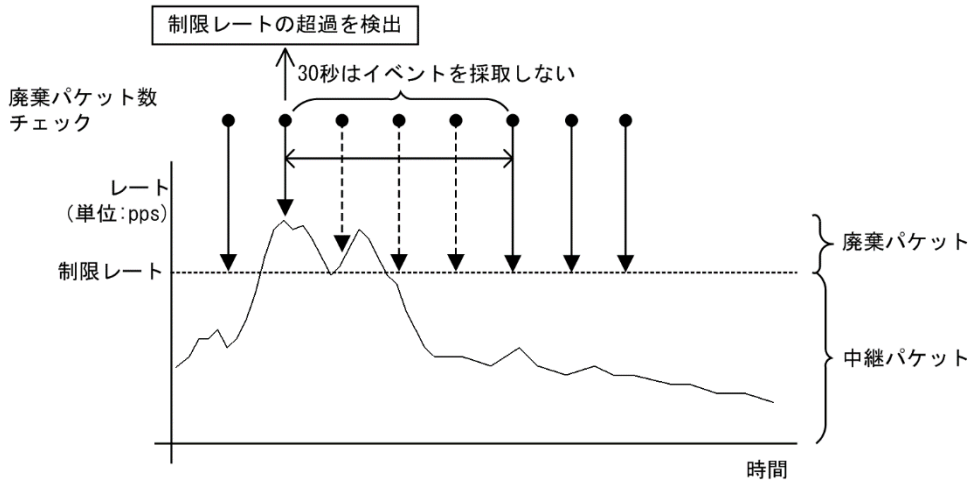
(1)　運用ログ情報の採取契機

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 13-6　DHCP パケット受信レートの運用ログ情報の採取契機



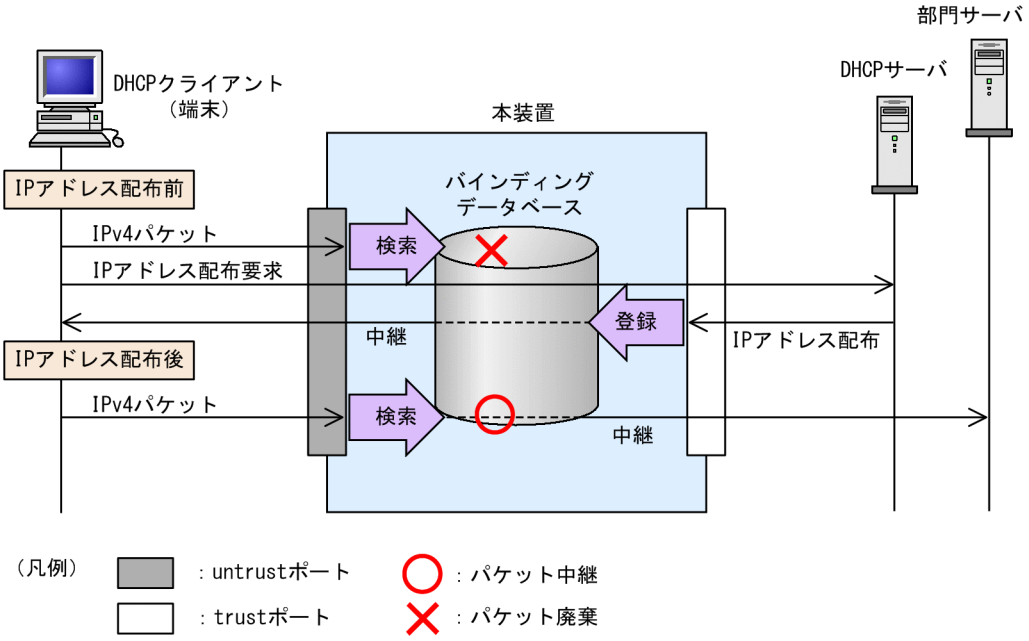
13.1.4 端末フィルタ

(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 13-7　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。

(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 13-3　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

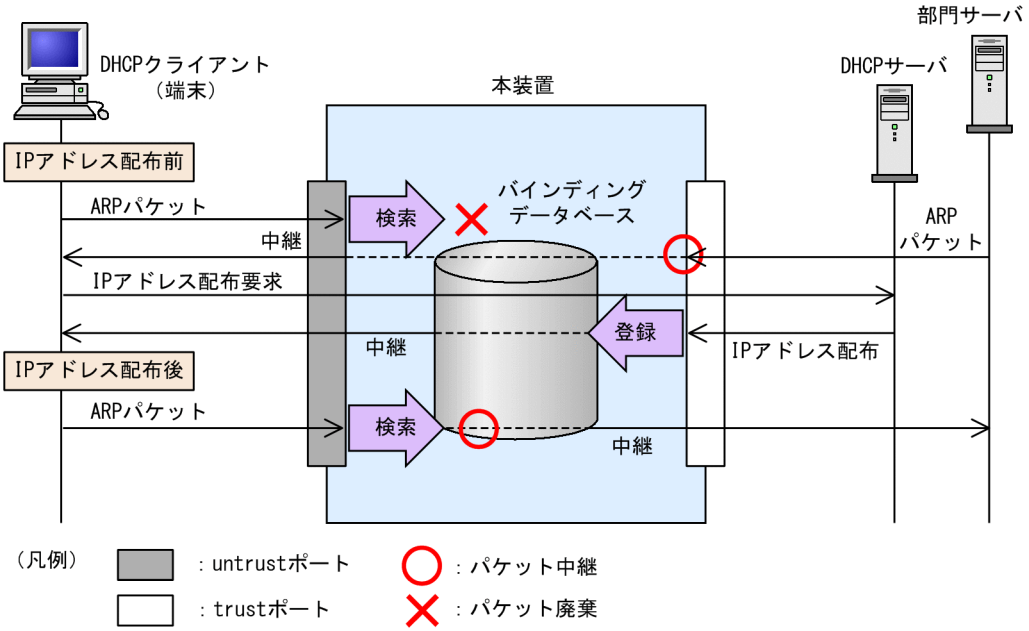
13.1.5 ダイナミック ARP 検査

(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 13-8　ダイナミック ARP 検査の動作概要



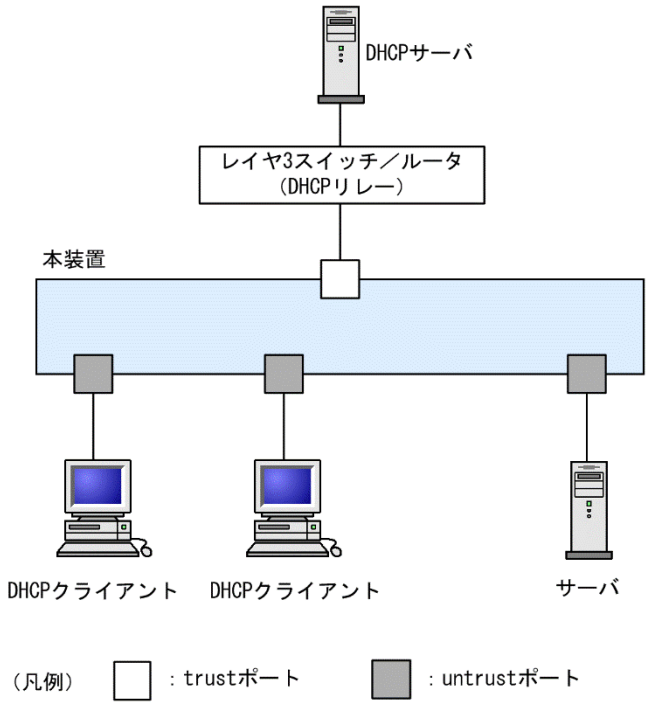
(2)　ポートの種別

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 13-9　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 13-4　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 13-5　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 13-6　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 13-7　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	－	－	－	－	－	－	－	－

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
Reply	－	－	－	－	－	－	－	○

（凡例）○：検査対象　－：検査対象外

13.1.6 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超えた 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。

受信レートを超えた ARP パケットは廃棄し，運用ログ情報を採取します。ただし，SNMP 通知は送信しません。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)　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，「13.1.3　DHCP パケットの受信レート制限　(1)　運用ログ情報の採取契機」を参照してください。

13.1.7 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」　「24.3　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)　レイヤ 2 認証との共存

「5.2.1　レイヤ 2 認証と他機能との共存」を参照してください。

(3)　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。

(4)　バインディングデータベースの保存と復元について

- コンフィグ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。

- コンフィグ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グ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。

(5) 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。

(6) 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。

(7) 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。

(8) 端末フィルタの収容条件について

端末フィルタの収容条件を超えている場合，バインディングデータベースには保持されますが，端末フィルタの登録に失敗します。登録に失敗したクライアントがバインディングデータベースに保持されている間，端末フィルタに自動的には登録されません。

端末フィルタへの登録には，本装置のバインディングデータベースからいったん削除したあと，再学習が必要です。例えば，次の手順を実施してください。

1. 不要なバインディングエントリを削除する（収容条件超えを解消）。
2. 再登録したいクライアントで，アドレスをいったん解放する（DHCP サーバにリリースを通知する）。
3. 再登録したいクライアントで，アドレスの払い出しを実施する。

(9) 監視および検査できないフレームについて

次に示す機能を設定したポートで，VLAN Tag フィールドが多数あり VLAN ID が 0 であるものを含む Tagged フレームや，802.3 LLC/SNAP 形式のフレームで，LENGTH が 1501～1535 のフレームを受信した場合，該当フレームに対して監視および検査が動作せず，中継されます。該当フレームを廃棄するには，コンフィグレーションコマンド switchport validation を設定してください。

- DHCP パケットの監視および検査
- 端末フィルタ
- ダイナミック ARP 検査

13.2 コマンドガイド

13.2.1 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 13-8 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。

DHCP snooping の運用コマンド一覧を次の表に示します。

表 13-9 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

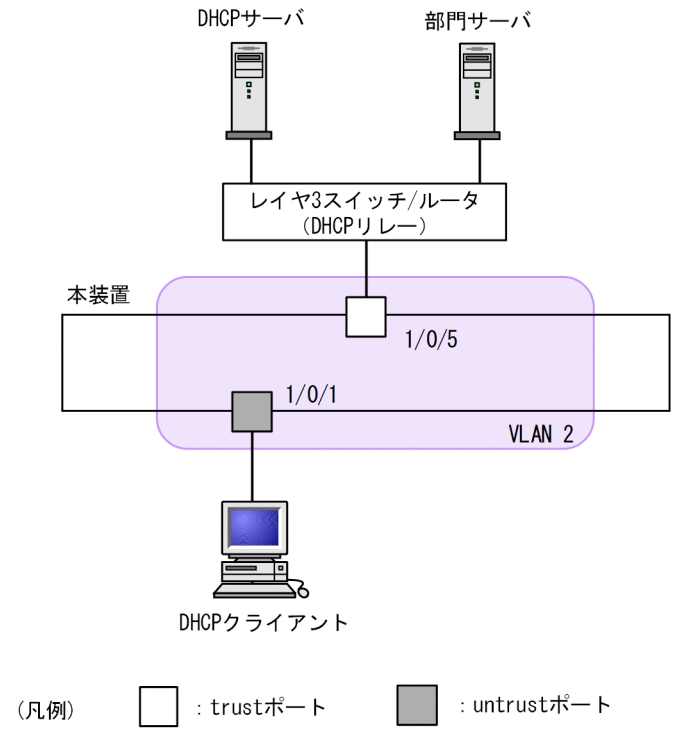
コマンド名	説明
	します。

13.2.2 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。

DHCP snooping の基本的な構成例を次の図に示します。

図 13-10　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 1/0/1
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 2
   (config-if)# exit
   ポート 1/0/1 をアクセスポートとし，ポート 1/0/1 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 13-10 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 1/0/5
   (config-if)# ip dhcp snooping trust
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 2
   (config-if)# exit
   ポート 1/0/5 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 1/0/5 をアクセスポートとし，ポート 1/0/5 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 はアラクサ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。

13.2.3 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。

13.2.4 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 1/0/1
   (config-if)# ip verify source port-security
   (config-if)# exit
   ポート 1/0/1 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。

13.2.5 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 1/0/5
   (config-if)# ip arp inspection trust
   (config-if)# exit
   ポート 1/0/5 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。

13.2.6 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］

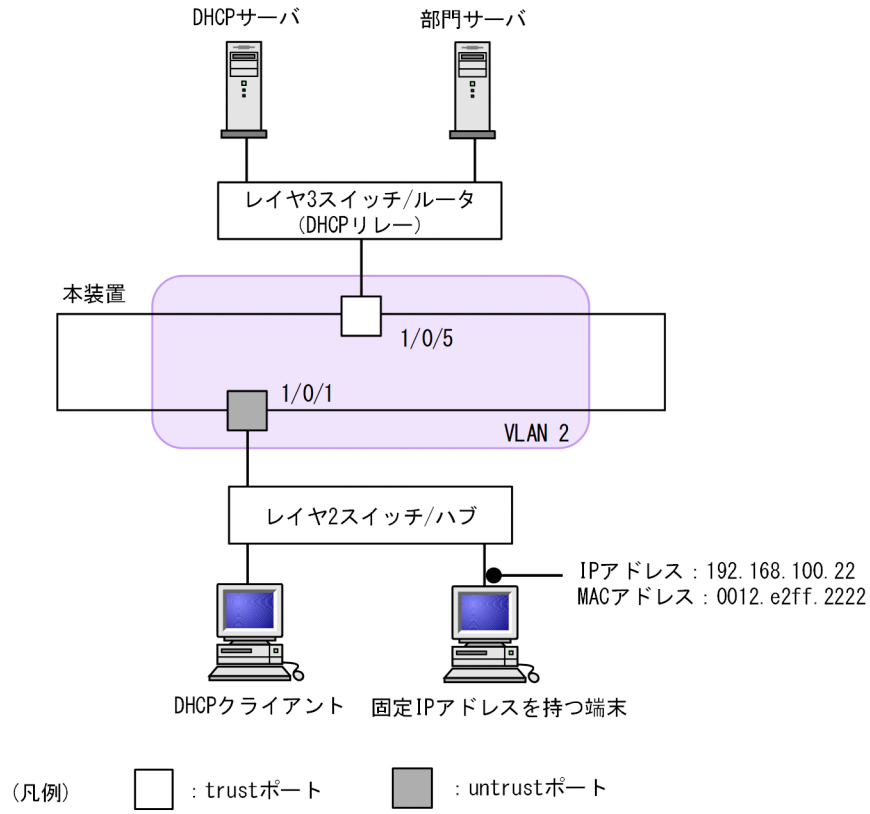
1. (config)# ip arp inspection limit rate 100
   本装置の受信レートを 100 パケット/秒に設定します。

13.2.7 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 13-11　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，「13.2.2　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 1/0/1

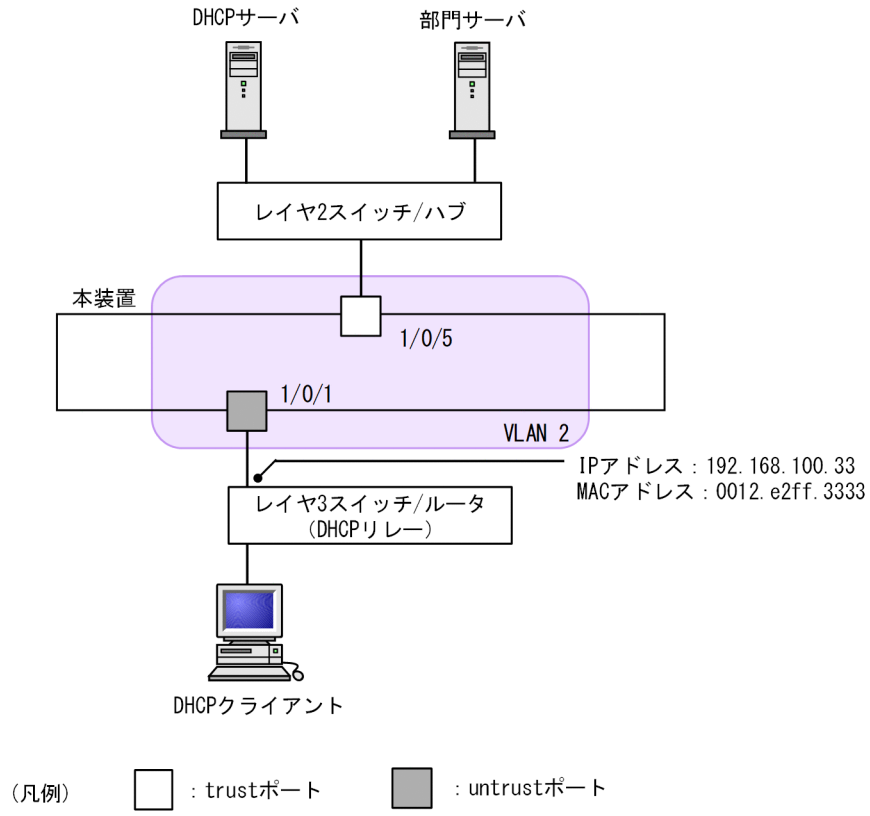
   端末の MAC アドレス，端末が所属する VLAN（VLAN ID），端末の IP アドレス，および端末が接続されているポート番号を，バインディングデータベースに設定します。

13.2.8 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 13-12　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，「13.2.2　基本設定」，「13.2.4　端末フィルタ」，および「13.2.5　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 1/0/1
(config-if)# ip verify source
(config-if)# exit
```
ポート 1/0/1 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。

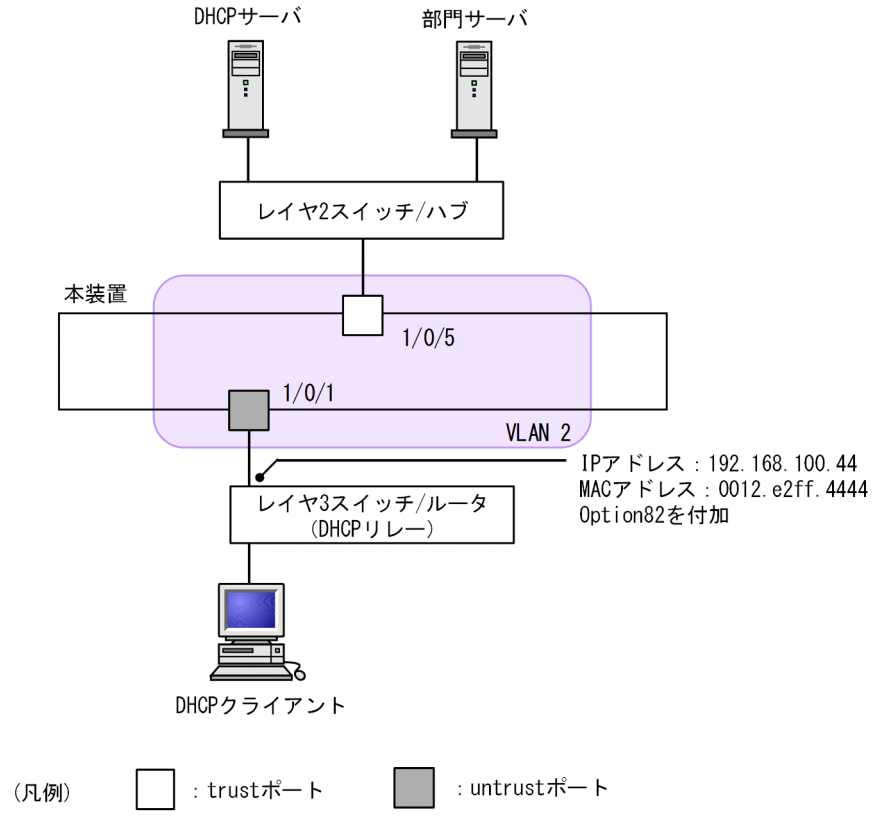
設定については，「13.2.7　固定 IP アドレスを持つ端末を接続した場合」を参照してください。

13.2.9 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 13-13　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「13.2.2　基本設定」，「13.2.4　端末フィルタ」，および「13.2.5　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，「13.2.8　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，「13.2.8　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，「13.2.7　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。

13.2.10 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，メッセージ種別に DHCP snooping を設定します。

第5編　冗長化構成による高信頼化機能

14 GSRP aware

GSRP aware は，GSRP スイッチからフレームを受信することによって，自装置の MAC アドレステーブルをクリアする機能です。この章では，GSRP aware について説明します。

14.1 解説

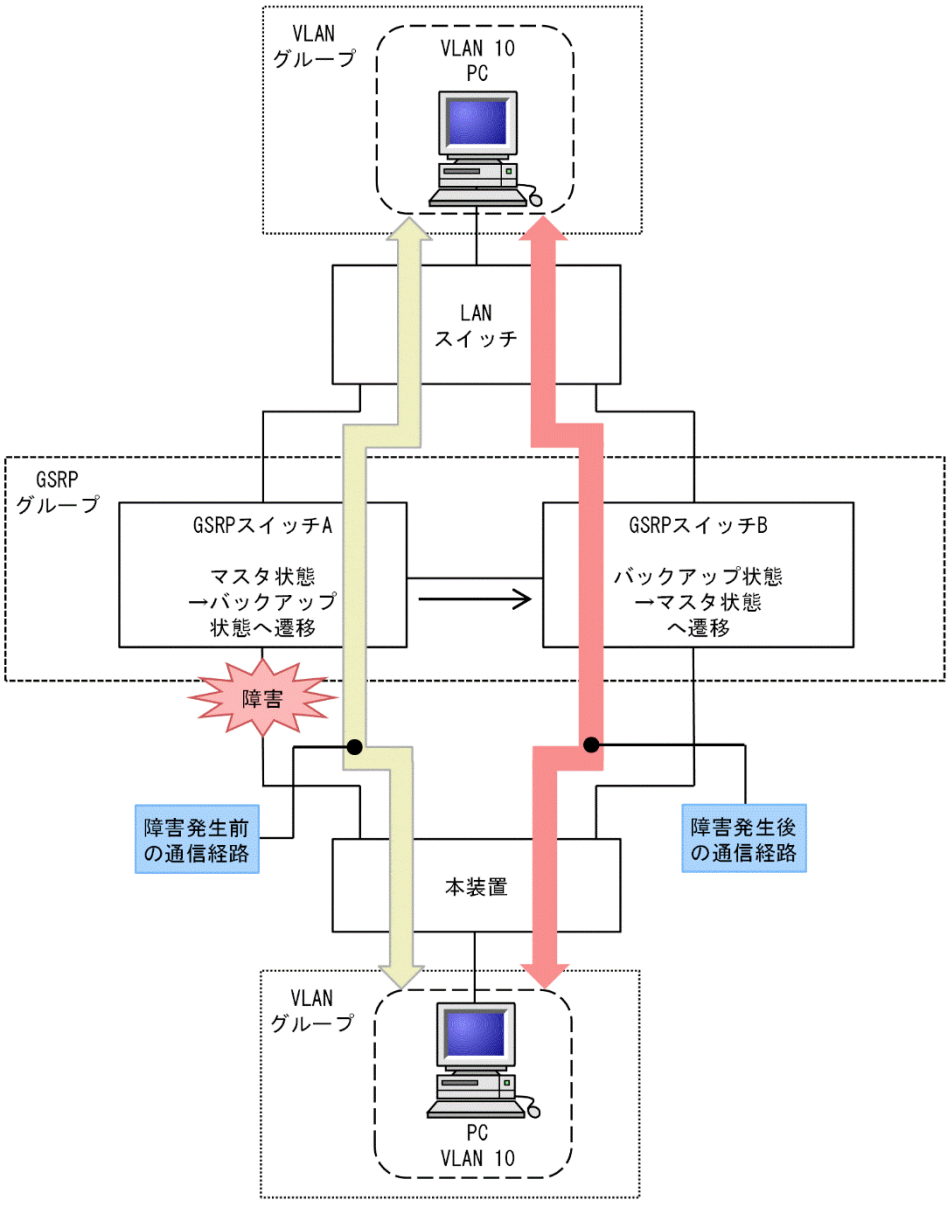
14.1.1 GSRP の概要

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。

ネットワークを冗長化する機能としてスパニングツリーがありますが，GSRP では 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。

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 14-1　GSRP の概要



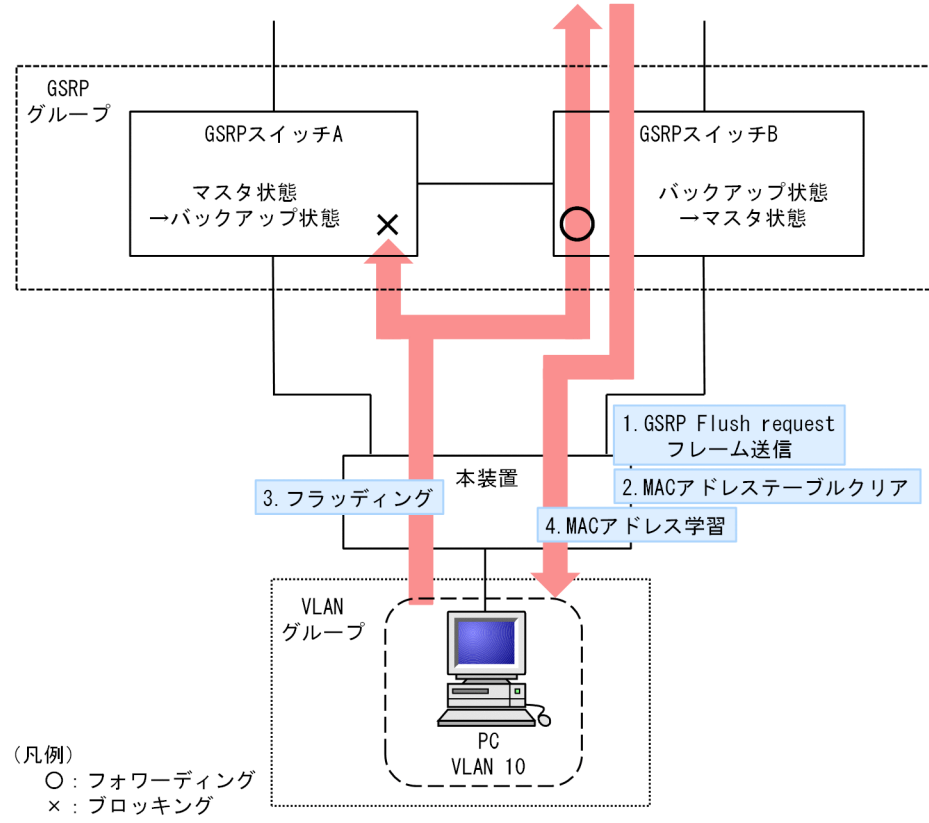
本装置は，GSRP aware をサポートします。GSRP aware は，GSRP スイッチから制御フレームを受信することによって，自装置の MAC アドレステーブルをクリアします。なお，GSRP aware について，コンフィグレーションコマンドでの設定はありません。

14.1.2 GSRP スイッチ切り替えの動作

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，エンドー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 スイッチ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，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。GSRP Flush request フレーム受信時の動作を次の図に示します。

図 14-2　GSRP Flush request フレーム受信時の動作



1. GSRP スイッチ A と GSRP スイッチ B との間で切り替えが行われ，GSRP スイッチ B は GSRP Flush request フレームを本装置へ向けて送信します。
2. 本装置は 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 GSRP スイッチ 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 宛てのフレームが戻ってくると，本装置は MAC アドレス学習を行います。
   以後，本装置は PC からのフレームを GSRP スイッチ B へ向けてだけフォワーディングするようになります。

14.1.3 GSRP aware 使用時の注意事項

(1) 他機能との共存について

(a) 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」　「24.3　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。

(b) レイヤ 2 認証との共存

「5.2.1　レイヤ 2 認証と他機能との共存」を参照してください。

(c) 冗長化構成による高信頼化機能との共存

GSRP との共存で制限のある，冗長化構成による高信頼化機能を次の表に示します。

表 14-1　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
アップリンク・リダンダント	アップリンク・リダンダントによるブロッキング状態のポートでは，GSRP Flush request フレームを受信しません。

14.2 コマンドガイド

14.2.1 コマンド一覧

GSRP aware の運用コマンド一覧を次の表に示します。

表 14-2　運用コマンド一覧

コマンド名	説明
show gsrp aware	GSRP の aware 情報を表示します。
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。

15 アップリンク・リダンダント

アップリンク・リダンダントは，アップリンクに使用する二つのポートのうち，どちらか一方で通信し，もう一方を障害時用に待機させることで，冗長化構成ができるようにするための機能です。アップリンクのポートには，物理ポートまたはリンクアグリゲーションを設定できます。

この章では，アップリンク・リダンダントの解説と操作方法について説明します。

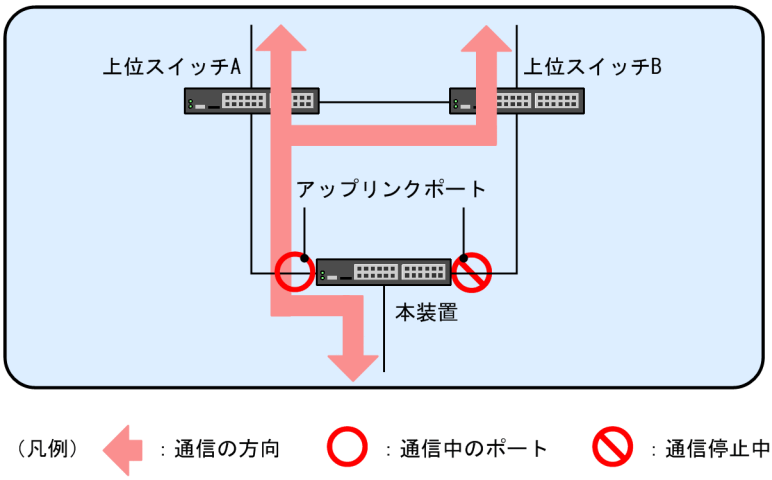
15.1 解説

15.1.1 概要

アップリンク・リダンダントは，本装置でアップリンクに用いるポートを二重化し，通信中にリンク障害が起こったときは待機中のポートに切り替えて上位スイッチとの通信を継続する機能です。本機能を使用すると，スパニングツリーなどの複雑なプロトコルを使わないでアップリンクに用いるポートを冗長化できます。冗長化するための二つのポートをあわせて，**アップリンクポート**と呼びます。

アップリンク・リダンダントの基本構成を次の図に示します。

図 15-1　アップリンク・リダンダントの基本構成



この図の構成でアップリンク・リダンダントを使用した場合，本装置と上位スイッチ A との間のリンクに障害が発生しても，本装置と上位スイッチ B との間のリンクに切り替えることで通信を継続できます。

15.1.2 サポート仕様

アップリンク・リダンダントでのサポート状況を次の表に示します。

表 15-1　アップリンク・リダンダントでのサポート状況

項目		サポート有無・仕様
適用インタフェース	物理ポート	○
	リンクアグリゲーション	○
アップリンクポート数		「コンフィグレーションガイド Vol.1」　「3　収容条件」参照
一つのアップリンクポートに設定可能なインタフェース数		2
プライマリポートへのアクティブポート自動切り戻し		○
プライマリポートへのアクティブポート自動切り戻し抑止		○
アクティブポート変更コマンド		○
アクティブポート変更時のフラッシュ制御フレーム送受信機能		○
アクティブポート変更時の MAC アドレスアップデート機能		○
アクティブポート変更時のポートリセット機能		○
起動時のアクティブポート固定機能		○※
プライベート MIB，プライベートの SNMP 通知		○

（凡例）○：サポート

注※

スタック構成時，マスタスイッチの切り替えが発生した場合，本機能を解除します。

15.1.3 アップリンク・リダンダント動作概要

アップリンク・リダンダントでは，1 対のポートまたはリンクアグリゲーションを用いて冗長性を確保します。このポート対がアップリンクポートです。アップリンクポートには，通常，通信を行うプライマリポートと，プライマリポートの障害時に通信を行うセカンダリポートの二つがあります。これらのポートは，コンフィグレーションで設定します。

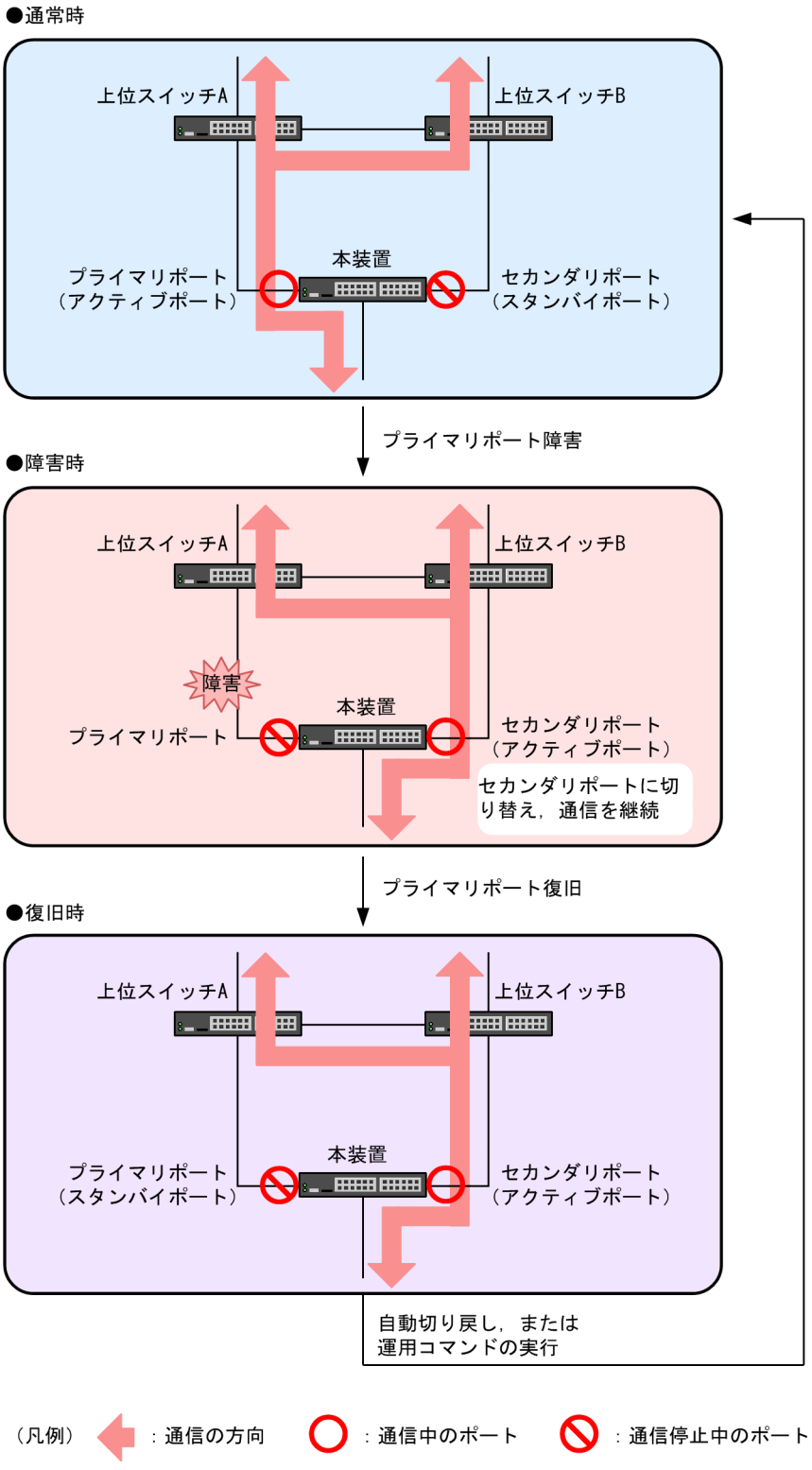
プライマリポートとセカンダリポートは，同じ帯域やポート数である必要はありません。例えば，プライマリポートには 10 ギガビット・イーサネットポートを，セカンダリポートには 1 ギガビット・イーサネットポートを 5 本束ねたリンクアグリゲーションを設定することもできます。

アップリンクポートのうち，現在通信を行っているポートをアクティブポートと呼びます。また，アクティブポートに障害が発生した場合に，通信継続のため，すぐに通信を開始できるような準備ができているポートをスタンバイポートと呼びます。

アップリンクポートを構成する 1 対のポートは，VLAN などの構成を同一設定にする必要があります。また，アップリンクポートに設定しているポートは，ほかのアップリンクポートでは設定できません。

アップリンク・リダンダントの動作概要を次の図に示します。

図 15-2　アップリンク・リダンダントの動作概要



通常時

本装置のプライマリポートを経由して，上位スイッチへ通信できる状態です。本装置のセカンダリポートは通信していない状態です。

障害時

プライマリポートのリンクダウンを契機に，本装置がアクティブポートをセカンダリポートに変更し，セカンダリポートを経由して上位スイッチへの通信を継続します。この動作を切り替えと呼びます。このとき，新しくアクティブポートになったセカンダリポートから上位スイッチへ，フラッシュ制御フレームという専用の制御フレームまたは MAC アドレスアップデートフレームを送信することで，上位スイッチの MAC アドレステーブルを更新し，通信を速やかに復旧できます。

復旧時

プライマリポートがリンクアップしてスタンバイポートになっていれば，自動切り戻し機能を使用する，または本装置で運用コマンドを実行することで，アクティブポートをプライマリポートに変更できます。この動作を切り戻しと呼びます。

また，切り替え時と同様に，フラッシュ制御フレームまたは MAC アドレスアップデートフレームを送信すること，またはポートリセット機能によって旧アクティブポートを一時的にダウンさせることで，通信を速やかに復旧できます。

15.1.4 切り替え・切り戻し動作

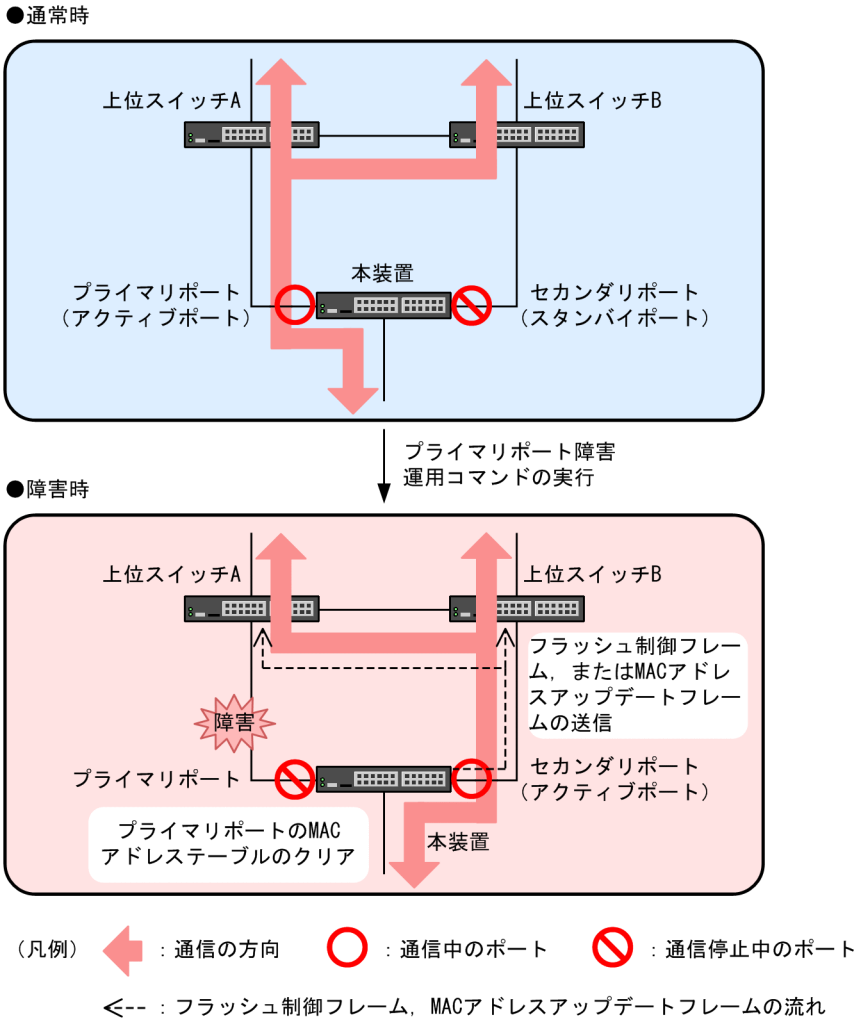
切り替え・切り戻しとは，通信を行っているポートを変更する動作です。切り替え・切り戻しは，アクティブポートの変更先ポートがスタンバイポートとなっている場合に，次の契機で動作します。

- アクティブポートに障害が発生する
- 自動切り戻し機能の待ち時間が経過する
- アクティブポートを変更する運用コマンドを実行する

切り替え・切り戻し動作と同時に，通信を行っていたポートで学習していた MAC アドレスをすべてクリアして，新しくアクティブポートになったポートで通信を行います。フラッシュ制御フレームまたは MAC アドレスアップデートフレームを送信する設定をしている場合は，切り替え・切り戻しと同時に新しくアクティブポートになったポートからフラッシュ制御フレームまたは MAC アドレスアップデートフレームを送信します。ポートリセット機能を設定している場合は，旧アクティブポートを一時的にダウンさせます。

切り替え動作を次の図に示します。

図 15-3　切り替え動作(フラッシュ制御フレームまたは MAC アドレスアップデートフレーム送信設定時)



15.1.5 自動切り戻し機能

自動切り戻し機能とは，プライマリポートの障害によってセカンダリポートがアクティブポートになっている状態で，プライマリポートが障害から復旧した場合に，自動的にアクティブポートをプライマリポートに変更する機能です。切り戻しの待ち時間は，0 秒（即時）から 300 秒の間で設定できます。

運用コマンドによってアクティブポートを変更した場合，自動切り戻しは動作しません。ただし，次のどちらかの条件を満たす場合には自動切り戻しが動作します。

- 運用コマンドによってアクティブポートを変更したあとで，コンフィグレーションで本機能を設定または変更した場合
- 運用コマンドによってアクティブポートを変更したあとで，プライマリポートの障害が発生または回復した場合

15.1.6 通信復旧の補助機能

アップリンク・リダンダントでは，切り替え・切り戻し動作時に通信復旧を補助する三つの機能をサポートしています。なお，一つのアップリンクポートに設定できる機能はどれか一つだけです。

- フラッシュ制御フレーム送受信機能
  フラッシュ制御フレームを送信することで，上位スイッチの MAC アドレステーブルをクリアして，フ

ラッディングによって通信を復旧します。上位スイッチは，フラッシュ制御フレームによる MAC アドレステーブルのクリアをサポートしている必要があります。

- MAC アドレスアップデート機能
  MAC アドレスアップデートフレームを送信することで，上位スイッチに端末の MAC アドレスを再学習させて通信を復旧します。上位スイッチに専用の受信機能は必要ありませんが，再学習させられる MAC アドレス数に制限があります。また，通信を復旧するまでに 10 秒程度時間が掛かる場合があります。
- ポートリセット機能
  旧アクティブポートを一時的にダウンさせることで，リンクダウンを検出した上位スイッチが，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し，フラッディングによって通信を復旧します。上位スイッチに専用の機能は必要ありませんが，プライマリポートとセカンダリポートは同一の上位スイッチと接続している必要があります。

フラッシュ制御フレーム送受信機能は，上位スイッチがフラッシュ制御フレームをサポートしている装置を想定しているのに対して，MAC アドレスアップデート機能およびポートリセット機能は，フラッシュ制御フレームを受信できない装置を想定しています。

15.1.7 フラッシュ制御フレーム送受信機能

(1) 送信動作

通信を行っているリンクの障害や運用コマンドによって，アクティブポートを変更した場合，通信を速やかに復旧させるために，上位スイッチの MAC アドレステーブルをクリアするフラッシュ制御フレームを送信できます。フラッシュ制御フレームの送信は，アップリンクポートごとに設定でき，送信先の VLAN を指定できます。

MAC アドレステーブルをクリアしたくない装置がネットワーク上にある場合には，フラッシュ制御フレームを送受信する専用の VLAN を作成し，その VLAN にフラッシュ制御フレームを送信するように設定することで，MAC アドレステーブルをクリアする装置の範囲を制限できます。

本装置はフラッシュ制御フレームを，アクティブポートの変更直後に，新しくアクティブポートになったポートから送信します。

トランクポートでフラッシュ制御フレームを送信する場合には，送信先の VLAN を指定する必要があります。アクセスポート，MAC ポートまたはプロトコルポートの場合には，送信先 VLAN の指定の有無に関係なく，Untagged フレームのフラッシュ制御フレームを送信します。

(2) 受信動作

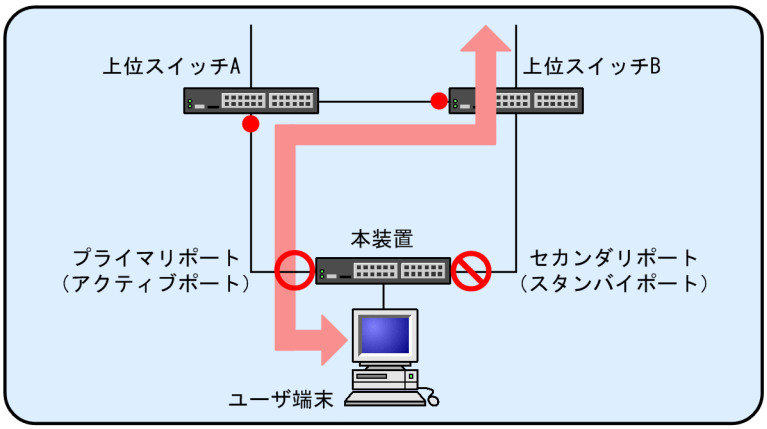
本装置は，フラッシュ制御フレームを受信すると MAC アドレステーブルをクリアします。

フラッシュ制御フレームを受信するためのコンフィグレーションは必要ありません。ただし，特定の VLAN にフラッシュ制御フレームを送信する設定となっている場合には，その VLAN でフラッシュ制御フレームが通信できる状態となっている必要があります。

フラッシュ制御フレームの使用による切り替え動作の違いを次の図に示します。

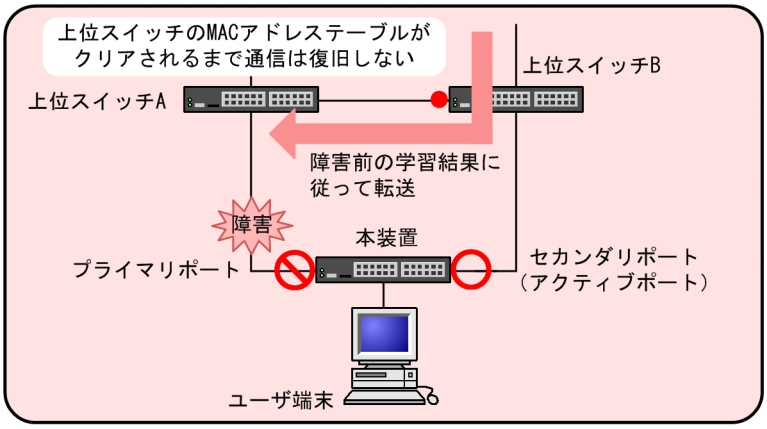
図 15-4　フラッシュ制御フレームの使用による切り替え動作の違い

●通常時（上位スイッチA，Bを経由するデータの流れ）

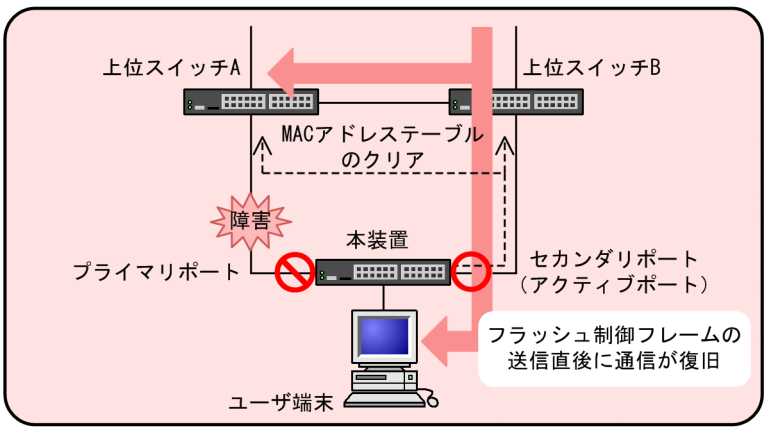


●障害時

フラッシュ制御フレームを送信しない場合



フラッシュ制御フレームを送信する場合



（凡例）　：通信の方向　　：通信中のポート　　：通信停止中のポート

<-- ：フラッシュ制御フレームの流れ　　：ユーザ端末のMACアドレス学習ポート

通常時

本装置のプライマリポートで通信を行っている状態では，上位スイッチはユーザ端末の MAC アドレスを，現在の通信経路で学習しています。

障害時（フラッシュ制御フレームの送信なし）

フラッシュ制御フレームを送信する設定がない場合，アクティブポートをセカンダリポートに切り替えても，上位スイッチ B がユーザ端末の MAC アドレスを以前のポートで学習しているため，上位スイッチ B が学習した MAC アドレスが消えるか，ユーザ端末からの通信がなければ，通信は復旧しません。

障害時（フラッシュ制御フレームの送信あり）

フラッシュ制御フレームを送信する設定の場合は，アクティブポートをセカンダリポートに切り替えると同時に，フラッシュ制御フレームによって上位スイッチ B が学習した MAC アドレスを削除するため，通信を速やかに復旧できます。

15.1.8 MAC アドレスアップデート機能

(1)　送信動作

通信を行っているリンクの障害や運用コマンドによって，アクティブポートを変更した場合，通信を速やかに復旧させるために，上位スイッチに端末の MAC アドレスを再学習させる MAC アドレスアップデートフレームを送信できます。MAC アドレスアップデートフレームの特徴は次のとおりです。

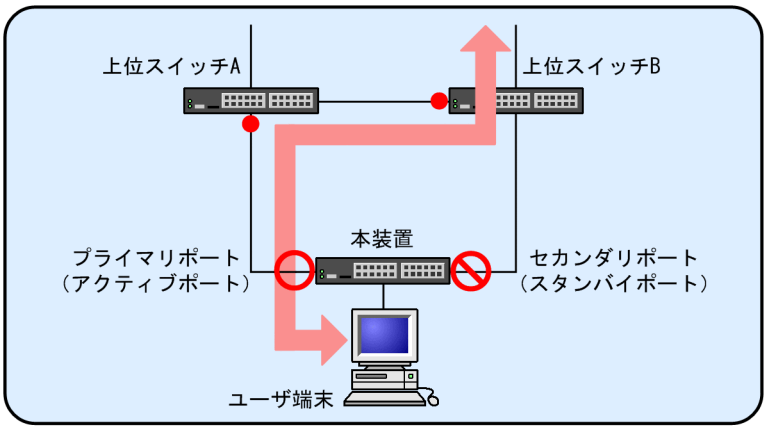
- マルチキャストフレームである
- 送信元 MAC アドレスに，上位スイッチに再学習させる MAC アドレスを設定する
- 専用の受信機能を必要としない

MAC アドレスアップデート機能は，アップリンクポートごとに設定できます。また，送信対象外とする VLAN を指定できます。

MAC アドレスアップデートフレームの使用による切り替え動作の違いを次の図に示します。

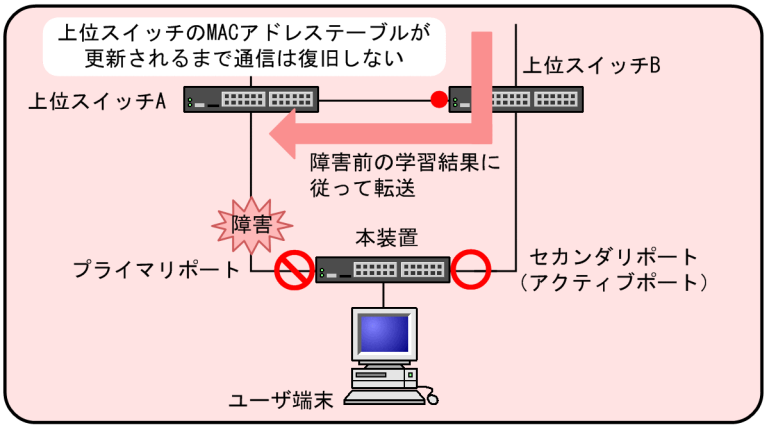
図 15-5　MAC アドレスアップデートフレームの使用による切り替え動作の違い

●通常時（上位スイッチA，Bを経由するデータの流れ）

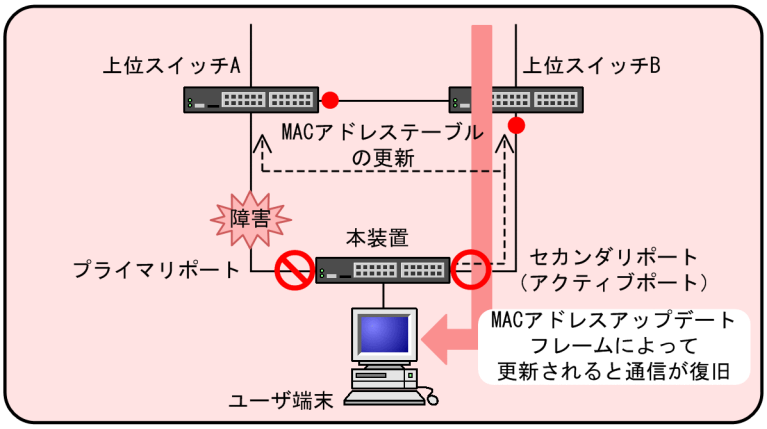


●障害時

MACアドレスアップデートフレームを送信しない場合



MACアドレスアップデートフレームを送信する場合



（凡例）　：通信の方向　　：通信中のポート　　：通信停止中のポート

<-- ：MACアドレスアップデートフレームの流れ　　：ユーザ端末のMACアドレス学習ポート

通常時

本装置のプライマリポートで通信を行っている状態では，上位スイッチはユーザ端末の MAC アドレスを，現在の通信経路で学習しています。

障害時（MAC アドレスアップデートフレームの送信なし）

MACアドレスアップデートフレームを送信する設定がない場合，アクティブポートをセカンダリポートに切り替えても，上位スイッチBがユーザ端末のMACアドレスを以前のポートで学習しているため，上位スイッチBが学習したMACアドレスが消えるか，ユーザ端末からの通信がなければ，通信は復旧しません。

障害時（MACアドレスアップデートフレームの送信あり）

MACアドレスアップデートフレームを送信する設定の場合は，アクティブポートをセカンダリポートに切り替えると同時に，MACアドレスアップデートフレームによって上位スイッチBがユーザ端末のMACアドレス学習ポートを更新するため，通信を速やかに復旧できます。

MACアドレスアップデート機能の仕様を次の表に示します。

表 15-2　MACアドレスアップデート機能の仕様

項目	内容
送信対象ポートの設定単位	アップリンクポート単位
送信ポート	通信可能となったアクティブポート
送信回数※	1～3回
送信対象となるMACアドレスエントリ	次の二つの条件を同時に満たすエントリ ・該当のアップリンクポートが所属するVLANで学習しているエントリ。ただし，コンフィグレーションで送信対象外に設定したVLANで学習しているエントリは除きます。 ・該当のアップリンクポート以外で学習しているエントリ
送信対象となるMACアドレスエントリ種別	・ダイナミックエントリ ・スタティックエントリ ・IEEE802.1Xによるエントリ ・Web認証機能によるエントリ ・MAC認証機能によるエントリ ・装置MACアドレス ・仮想MACアドレス
最大送信MACアドレスエントリ	3000エントリ。 送信対象のエントリが3000エントリを超えていた場合は，3000エントリ分を送信するとともに，収容条件を超えていたことを示す運用ログを出力します。
送信レート	最大300pps

注※

コンフィグレーションで設定できます。

(2)　受信動作

MACアドレスアップデートフレームの中継時に，ほかの受信フレームと同様に送信元MACアドレスを学習してMACアドレステーブルに登録します。詳細は，「コンフィグレーションガイド Vol.1」　「25　MACアドレス学習」を参照してください。

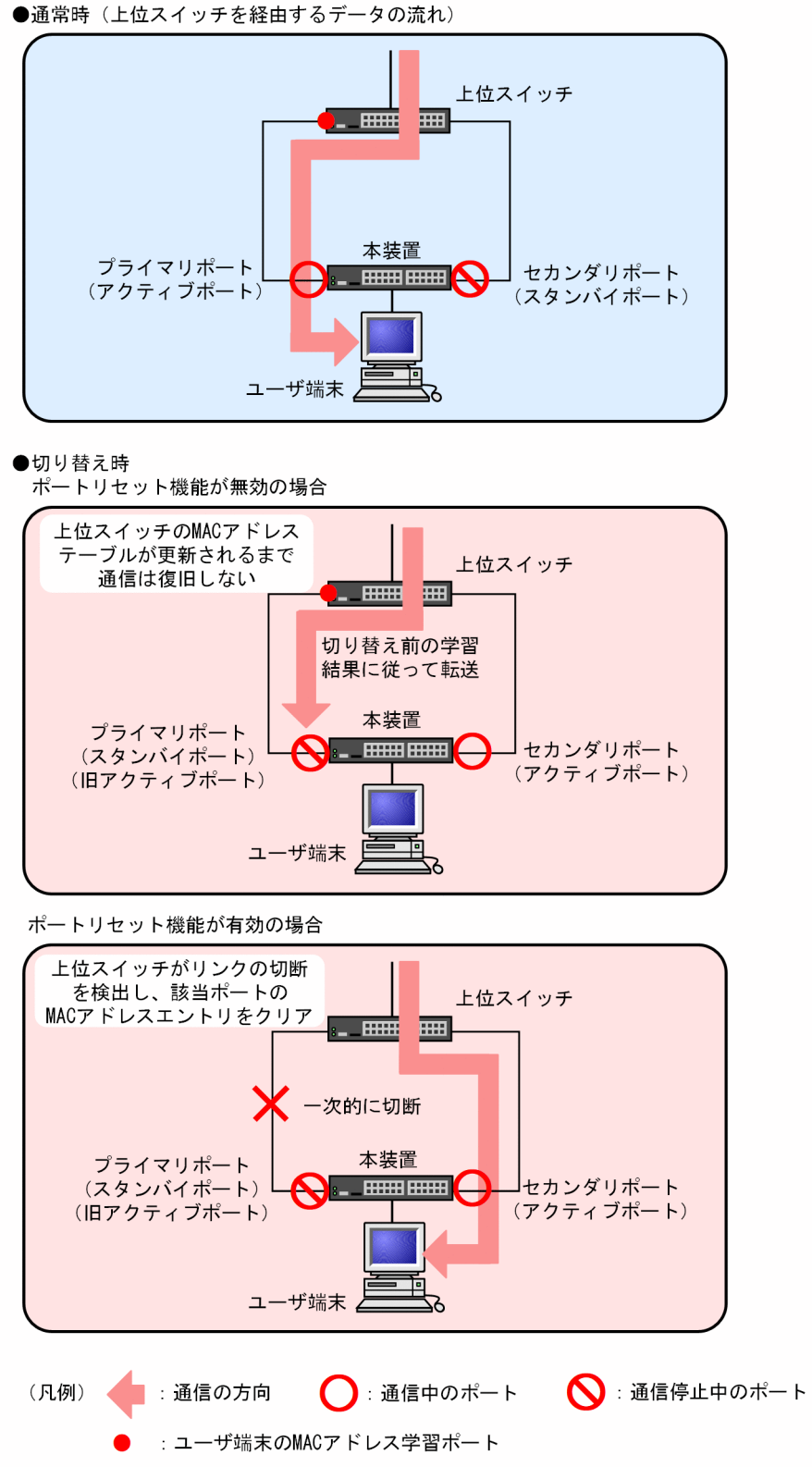
15.1.9 ポートリセット機能

(1)　動作概要

運用コマンドや自動切り戻しによって，アクティブポートを変更した場合，通信を速やかに復旧させるために，旧アクティブポートを一時的にダウンさせます。旧アクティブポートの接続先となる上位スイッチはリンクダウンを検出し，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します。

ポートリセット機能の有効／無効による切り替え動作の違いを次の図に示します。

図 15-6　ポートリセット機能の有効／無効による切り替え動作の違い



通常時

本装置のプライマリポートで通信を行っている状態では，上位スイッチはユーザ端末の MAC アドレスを，現在の通信経路で学習しています。

切り替え時（ポートリセット機能が無効）

ポートリセット機能が無効の場合，アクティブポートをセカンダリポートに切り替えても，上位スイッチがユーザ端末の MAC アドレスを以前のポートで学習しているため，該当ポート上で学習した MAC アドレスが消えるか，ユーザ端末からの通信がなければ，通信は復旧しません。

切り替え時（ポートリセット機能が有効）

ポートリセット機能が有効の場合，アクティブポートをセカンダリポートに切り替えると同時に，旧アクティブポートであるプライマリポートを一時的にダウンさせます。旧アクティブポートの接続先である上位スイッチは，リンクダウンを検出し，該当ポート上で学習した MAC アドレスを削除するため，通信を速やかに復旧できます。

15.1.10 装置起動時のアクティブポート固定機能

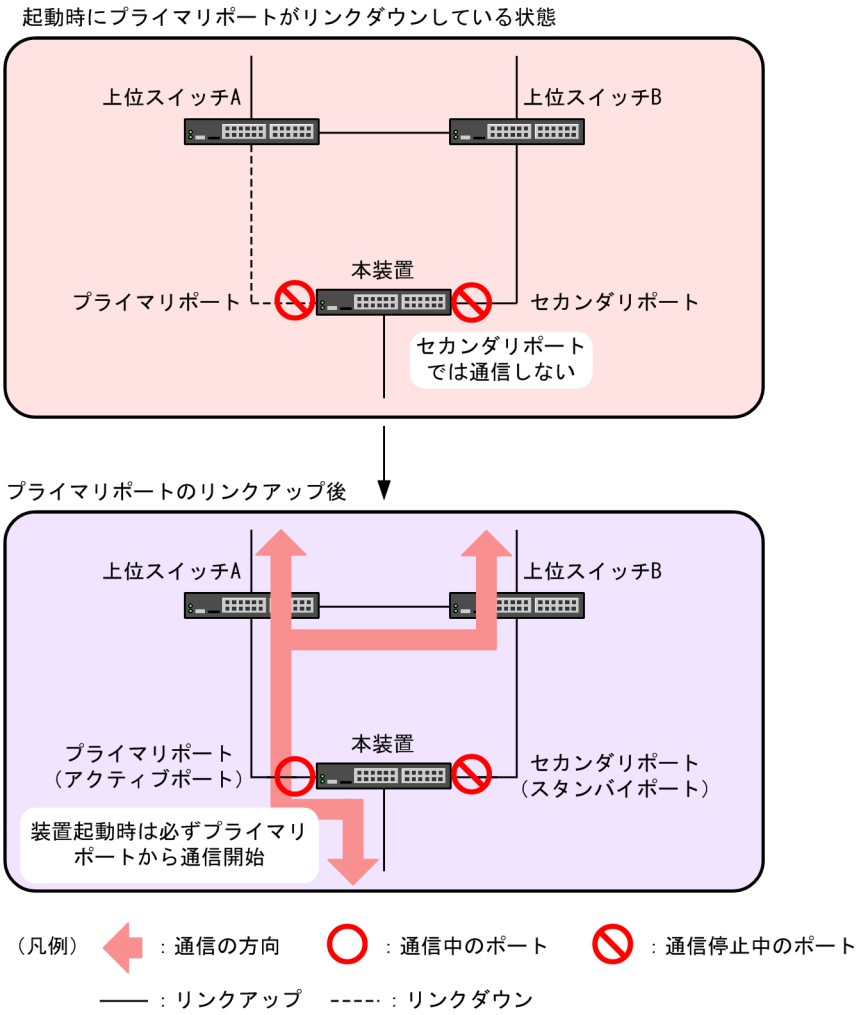
装置起動時のアクティブポート固定機能は，本装置の起動時に，必ずプライマリポートから通信を開始したい場合に利用します。この機能を有効にした装置は，起動時にセカンダリポートがリンクアップしていても，プライマリポートがリンクアップするまではアップリンクポートでの通信をしません。

アクティブポート固定機能は次に示す条件のどれかを満たすと解除されて，アクティブポートを決定します。アクティブポートが決定したあとは，通常と同じ動作となり，アクティブポートでの障害発生，または運用コマンド実行によってアクティブポートを切り替えます。

- プライマリポートがリンクアップした場合
- 運用コマンドの実行によって，セカンダリポートがアクティブポートに遷移した場合
- スタック構成時，マスタスイッチの切り替えが発生した場合

装置起動時のアクティブポート固定機能有効時の動作を次の図に示します。

図 15-7　装置起動時のアクティブポート固定機能有効時の動作



15.1.11 アップリンク・リダンダント使用時の注意事項

(1)　他機能との共存について

(a)　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」　「24.3　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。

(b)　レイヤ 2 認証との共存

「5.2.1　レイヤ 2 認証と他機能との共存」を参照してください。

(c)　冗長化構成による高信頼化機能との共存

アップリンク・リダンダントとの共存で制限のある，冗長化構成による高信頼化機能を次の表に示します。

表 15-3　アップリンク・リダンダントとの共存で制限のある機能

制限のある機能	制限の内容
GSRP aware	アップリンク・リダンダントによるブロッキング状態のポートでは，GSRP Flush request フレームを受信しません。

(2) フラッシュ制御フレーム送受信機能の使用について

上位スイッチで，アップリンク・リダンダントのフラッシュ制御フレーム受信機能をサポートしていることを確認してください。

上位スイッチが未サポートの場合，フラッシュ制御フレームを本装置から送信しても，MAC アドレステーブルがクリアされないため，通信の復旧までに時間が掛かることがあります。

(3) トランクポートでのフラッシュ制御フレーム送信設定について

トランクポートでフラッシュ制御フレームを送信する場合は，必ず送信先の VLAN を指定してください。VLAN の指定がない場合はネイティブ VLAN が存在するときだけ Untagged フレームのフラッシュ制御フレームを送信します。このとき，ネイティブ VLAN の設定がなければ，フラッシュ制御フレームは送信されません。

(4) VLAN のダウンを伴うコンフィグレーションコマンドの設定について

本装置にアップリンク・リダンダントに関するコンフィグレーションコマンドが設定されていない状態で，一つ目のアップリンク・リダンダントに関するコンフィグレーションコマンド（次に示すどれかのコマンド）を設定した場合に，すべての VLAN が一時的にダウンします。そのため，アップリンク・リダンダントを用いたネットワークを構築するときには，あらかじめ次に示すコンフィグレーションコマンドを設定しておくことを推奨します。

- switchport backup flush-request
- switchport backup interface
- switchport backup mac-address-table update exclude-vlan
- switchport backup mac-address-table update transmit

(5) ポートリセット機能を使用する場合について

アップリンクポートと対向装置との間に伝送装置などを設置した場合，対向装置で正しく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，対向装置でリンクダウンを直接検出できるようにネットワークを設計してください。

また，チャネルグループに所属する物理ポートの一部が inactive 状態でポートリセット機能が動作した場合，旧アクティブポートで該当する物理ポートが active 状態になります。

(6) スタック構成でポートリセット機能を使用する場合について

スタック構成時，ポー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，マスタスイッチの切り替えが発生すると，該当ポートがダウンしたままになることがあります。この場合，該当ポートに対して運用コマンド activate を実行してください。

(7) スタック構成で MAC アドレスアップデート機能を使用する場合について

本機能を使用する場合は，学習した MAC アドレスのエージング時間を 300 秒以上に設定してください。なお，バックアップスイッチの初期化完了後，300 秒以内にマスタスイッチの切り替えが発生した場合，本機能は正しく動作しないことがあります。

15.2 コマンドガイド

15.2.1 コマンド一覧

アップリンク・リダンダントのコンフィグレーションコマンド一覧を次の表に示します。

表 15-4　コンフィグレーションコマンド一覧

コマンド名	説明
switchport backup flush-request transmit	切り替えおよび切り戻し時に，上位スイッチに対して MAC アドレステーブルをクリアするためのフラッシュ制御フレームを送信する設定をします。
switchport backup interface	アップリンク・リダンダントのプライマリポートでセカンダリポートを指定し，アップリンクポートに設定します。また，自動切り戻し待ち時間を設定することで，自動切り戻しを有効にできます。
switchport backup mac-address-table update exclude-vlan	MAC アドレスアップデートフレームの送信時に送信対象外とする VLAN を設定します。
switchport backup mac-address-table update transmit	切り替えおよび切り戻し時に，上位スイッチに対して MAC アドレステーブルを更新するための MAC アドレスアップデートフレームを送信する設定をします。
switchport backup reset-flush-port	切り替えおよび切り戻し時に，ポートリセット機能を有効にします。
switchport backup reset-flush-time	ポートリセット機能によるポートのダウン時間を設定します。
switchport-backup startup-active-port-selection	装置起動時のアクティブポート固定機能の設定を有効にします。

アップリンク・リダンダントの運用コマンド一覧を次の表に示します。

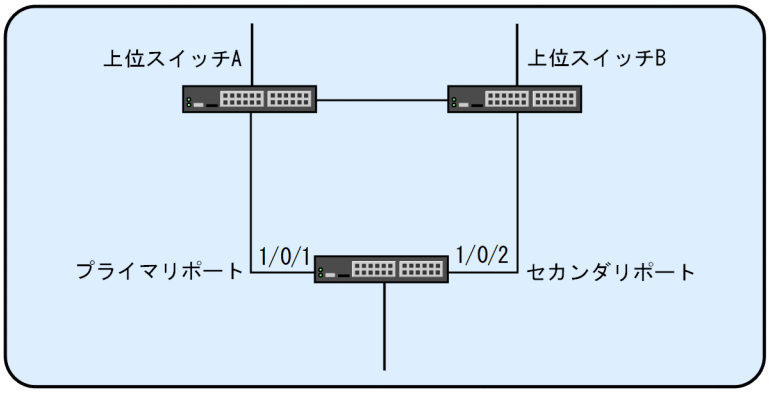
表 15-5　運用コマンド一覧

コマンド名	説明
show switchport-backup	アップリンク・リダンダントの情報を表示します。
show switchport-backup statistics	アップリンク・リダンダントの統計情報を表示します。
clear switchport-backup statistics	アップリンク・リダンダントの統計情報を削除します。
set switchport-backup active	アクティブポートを変更する場合に，新しくアクティブポートになるポートを指定します。
restart uplink-redundant	アップリンク・リダンダントプログラムを再起動します。
dump protocols uplink-redundant	アップリンク・リダンダントのダンプ情報をファイルへ出力します。

15.2.2 アップリンク・リダンダントの設定

アップリンク・リダンダントの設定例を次の図に示します。ここでは，この図を基にアップリンク・リダンダントの設定手順を説明します。

図 15-8　アップリンク・リダンダントの設定例



本装置では，ポート 1/0/1 をプライマリポートに設定し，ポート 1/0/2 をセカンダリポートに設定します。また，自動切り戻しの待ち時間を 60 秒に設定し，フラッシュ制御フレームは送信する設定にします。

(1)　アップリンク・リダンダントの設定

［設定のポイント］

ポート 1/0/1 をプライマリポート，ポート 1/0/2 をセカンダリポートとして設定し，自動切り戻しの待ち時間を 60 秒に設定します。アップリンク・リダンダントを設定するためには，事前にスパニングツリーを停止する必要があります。また，フラッシュ制御フレームを送信する設定は，プライマリポートで行う必要があります。

［コマンドによる設定］

1. `(config)# spanning-tree disable`
   スパニングツリーを停止します。
2. `(config)# interface gigabitethernet 1/0/1`
   `(config-if)# switchport backup interface gigabitethernet 1/0/2 preemption-delay 60`
   ポート 1/0/1 のコンフィグレーションモードへ移行します。
   プライマリポートになるポート 1/0/1 のコンフィグレーションモードで，セカンダリポートにするポート 1/0/2 を設定します。また，自動切り戻しの待ち時間を 60 秒に設定します。
3. `(config-if)# switchport backup flush-request transmit`
   `(config-if)# exit`
   フラッシュ制御フレームを送信する設定をします。

［注意事項］

- 本機能を設定する前は，ループ構成となります。プライマリポートまたはセカンダリポートのインタフェースを shutdown に設定するなどして，ループが発生しない状態にした上で，設定してください。
- プライマリポートをリンクアグリゲーションに設定する場合には，ポートチャネルインタフェースに設定してください。リンクアグリゲーションに設定されているポートのイーサネットインタフェースには設定できません。

15.2.3 アクティブポートの手動変更

set switchport-backup active コマンドで，アクティブポートを変更できます。

このコマンドは，指定したポートがスタンバイポートの場合だけ動作します。

図 15-9　set switchport-backup active の実行結果

```
> set switchport-backup active port 1/0/1
Are you sure to change the forwarding port to specified port? (y/n): y
>
```

15.2.4 ポートリセット機能の設定

ポートリセット機能を設定したアップリンクポートは，アクティブポートが切り替わった場合，旧アクティブポートを一時的にダウンさせます。

［設定のポイント］

ポート 1/0/1 をプライマリポート，ポート 1/0/2 をセカンダリポートとして設定した場合，ポートリセット機能はプライマリポートであるポート 1/0/1 に設定します。

また，ポートのダウン時間を 5 秒で設定します。デフォルトは 3 秒ですが，対向装置のリンクダウン検出時間（本装置のコンフィグレーションコマンド link debounce 相当を設定している場合など）よりも長く設定してください。

［コマンドによる設定］

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# switchport backup reset-flush-port
(config-if)# switchport backup reset-flush-time 5
(config-if)# exit
```
プライマリポートであるポート 1/0/1 のコンフィグレーションモードへ移行し，ポートリセット機能を設定します。また，ポートのダウン時間を 5 秒で設定します。

第6編　ネットワーク監視機能

16 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。

16.1 解説

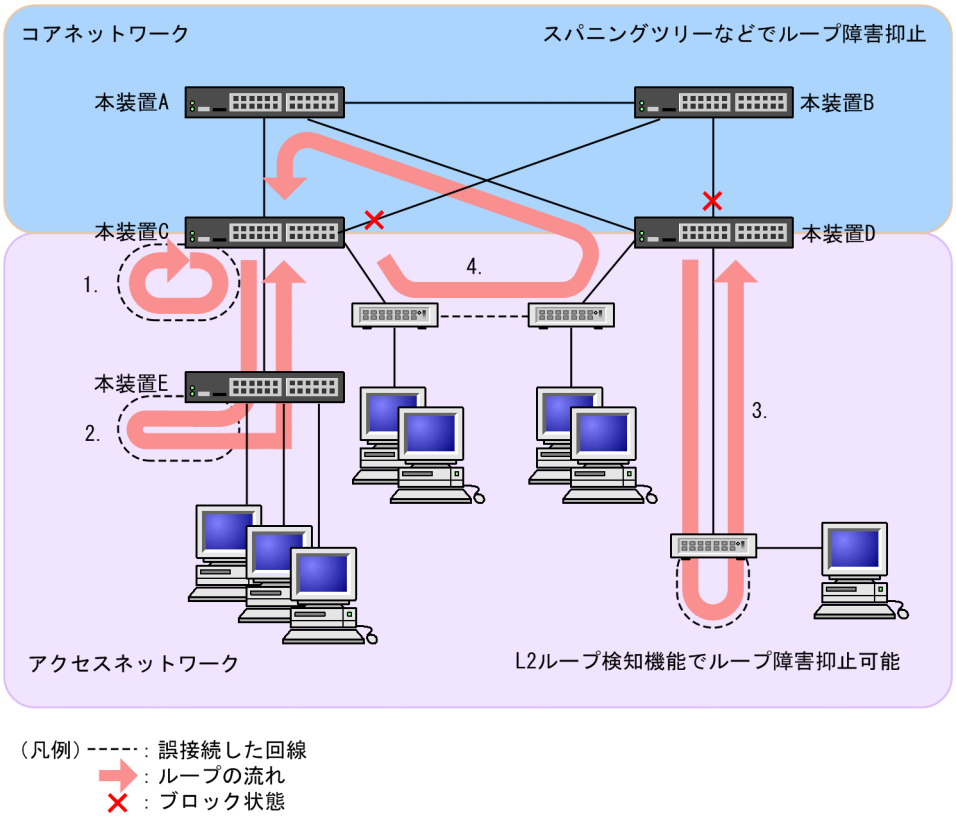
16.1.1 概要

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，原因となっている個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 16-1　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
：ブロック状態

ループ障害のパターン例

1. 本装置 C で回線を誤接続して，ループ障害が発生している。
2. 本装置 C より下位の本装置 E で回線を誤接続して，ループ障害が発生している。
3. 本装置 D より下位の装置で回線を誤接続して，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て，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。

16.1.2 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）を定期的に送信します。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 16-1　ポート種別

種別	機能
検知送信閉塞ポート	・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	・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）	・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	・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	・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て，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。詳細は，「コンフィグレーションガイド Vol.1」　「3.11.1　L2 ループ検知」を参照してください。

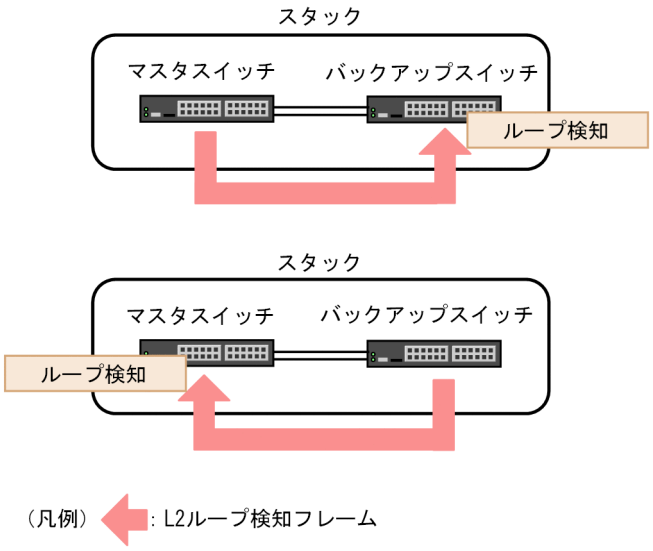
(3) ループ障害の検知方法とポートを inactive 状態にする条件

L2 ループ検知フレームを受信した場合，自装置から送信した L2 ループ検知フレームで，かつ受信ポートに設定されている VLAN であれば，異なる VLAN 間でもループ障害と見なします。L2 ループ検知フレームの受信によってループ障害と判定すると，ポートごとにフレームの受信数をカウントします。この値が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，該当ポートを inactive 状態にします。

(4)　スタック構成での L2 ループ検知動作

同一スタック内のメンバスイッチ間で送信された L2 ループ検知フレームを受信した場合でも，L2 ループ検知が動作します。スタック構成時の L2 ループ検知フレームの受信によるループ検知について次の図に示します。

図 16-2　スタック構成時の L2 ループ検知フレームの受信によるループ検知



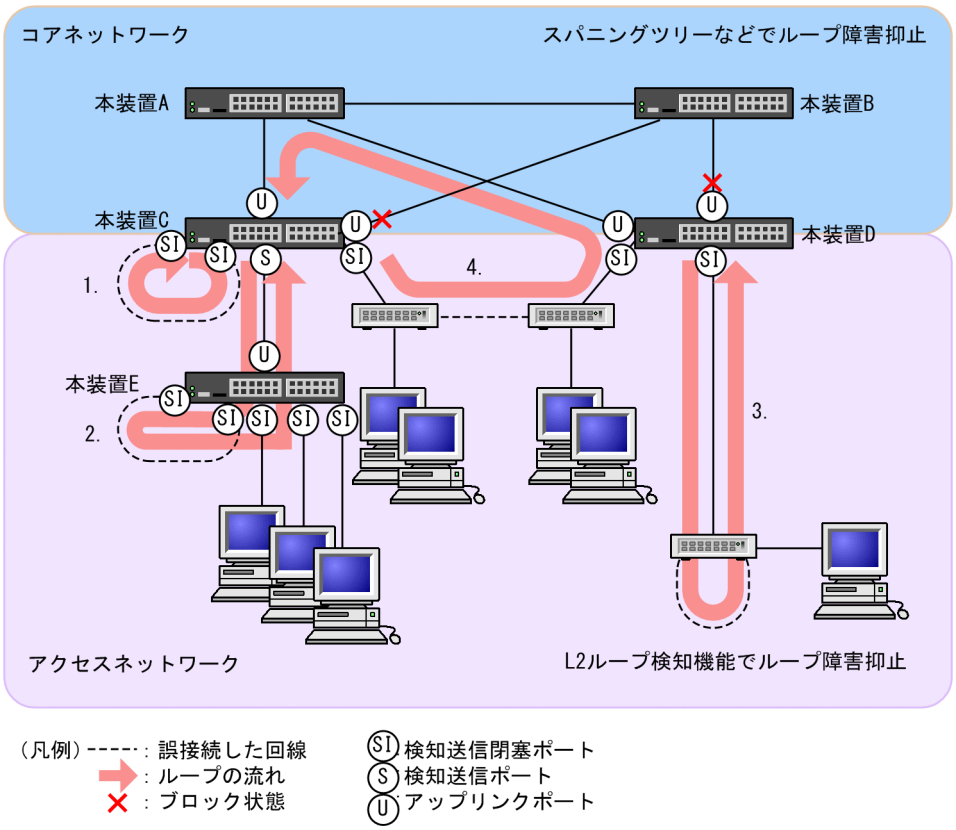
(5)　運用メッセージの表示について

ループ障害検知の運用メッセージをどこかのポートで表示し，その直後に同じポートで L2 ループ検知フレームを受信しても，前回の表示から 1 分間は運用メッセージを表示しません。前回の表示から 1 分間経過し，その後 L2 ループ検知フレームを受信したとき，ループ障害検知の運用メッセージを表示します。

16.1.3 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 16-3　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，本装置 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。

16.1.4 L2 ループ検知使用時の注意事項

(1)　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

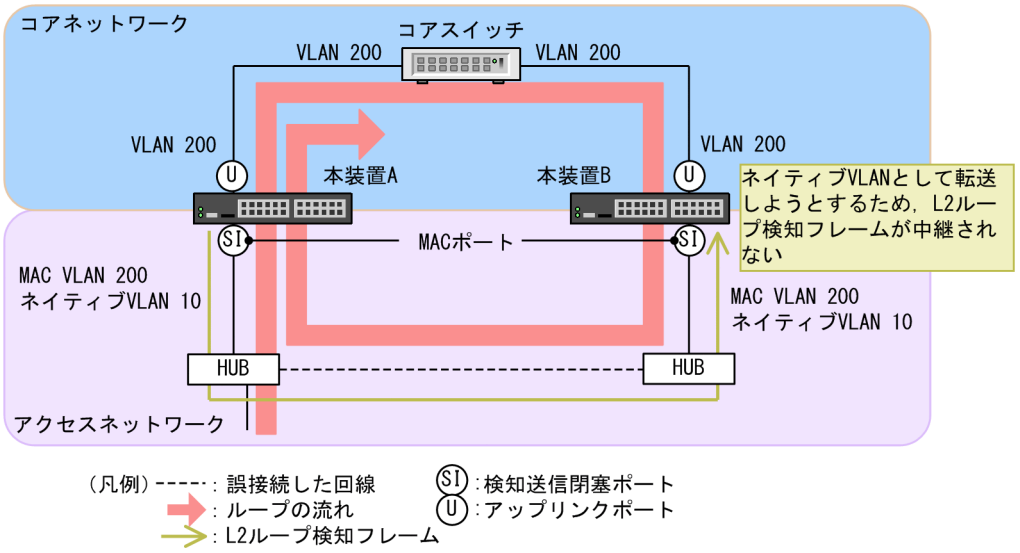
この場合は，アップリンクポートとして設定しているコアネットワーク側のポートを検知送信ポートに設定すると，ループ障害を検知できます。具体的な構成例を次に示します。

(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。

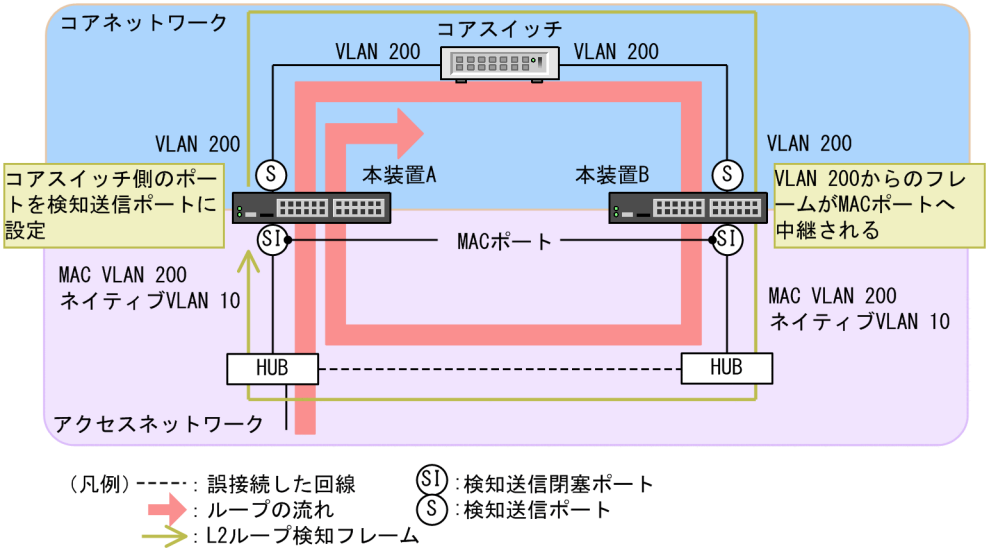
図 16-4　ループ検知の制限となる構成



(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 16-5　ループ検知可能な構成



(2)　Tag 変換使用時の動作について

次のような場合に，ループ障害を検知します。

- 自装置の Tag 変換ポートから送信した Tag 変換された L2 ループ検知フレームが，ネットワーク内で折り返り，自装置で受信した場合
- 他装置で Tag 変換された L2 ループ検知フレームを自装置で受信した場合

意図的に自装置に折り返すようなネットワーク構成にする場合は，対象ポートを検知対象外ポートに設定して，ループ障害を回避してください。

(3)　L2 ループ検知機能の動作環境について

同一ネットワーク内に L2 ループ検知未サポートの装置を配置すると，その装置でループ検知フレームを受信したときにフレームを廃棄する場合があります。その場合，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。

(4)　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

(a)　チャネルグループで使用時

チャネルグループの自動復旧機能が動作している状態で，該当チャネルグループ内のポートが 1 つでも active 状態となった場合，該当チャネルグループは復旧状態となります。そのため，該当チャネルグループで inactive 状態のままとなっているポートは，運用コマンド activate でポートを active 状態にしてください。

(b)　スタティックリンクアグリゲーションで使用時

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）すると，回線速度の変更中にループを検知して，該当チャネルグループで自動復旧機能が動作しないことがあります。
- 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。

(5)　スタック構成での自動復旧機能について

スタック構成では，自動復旧機能（inactive 状態にしたポートを自動的に active 状態にする機能）を設定していても，ループ障害の検知によってポートが inactive 状態のときにマスタスイッチが切り替わると，新しいマスタスイッチの該当するポートは inactive 状態のままです。この場合は，運用コマンド activate でポートを active 状態にしてください。

(6)　スタック構成と Ring Protocol またはスパニングツリーの併用について

スタック構成で，Ring Protocol またはスパニングツリーが有効な場合，Blocking 状態になるポートを L2 ループ検知の対象にしないでください。

16.2 コマンドガイド

16.2.1 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 16-2　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。

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 16-3　運用コマンド一覧

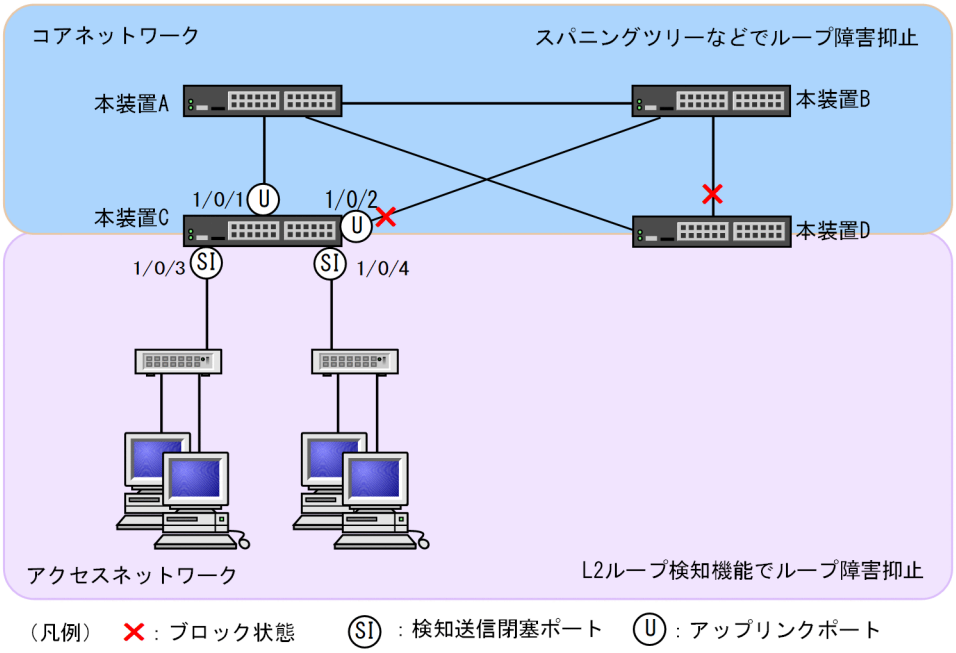
コマンド名	説明
show loop-detection	L2 ループ検知情報を表示します。
show loop-detection statistics	L2 ループ検知の統計情報を表示します。
show loop-detection logging	L2 ループ検知のログ情報を表示します。
clear loop-detection statistics	L2 ループ検知の統計情報をクリアします。
clear loop-detection logging	L2 ループ検知のログ情報をクリアします。
restart loop-detection	L2 ループ検知プログラムを再起動します。
dump 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。

16.2.2 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 1/0/1 および 1/0/2 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 1/0/3 および 1/0/4 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 16-6　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グレーションでは，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**
   本装置で L2 ループ検知機能を有効にします。
2. **(config)# interface range gigabitethernet 1/0/1-2**
   (config-if-range)# loop-detection uplink-port
   (config-if-range)# exit
   ポート 1/0/1 および 1/0/2 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 1/0/1 および 1/0/2 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 1/0/3-4**
   (config-if-range)# loop-detection send-inact-port
   (config-if-range)# exit
   ポート 1/0/3 および 1/0/4 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 1/0/3 および 1/0/4 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。

17 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。

17.1 解説

17.1.1 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になります。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，イーサネットインタフェースごとに許容する受信レート（ストーム検出閾値）を設定でき，その受信レートを超えたフラッディング対象フレームを廃棄します。ストームコントロールに指定できる対象フレームを次に示します。

表 17-1　ストームコントロールの対象フレーム

対象フレーム	説明
ブロードキャスト	ブロードキャストフレームが対象です。 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，受信レートには通常使用するフレームを考慮して余裕のある値を設定してください。
マルチキャスト	マルチキャストフレームが対象です。 マルチキャストフレームには，IP マルチキャストルーティングプロトコル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，受信レートには通常使用するフレームを考慮して余裕のある値を設定してください。
ユニキャスト	MAC アドレステーブルに宛先 MAC アドレスが登録されていないためにフラッディングされるユニキャストフレームが対象です。 受信レートには通常使用するフレームを考慮して余裕のある値を設定してください。

さらに，ストームを検出・回復した場合の設定できる動作を次に示します。

表 17-2　ストームコントロール検出・回復時の動作

動作	説明
SNMP 通知の送信	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，プライベートの SNMP 通知を送信します。
運用メッセージの出力	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，運用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。
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，またはポート閉塞時の自動復旧を設定する必要があります。
流量制限	ストームを検出したとき，自動でトラフィックを制限します。詳細は「17.1.2　流量制限」を参照してください。

17.1.2 流量制限

本機能は，ストーム検出時に本装置が自動でトラフィック停止または流量制限を行い，加えて，一定の監視条件を基に自動で制限を解除できます。

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 1 秒間の受信フレーム数がストーム検出閾値（上限閾値）を超えた場合，トラフィックを流量制限値（下限閾値）に制限します。流量制限値を 0 に指定すればストーム検出後のトラフィックを停止できます。

また，ストーム回復閾値以下の値を，指定した時間（流量制限解除監視時間）以上継続した場合，自動的に流量の制限を解除します。流量制限解除後は，ストーム回復閾値でストームを監視します。

流量制限動作を次の図に示します。

図 17-1　流量制限の動作

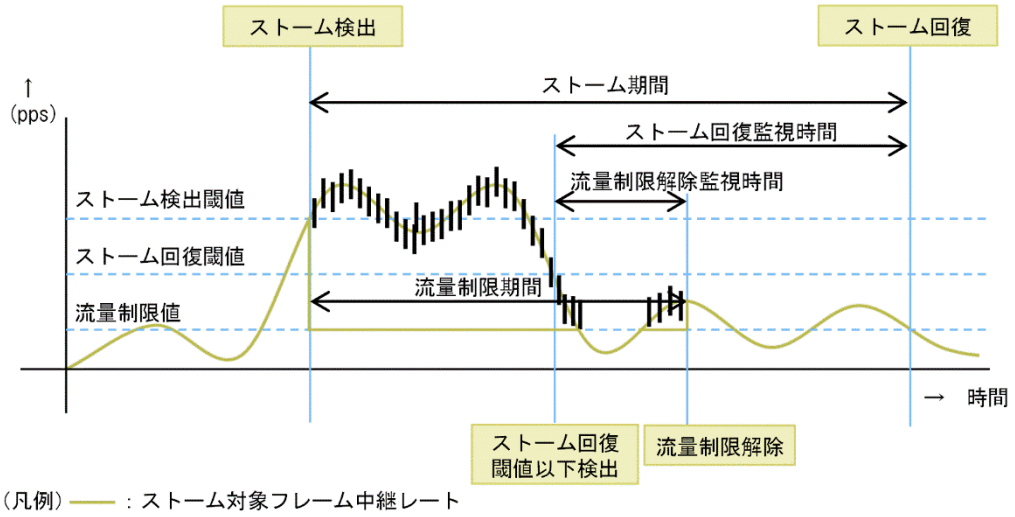


表 17-3　流量制限の説明

項目	説明
ストーム検出	ストームを検出した時点です。 流量制限を設定している場合，流量制限を開始します。
ストーム回復	ストームが回復と判断した時点です。
ストーム期間	ストームを検出してから回復と判断するまでの期間です。
ストーム検出閾値（上限閾値）	ストームを検出する閾値です。 コンフィグレーションで指定した閾値（ストーム検出閾値）を超えたとき，ストームを検出し超過分を廃棄します。
ストーム回復閾値	ストームの回復を判断する閾値です。 コンフィグレーションで指定した閾値（ストーム回復閾値）をストーム回復監視時間下回ったとき，ストームが回復したと判断します。 ストーム回復閾値の指定がない場合は，「ストーム検出閾値＝ストーム回復閾値」として動作します。
流量制限値（下限閾値）	ストームを検出したとき，トラフィック量を制限する閾値です。 コンフィグレーションで指定した閾値（流量制限値）に流量を制限します。
流量制限期間	流量制限を行う期間です。
ストーム回復監視時間	ストームが回復したと判断するまでの期間です。 ストーム回復閾値以下の値がコンフィグレーションで指定した時間（ストーム回復監視時間）以上継続したとき，ストームが回復したと判断します。
流量制限解除監視時間	流量制限の解除を判断するための期間です。 ストーム回復閾値以下の値がコンフィグレーションで指定した時間（流量制限解除監視時間）以上継続したとき，流量制限を解除します。

17.1.3 ポート閉塞時の自動復旧

ストーム検出により閉塞したポートは，設定した時間の経過後に，自動で閉塞を解除できます。

また，チャネルグループ内のポートが閉塞した場合，復旧時は，チャネルグループに所属するすべてのポートに対して自動で閉塞を解除します。

17.1.4 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，1 秒間に受信したフレーム数が，コンフィグレーションで設定した受信レートを超えたときに，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，1 秒間に受信したフレーム数が受信レート以下の状態がコンフィグレーションで指定した時間（ストーム回復監視時間）続いたときに，ストームが回復したと判定します。

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を閉塞した場合は，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後に activate コマンドを使用して active 状態にしてください。または，ポート閉塞時の自動復旧を設定することでポートを自動で active 状態にできます。

(2) ストームの検出閾値と中継動作について

ストーム検出閾値を小さい値で指定した場合，ストーム検出後の数秒間は閾値以上のフレームを中継することがあります。その後は閾値を超えたフレームを廃棄します。

例：閾値を 125pps で指定した場合

- 閾値に対して 200％のフレームを受信時：最大約 1 秒間，125pps×200％中継
- 閾値に対して 110％のフレームを受信時：最大約 6 秒間，125pps×110％中継

(3) ストームの検出時の統計クリア

ストーム検出時に実行する動作は，指定した受信レートを 1 秒間に受信したフレーム数が超過した場合に動作します。ストーム検出時に運用コマンド clear storm-control で統計をクリアすると，正しく動作しないことがあります。

17.2 コマンドガイド

17.2.1 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 17-4　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	ストームコントロールの閾値を設定します。また，ストームを検出・回復した場合の動作を設定できます。

ストームコントロールの運用コマンド一覧を次の表に示します。

表 17-5　運用コマンド一覧

コマンド名	説明
show storm-control	ストームコントロール情報を表示します。
clear storm-control	ストームコントロール情報の統計カウンタを 0 クリアします。

17.2.2 ストームコントロールの設定

フレーム種別ごとにストームの検出，および検出・回復したときの動作を設定します。

［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。

ストームが発生したとき，SNMP 通知を送信および運用メッセージを出力します。

［コマンドによる設定］

1. (config)# interface gigabitethernet 1/0/10
   (config-if)# storm-control broadcast level pps 250
   ブロードキャストフレームのストーム検出閾値を 250pps に設定します。
2. (config-if)# storm-control multicast level pps 500
   マルチキャストフレームのストーム検出閾値を 500pps に設定します。
3. (config-if)# storm-control unicast level pps 1000
   ユニキャストフレームのストーム検出閾値を 1000pps に設定します。
4. (config-if)# storm-control action trap
   ストームの検出および回復を検知したときに，プライベートの SNMP 通知を送信します。
5. (config-if)# storm-control action log
   ストームの検出および回復を検知したときに，運用メッセージを出力します。

17.2.3 流量制限の設定

ストーム検出時，フレーム種別ごとに指定した閾値までトラフィックを制限します。

［設定のポイント］

ストーム検出閾値とストーム回復閾値，および流量制限値，加えてストーム検出の動作に流量制限を設定します。流量制限を設定した場合，ストーム検出時の動作として，ポートの閉塞は設定できません。

また，ストーム回復閾値以内に戻ったとき，自動的に流量制限を解除する流量制限解除監視時間を設定します。流量制限解除監視時間は，ストーム回復監視時間以内を設定してください。

［コマンドによる設定］

1. (config)# interface gigabitethernet 1/0/20
   (config-if)# storm-control broadcast level pps 500 250
   ポート 1/0/20 に，ブロードキャストフレームのストーム検出閾値を 500pps に，ストーム回復閾値を 250pps に設定します。
2. (config-if)# storm-control multicast level pps 750 500
   マルチキャストフレームのストーム検出閾値を 750pps に，ストーム回復閾値を 500pps に設定します。
3. (config-if)# storm-control unicast level pps 1000 750
   ユニキャストフレームのストーム検出閾値を 1000pps に，ストーム回復閾値を 750pps に設定します。
4. (config-if)# storm-control action filter
   ストームを検出したときに，流量制限が動作するように設定します。
5. (config-if)# storm-control filter-broadcast 125
   ブロードキャストフレームの流量制限値を 125pps に設定します。
6. (config-if)# storm-control filter-multicast 250
   マルチキャストフレームの流量制限値を 250pps に設定します。
7. (config-if)# storm-control filter-unicast 500
   ユニキャストフレームの流量制限値を 500pps に設定します。
8. (config-if)# storm-control filter-recovery-time 15
   流量制限解除監視時間を 15 秒に設定します。

17.2.4 ポート閉塞時の自動復旧の設定

ストーム検出により閉塞したポートで，時間経過により自動でポートの閉塞解除をします。

［設定のポイント］

ストーム検出をしたときの動作としてポートの閉塞を設定し，自動的にポートの閉塞解除をするまでの時間を設定します。

［コマンドによる設定］

1. (config)# interface gigabitethernet 1/0/5
   (config-if)# storm-control unicast level pps 500
   ユニキャストフレームのストーム検出閾値を 500pps に設定します。
2. (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。
3. (config-if)# storm-control auto-restore-time 300
   閉塞したポートを，自動的に active 状態にする時間として 300 秒を設定します。

第7編　ネットワークの管理

18 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。

18.1 解説

18.1.1 ポートミラーリングの概要

ポートミラーリングは，指定した物理ポートで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**，コピーされたフレームのことを**ミラーリングフレーム**と呼びます。この機能を利用して，ミラーリング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を行えます。

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 18-1　受信フレームのミラーリング

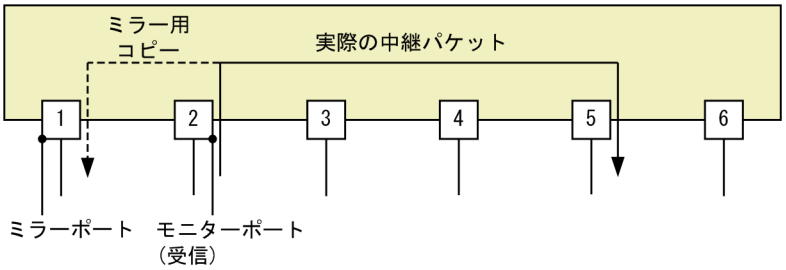
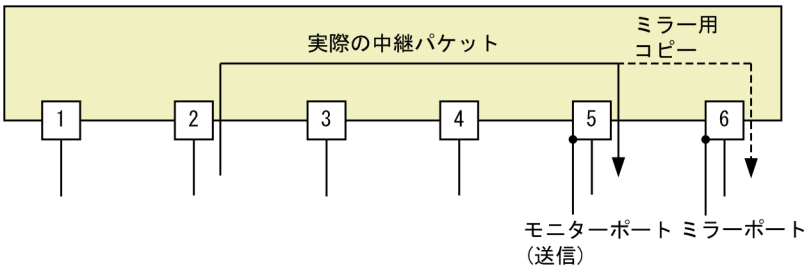


図 18-2　送信フレームのミラーリング



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。

18.1.2 ポートミラーリングの動作仕様

(1)　基本動作

本装置のポートミラーリングは，トラフィックを監視するポートをモニターポートとして設定します。また，ミラーリングフレームの送信先ポートをミラーポートとして設定します。ミラーポートは，ミラーリング専用のポートになります。

(2)　モニターセッション

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**と呼びます。モニターセッションでは，モニター対象フレーム，モニターポート，ミラーポートを指定できます。モニター対象フレームは，受信フレーム，送信フレーム，または送受信フレームの 3 種類からどれかを選択します。

本装置では，最大四つのモニターセッションを設定できます。

各モニターセッションでは，モニターポートとミラーポートを「多対一」で設定できます。こうすると，複数のモニターポートで送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。ミラーポートにはポートチャネルインタフェースも設定でき，一つまたは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，ポートチャネルインタフェースへ送信できます。

また，モニターポートとミラーポートは，速度や回線種別が異なる場合でもミラーリングできます。一つのモニターセッションでモニターポートを複数指定する場合には，速度や回線種別が異なるモニターポートでも同時に指定できます。ただし，ミラーリングフレームは，ミラーポートの回線帯域以下で送信するため，ミラーリングフレームの量がミラーポートの帯域を超えると，ミラーリングフレームを廃棄することがあります。

(3) モニターポート

モニターポートには，次に示すポート以外のイーサネットインタフェースを指定できます。モニターポートに指定しても，ポートやインタフェースの各機能に対する制限はありません。

- ミラーポートとして設定したポート
- ほかのモニターセッションのモニターポートに指定されたポート

(4) ミラーポート

ミラーリングフレームを送信したいポートをミラーポートに設定します。ミラーポートはミラーリング専用のポートです。ミラーポートでの各機能について次に示します。

- VLAN 機能およびレイヤ 3 通信機能を使用できません。このため，VLAN 機能を前提とするスパニングツリー，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を送信する機能を設定すると，ミラーポートにはミラーリングフレームのほかに，設定した機能の制御フレームを送信します。
- ミラーポートに送信側フィルタを設定すると，ミラーリングフレームもフィルタの対象となります。このため，フィルタで廃棄を設定することで，ポート単位でミラーリングするとき，ミラーリングフレームから必要なフレームだけを送信できます。
- QoS の送信制御は，ミラーポートでも動作します。このため，ミラーリングフレームが廃棄されて，ミラーポートから送信されないことがあります。詳細は，「4　送信制御」を参照してください。
- アップリンク・リダンダントのアップリンクポートとして使用し，スタンバイポートの状態のポートに対してミラーポートを設定した場合にも，ミラーリングフレームは送信されます。
- リンクアグリゲーションの非リンクダウンモードによってスタンバイリンクの状態のポートに対して，802.1Q Tag 付与機能を使用したミラーポートを設定した場合にも，ミラーリングフレームは送信されます。

(5) 受信フレームのミラーリング

モニター対象フレームとして送受信フレームまたは受信フレームを指定すると，受信フレームをミラーリングできます。このとき，モニターポートで受信するすべてのフレームが，ミラーリングの対象となります。

そのため，モニターポートに設定した受信フィルタまたはストームコントロールによってモニターポートで廃棄となったフレームは，中継はしませんがミラーリングの対象となります。ただし，フレームを受信したときにイーサネットインタフェースでエラーフレームとして廃棄したフレームは，ミラーリングしません。

(6) 送信フレームのミラーリング

モニター対象フレームとして送受信フレームまたは送信フレームを指定すると，送信フレームをミラーリングできます。ミラーリング対象フレームおよび条件ごとの動作は次のとおりです。

- モニターポートで送受信する制御フレームもミラーリングします。
- モニターポートで Tag 変換を使用している場合，モニターポートで送信する VLAN の VLAN ID を付けた Tagged フレームとしてミラーリングします。

- ミラーリングフレームの TPID は，モニターポートの TPID になります。
- モニターポートで QoS の送信制御によって廃棄したフレームは，ミラーリングしません。
- 送信側フィルタで廃棄を設定している場合，廃棄対象フレームのミラーリングは次のとおりになります。
  - イーサネットインタフェースに設定した場合，モニターポートでフィルタによって廃棄したフレームもミラーリング対象となり，ミラーポートから送信されます。
  - モニターポートが所属する VLAN インタフェースに設定した場合，モニターポートでフィルタによって廃棄したフレームはミラーポートから送信されません。

18.1.3 802.1Q Tag 付与機能

802.1Q Tag 付与機能は，ミラーリングフレームに VLAN Tag を付ける機能です。この機能を利用することで，ミラーリングフレームは，付けた VLAN Tag に基づいてレイヤ 2 中継ができ，離れた場所にあるアナライザなどのトラフィック監視装置まで転送できます。ただし，ミラーリングフレームの MAC アドレスは，モニターポートで受信したフレームの MAC アドレスをそのまま使用するため，ミラーリングフレームを中継する装置では，実際のネットワーク構成と異なる MAC アドレスのフレームを受信することになります。そのため，中継に使用する VLAN（ミラーリングフレームに付けた VLAN Tag）では MAC アドレス学習を抑止してください。

ミラーポートとして設定してもこの機能を使用する場合は，プロトコル VLAN および MAC VLAN の機能以外を使用できます。

802.1Q Tag 付与機能がフレームに付ける VLAN Tag のフィールドについて次の表に示します。

表 18-1　802.1Q Tag 付与機能がフレームに付ける VLAN Tag のフィールド

フィールド	説明	サポート内容
TPID	IEEE802.1Q VLAN Tag が続くことを示す EtherType 値	コンフィグレーションで設定した値になります。装置で 1 種類だけ指定できます。
User Priority	IEEE802.1D のプライオリティ	本機能ではデフォルト（3）だけをサポートします。
CF（Canonical Format）	MAC ヘッダ内の MAC アドレスが標準フォーマットに従っているかどうか	本機能では標準（0）だけをサポートします。
VLAN ID	VLAN ID	ユーザが使用できる VLAN ID は 2～4094 です。装置で 1 種類だけ指定できます。

18.1.4 ポートミラーリング使用時の注意事項

(1)　送信フレームをミラーリングの対象とする場合の注意事項

ミラーポートから送信されるフレームの順序は，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ことがあります。

(2)　ポートミラーリング 802.1Q Tag 付与機能使用時の注意事項

- VLAN Tag が付くため，通常より 4 バイト大きいサイズのフレームを扱える必要があります。特に，Tagged フレームおよび送信フレームをミラーリングする場合，ミラーリングフレームは VLAN Tag が 2 段になるため，8 バイト大きいサイズのフレームを扱える必要があります。
- ミラーポートとして設定するポートには，トランクポートを接続してください。
- ミラーリングフレームは，ミラーポートに設定されたレイヤ 2 スイッチ機能の通信状態に関係なく送信

されます。

- モニターポートでミラーリングするパケットの VLAN Tag 内の TPID 値と，ミラーポートに設定している TPID 値が異なる場合，次のような設定パターンのときは，ミラーポートで付与する VLAN Tag を除いた 1 段目の VLAN Tag の TPID 値が，モニターポートの TPID 値ではなく，ミラーポートの TPID 値となります。
  - ミラーポートとモニターポートを異なるメンバスイッチに設定
  - AX2630S-48T4XW または AX2630S-48P4XW で，モニターポートとミラーポートが，ポート 1～24，49～50 のどれかと，ポート 25～48，51～54 のどれかにわたって設定

(3)　sFlow 統計と併用する場合の注意事項

同一ポートで，次の併用はしないでください。

- sFlow 統計の送信（egress）指定と，送信フレームを対象とするモニターポートの併用。
- sFlow 統計の送信（egress）指定と，802.1Q Tag 付与機能を使用したミラーポートの併用。

(4)　ポリシーベースミラーリングと併用する場合の注意事項

- ポリシーベースミラーリングで使用しているモニターセッション番号は使用できません。
- ポリシーベースミラーリングでミラーポートとして使用しているポートは，ミラーポートとして設定できません。
- 同一フレームがポリシーベースミラーリングと受信側ポートミラーリングの対象となった場合，各機能で使用しているモニターセッション番号の数の大きい方で設定しているミラーポートへだけミラーリングします。

18.2 コマンドガイド

18.2.1 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 18-2　コンフィグレーションコマンド一覧

コマンド名	説明
monitor session	ポートミラーリングを設定します。

18.2.2 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。

組み合わせごとに 1 から 4 のセッション番号を使用します。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。

(1)　1 モニターポート対 1 ミラーポートの設定

［設定のポイント］

モニターポートに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 1/0/1 rx destination interface gigabitethernet 1/0/5
   アナライザをポート 1/0/5 に接続し，ギガビットイーサネットインタフェース 1/0/1 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。

(2)　複数モニターポートのミラーリング

［設定のポイント］

複数のモニターポートをリスト形式で設定できます。設定済みのリストにポートを追加することや，削除することもできます。

［コマンドによる設定］

1. (config)# monitor session 1 source interface gigabitethernet 1/0/1-23, tengigabitethernet 1/0/25 both destination interface gigabitethernet 1/0/24
   アナライザをポート 1/0/24 に接続し，ギガビットイーサネットインタフェース 1/0/1 から 1/0/23 および 10 ギガビットイーサネットインタフェース 1/0/25 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。

(3)　ミラーポート（ポートチャネルインタフェース）へのミラーリング

［設定のポイント］

ミラーポートにチャネルグループを設定できます。

［コマンドによる設定］

1. (config)# monitor session 1 source interface gigabitethernet 1/0/1-23 both destination interface channel-group 10
   アナライザをチャネルグループ 10 に接続し，ギガビットイーサネットインタフェース 1/0/1 から 1/0/23 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。

18.2.3 802.1Q Tag 付与機能の設定

ミラーポートに 802.1Q Tag 付与機能を使用してミラーリングフレームをレイヤ 2 中継するポートを指定します。

［設定のポイント］

モニターポートに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。

なお，Tagged フレームや送信フレームをミラーリングする場合は，VLAN Tag が 2 段となるため，8 バイト大きいサイズのフレームを扱うこととなります。そのため，mtu コマンドで MTU 長を変更する必要があります。

［コマンドによる設定］

1. (config)# monitor session 1 source interface gigabitethernet 1/0/1 both destination interface gigabitethernet 1/0/2 encapsulation dot1q 10 ethertype 9100
   ギガビットイーサネットインタフェース 1/0/1 で送受信するフレームをミラーリングし，ミラーリングフレームに VLAN 10，TPID 0x9100 の VLAN Tag を付けてポート 1/0/2 から送信することを設定します。

19 ポリシーベースミラーリング

ポリシーベースミラーリングは，受信するフレームから特定のフローをコピーして，指定したインタフェースへ送信する機能です。この章では，ポリシーベースミラーリングの解説と操作方法について説明します。

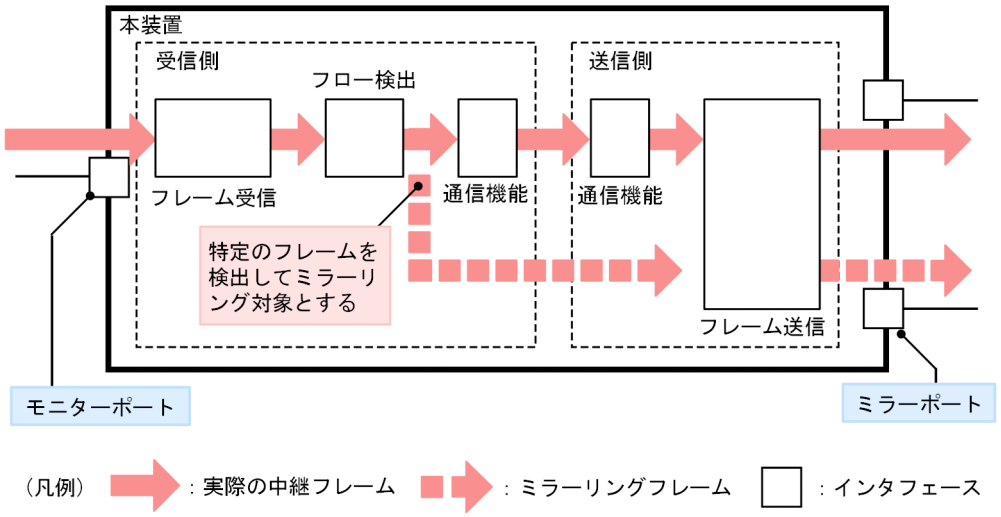
19.1 解説

19.1.1 概要

ポリシーベースミラーリングは，受信するフレームから特定のフローをコピーして，指定したインタフェース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**，コピーされたフレームのことを**ミラーリングフレーム**と呼びます。この機能を利用して，フロー単位のミラーリング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。

受信フレームに対するミラーリングの動作を次の図に示します。

図 19-1　受信フレームのミラーリング



図で示すとおり，トラフィックを監視するインタフェースを**モニターポート**と呼び，ミラーリングフレームの送信先となるインタフェースを**ミラーポート**と呼びます。

本装置のポリシーベースミラーリングは，フロー検出によって細かくフレームを特定できます。

19.1.2 ポリシーベースミラーリングの動作仕様

(1)　基本仕様

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ミラーポートに設定します。ミラーポートは，ミラーリング専用のポートになります。

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**と呼びます。本装置では，複数のモニターセッションを設定できます。また，モニターポートの受信フレームは，それぞれ異なるミラーポートへ送信できます。

モニターポートとミラーポートは，次に示す組み合わせで使用できます。

- 1 モニターポート対 1 ミラーポート
- 複数モニターポート対 1 ミラーポート

モニターポートおよびミラーポートには，それぞれ異なる速度のポートを設定できます。なお，ミラーリングしたフレームは，ミラーポートの回線帯域内で送信するため，回線帯域を超えるフレームは廃棄します。

(2)　モニターポート

ポリシーベースミラーリングのモニターポートは，対象とするフローを特定するアクセスリストを使用し

て設定します。モニターポートを設定する場合は，受信側のフロー検出モードを，ポリシーベースミラーリング対応のモード（layer-2-1-mirror または layer2-2-mirror）に設定してください。

ポリシーベースミラーリングの送信先インタフェースリストを動作に指定したアクセスリストをインタフェースに適用することで，該当するインタフェースをモニターポートとして使用します。アクセスリストをインタフェースに適用するときに指定する，コンフィグレーションコマンドのパラメータを次の表に示します。

表 19-1 アクセスリスト適用時に指定するパラメータ

ミラーリング方向	パラメータ
受信側	in-mirror

なお，対象インタフェース，フロー検出条件，注意事項などについては，「1 フィルタ」を参照してください。

(3) ミラーポート

ポリシーベースミラーリングのミラーポートは，送信先インタフェースリストで設定します。

送信先インタフェースリストには，次のどちらか一つのインタフェースを指定できます。

- 物理ポートインタフェース
- ポートチャネルインタフェース

ミラーポートでの各機能について次に示します。

- VLAN 機能を使用できません。このため，VLAN 機能を前提とする機能も使用できません。
- ミラーポートに制御フレームを送信する機能を設定すると，ミラーポートにはミラーリングフレームのほかに，設定した機能の制御フレームを送信します。
- ミラーポートに送信側フィルタを設定すると，ミラーリングフレームもフィルタの対象となります。このため，フィルタで廃棄を設定した場合，ミラーリングフレームはミラーポートで廃棄されます。
- アップリンク・リダンダントのアップリンクポートとして使用し，スタンバイポートの状態のポートに対してミラーポートを設定した場合にも，ミラーリングフレームは送信されます。

(4) 受信フレームのミラーリング

- モニターポートで受信するフレームのうち，ポリシーベースミラーリングを指定したアクセスリストでフローを検出したフレームがミラーリングの対象となります。ただし，次のように廃棄したフレームはミラーリングしません。
  - 受信したイーサネットインタフェースでエラーフレームとして廃棄
  - IEEE802.1X または Web 認証を使用時に未認証による廃棄
  - 認証専用 IPv4 アクセスリストによる廃棄
  - DHCP snooping の端末フィルタによる廃棄
- モニターポートに設定した受信フィルタ，またはストームコントロールによってモニターポートで廃棄となったフレームは，中継はしませんがミラーリングの対象となります。

19.1.3 ポリシーベースミラーリング使用時の注意事項

(1) ポートミラーリングとの共存

- ポートミラーリングで使用しているモニターセッション番号は，ポリシーベースミラーリングでは設定できません。
- 同一フレームがポリシーベースミラーリングと受信側ポートミラーリングの対象となった場合，各機能

で使用しているモニターセッション番号の数の大きい方で設定しているミラーポートへだけミラーリングします。

(2)　ポリシーベースミラーリング使用時の注意事項

VLAN インタフェースに送信側フィルタを設定すると，ミラーリングしたフレームの VLAN ID が一致したときにも有効となります。フィルタで廃棄を設定した場合，ミラーリングしたフレームは廃棄されます。

19.2 コマンドガイド

19.2.1 コマンド一覧

ポリシーベース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 19-2　コンフィグレーションコマンド一覧

コマンド名	説明
destination session	ポリシーベースミラーリングのミラーポートを設定します。
destination-interface-list	ポリシーベースミラーリングの送信先インタフェースリストを設定します。
flow detection mode※1	受信側のフロー検出モードを設定します。
ip access-group※2	インタフェースに対して，ポリシーベースミラーリングの対象フレームを検出する IPv4 パケットフィルタを適用します。
ip access-list extended※2	ポリシーベースミラーリングの対象フレームを IPv4 パケットフィルタで検出するアクセスリストを設定します。
mac access-group※2	インタフェースに対して，ポリシーベースミラーリングの対象フレームを検出する MAC フィルタを適用します。
mac access-list extended※2	ポリシーベースミラーリングの対象フレームを MAC フィルタで検出するアクセスリストを設定します。
permit※2	対象パケットを検出するフロー検出条件と，対象フレームのミラーリング先となる送信先インタフェースリストを，アクセスリストに指定します。

注※1

「コンフィグレーションコマンドレファレンス」　「27　フロー検出モード/フロー動作」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」　「28　アクセスリスト」を参照してください。

ポリシーベースミラーリングの運用コマンド一覧を次の表に示します。

表 19-3　運用コマンド一覧

コマンド名	説明
show access-filter※	ポリシーベースミラーリングの送信先インタフェースリストを動作に指定したアクセスリストの設定内容と統計情報を表示します。
clear access-filter※	ポリシーベースミラーリングの送信先インタフェースリストを動作に指定したアクセスリストの統計情報を 0 クリアします。

注※

「運用コマンドコマンドレファレンス」　「31　フィルタ」を参照してください。

19.2.2 ポリシーベースミラーリングの設定

ポリシーベースミラーリングの対象フレーム，および対象フレームのミラーリング先となる送信先インタフェースリストは，アクセスリストで指定します。送信先のインタフェースは，送信先インタフェースリストで設定します。

なお，ポリシーベースミラーリングを使用する場合は，受信側のフロー検出モードをポリシーベースミラーリング対応のモードに設定してください。

(1) 1モニターポート対1ミラーポートの設定

1モニターポート対1ミラーポートで動作させる場合の例を次に示します。この例では，アナライザをイーサネットインタフェース 1/0/10 に接続します。

［設定のポイント］

ミラーポートには，送信先インタフェースリストを設定します。モニターポートには，送信先インタフェースリストを動作に指定したアクセスリストをポリシーベースミラーリングとして設定します。

［コマンドによる設定］

1. (config)# destination-interface-list MIRROR-LIST-A mode mirror
   (config-dest-mirror)# destination session 1 interface gigabitethernet 1/0/10
   (config-dest-mirror)# exit
   送信先インタフェースリスト（MIRROR-LIST-A）に，イーサネットインタフェース 1/0/10 をミラーポートとして設定します。
2. (config)# mac access-list extended MIRROR-A
   (config-ext-macl)# permit any any vlan 100 action policy-mirror-list MIRROR-LIST-A
   (config-ext-macl)# exit
   MAC アクセスリスト（MIRROR-A）を作成して，VLAN 100 のパケットに対して送信先インタフェースリスト（MIRROR-LIST-A）を設定します。
3. (config)# interface gigabitethernet 1/0/1
   (config-if)# mac access-group MIRROR-A in-mirror
   (config-if)# exit
   イーサネットインタフェース 1/0/1 の受信側に，MAC アクセスリスト（MIRROR-A）をポリシーベースミラーリングとして適用します。

(2) 複数モニターポートのミラーリング

複数モニターポートからミラーリングさせる場合の例を次に示します。この例では，アナライザをイーサネットインタフェース 1/0/10 に接続します。

［設定のポイント］

送信先インタフェースリストを動作に指定したアクセスリストを，ポリシーベースミラーリングとして複数のモニターポートに設定します。

［コマンドによる設定］

1. (config)# destination-interface-list MIRROR-LIST-B mode mirror
   (config-dest-mirror)# destination session 1 interface gigabitethernet 1/0/10
   (config-dest-mirror)# exit
   送信先インタフェースリスト（MIRROR-LIST-B）に，イーサネットインタフェース 1/0/10 をミラーポートとして設定します。
2. (config)# ip access-list extended MIRROR-B
   (config-ext-nacl)# permit udp any any action policy-mirror-list MIRROR-LIST-B
   (config-ext-nacl)# exit
   IPv4 アクセスリスト（IPv4-MIRROR-B）を作成して，IPv4 パケットに対して送信先インタフェースリスト（MIRROR-LIST-B）を設定します。
3. (config)# interface gigabitethernet 1/0/1
   (config-if)# ip access-group MIRROR-B in-mirror
   (config-if)# exit
   (config)# interface gigabitethernet 1/0/2
   (config-if)# ip access-group MIRROR-B in-mirror

```
(config-if)# exit
(config)# interface gigabitethernet 1/0/3
(config-if)# ip access-group MIRROR-B in-mirror
(config-if)# exit
```

イーサネットインタフェース 1/0/1，1/0/2，および 1/0/3 の受信側に，IPv4 アクセスリスト（IPv4-MIRROR-B）をポリシーベースミラーリングとして適用します。

20 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。

20.1 解説

20.1.1 sFlow 統計の概要

sFlow 統計はエンドー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 20-1　sFlow 統計のネットワーク構成例

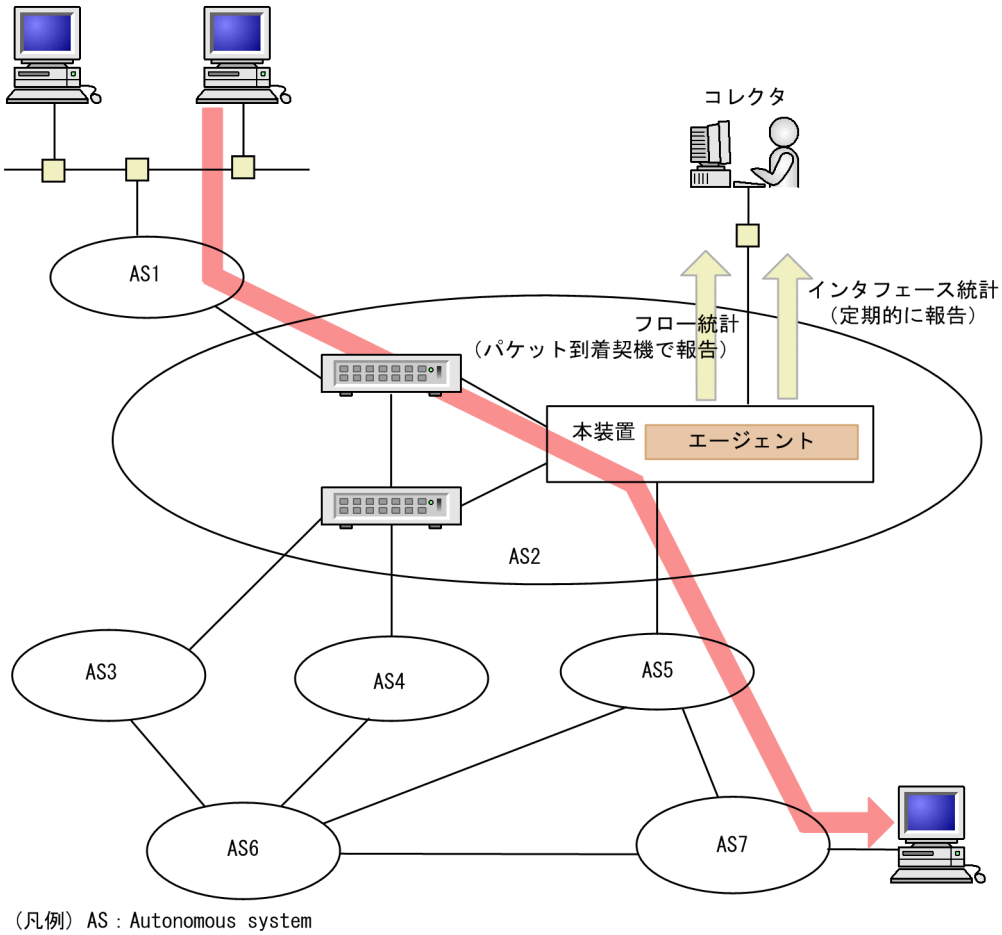
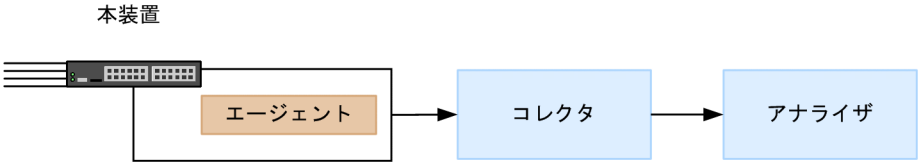


図 20-2　システム構成



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 20-1　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なっている場合もあります。

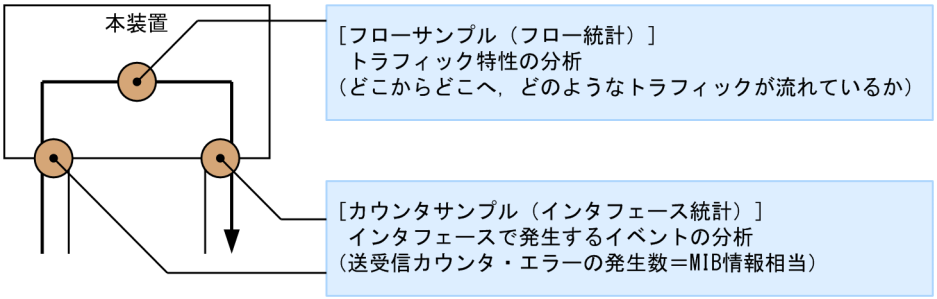
20.1.2 sFlow 統計エージェント機能

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。

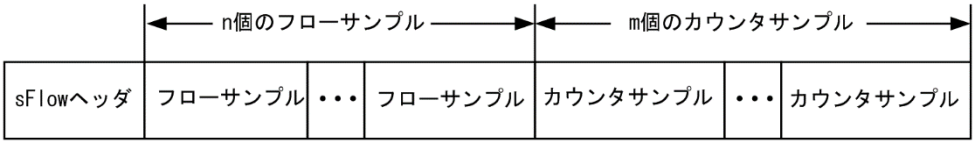
図 20-3　フローサンプルとカウンタサンプル



20.1.3 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（フローサンプルとカウンタサンプル）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 20-4　sFlow パケットフォーマット



なお，本装置では，一つの sFlow パケットにフローサンプルとカウンタサンプルは同時に入りません。

(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 20-2　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 20-4　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

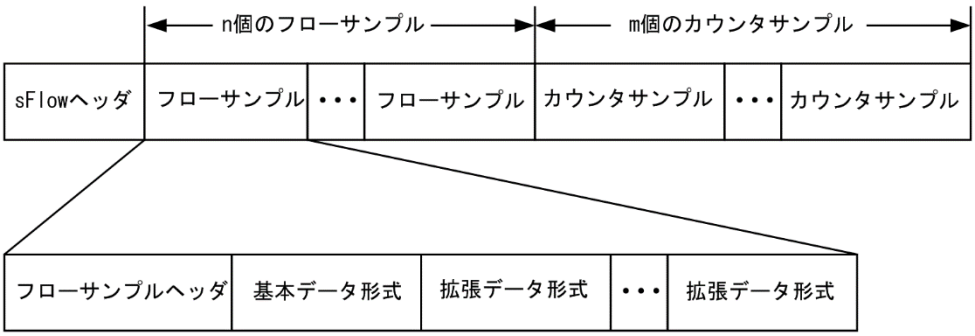
注※

スタック構成時，マスタスイッチが切り替わったときにリセットします。

(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。ただし，本装置は，本装置宛てのパケットのフローサンプルはサポートしません。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 20-5　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 20-3　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※1	○
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	○※2
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 本装置では 0 固定を設定	○

設定項目	説明	サポート
input	受信インタフェースの SNMP Interface Index インタフェースが不明な場合 0 を設定	○※2
output	送信インタフェースの SNMP Interface Index 送信インタフェースが不明な場合は 0 を設定	○※2

（凡例）○：サポートする　×：サポートしない

注※1

スタック構成時，マスタスイッチが切り替わったときにリセットします。

注※2

本装置では，サンプリング位置によって，SNMP Interface Index（以降 ifindex）情報が次の表のとおりになります。

表 20-4　サンプリング位置による ifindex 情報

項目	受信（Ingress）	送信（Egress）
source_id	受信インタフェースの ifindex	送信インタフェースの ifindex
input	受信インタフェースの ifindex	0 固定
output	0 固定	送信インタフェースの ifindex

(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 20-5　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できない場合には，本フォーマットになります。

表 20-6　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	○
dst_port	宛先ポート番号	○

設定項目	説明	サポート※
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

注※

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 20-7　IPv6 型のフォーマット

設定項目	説明	サポート※1
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※2	○

（凡例）○：サポートする

注※1

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。

注※2

本装置ではトラフィッククラスを収集します。

(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。本装置では，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対象としますが，その中で実際に収集できた拡張形式だけを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 20-8　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
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
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　×：サポートしない

注※1

コンフィグレーション指定はできますが，収集する条件を満たさないため，実際に収集することはありません。

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 20-9　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	○※1
src_priority	受信パケットの 802.1p 優先度	○※1
dst_vlan	送信パケットの 802.1Q VLAN ID	×※2
dst_priority	送信パケットの 802.1p 優先度	×※2

（凡例）○：サポートする　×：サポートしない

注※1

本装置が送信する自発パケットの場合，送信パケットの情報が設定されます。

注※2

未サポートのため 0 固定です。

表 20-10　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）	○
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	×※
dst_user<>	宛先のユーザ名	×※

（凡例）○：サポートする　×：サポートしない

注※

未サポートのため 0 固定です。

表 20-11　URL 型のフォーマット

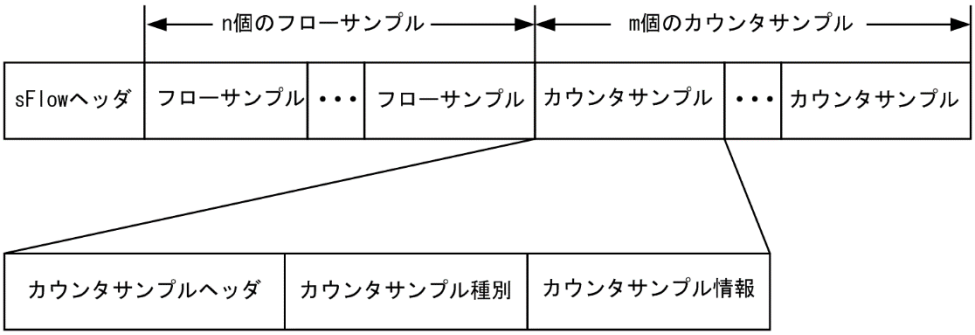
設定項目	説明	サポート
extended_information_type	拡張データ形式のタイプ（URL 型=5）	○
url_direction	URL 情報源 （source address=1，destination address=2） 本装置では 2 固定を設定	○
url_len	URL 長	○
url<>	URL 内容	○

（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 20-6　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 20-12　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）を表す 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

注※

スタック構成時，マスタスイッチが切り替わったときにリセットします。

(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 20-13　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）	×※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）	×※1
FDDI	FDDI 統計（counters_type=4）	×※1
100BaseVG	VG 統計（counters_type=5）	×※1
WAN	WAN 統計（counters_type=6）	×※1
VLAN	VLAN 統計（counters_type=7）	×※2

（凡例）○：サポートする　×：サポートしない

注※1

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。

注※2

本装置では VLAN 統計はサポートしていません。

(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 20-14　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［RFC3176 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。

20.1.4 本装置の sFlow 統計動作

(1)　sFlow 統計の収集対象ポート

本装置は，イーサネットインタフェースを，sFlow 統計のサンプリング対象にできます。また，サンプリング属性として，受信（ingress）または送信（egress）のどちらかを装置単位で選択できます。

(2)　フローサンプルの対象パケット

本装置は，本装置で処理するすべてのパケットをフローサンプルの対象とします。

サンプリング属性によって，次に示すパケットはサンプリング対象として扱いません。

受信指定でサンプリング対象として扱わないパケット

- イーサネットインタフェースによって廃棄されたパケット

送信指定でサンプリング対象として扱わないパケット

- ポートミラーリングおよびポリシーベースミラーリングのミラーポートから送信するパケット

(3)　廃棄パケットのフローサンプル動作

本装置のフローサンプルは，本装置でパケットを廃棄する場合でもコレクタには中継しているように sFlow パケットを送信する場合があります。他機能で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。
他機能による廃棄パケットのフローサンプル動作を次の表に示します。

表 20-15　他機能による廃棄パケットのフローサンプル

廃棄する機能		受信指定	送信指定
フィルタ（受信側）		収集しない	収集しない
フィルタ（送信側）	イーサネットインタフェースに適用	収集する	収集する
	VLAN インタフェースに適用	収集する	収集しない
QoS（帯域監視）		収集しない	収集しない
QoS（廃棄制御）		収集する	収集しない
ストームコントロール		収集しない	収集しない
ポート間中継遮断		収集する	収集しない
レイヤ 2 機能※1		収集しない	収集しない

廃棄する機能	受信指定	送信指定
レイヤ 3 機能※2	収集しない	収集しない

注※1

レイヤ 2 による廃棄フレームには次に示すものがあります。

- MAC アドレス学習機能による廃棄
- VLAN によって中継できないで廃棄
- レイヤ 2 プロトコルによる Blocking で廃棄
- レイヤ 2 認証による廃棄
- IGMP snooping，MLD snooping，DHCP snooping による廃棄
- レイヤ 2 プロトコルが無効な場合の廃棄

注※2

レイヤ 3 による廃棄パケットは次に示すものがあります。

- IP レイヤによるエラーパケット廃棄

(4)　フローサンプル内容のサンプリング位置による注意事項

本装置のフローサンプリング内容を次の表に示します。本装置で廃棄したパケットがフローサンプルの対象となる場合も同様です。

表 20-16　フローサンプリング内容

サンプリング属性	フローサンプリング内容
受信指定	受信時の内容
送信指定	送信時の内容

(5)　他機能併用時のフローサンプル内容に関する注意事項

本装置のフローサンプルは，サンプリング対象ポートで併用する機能およびサンプリングパケットの中継条件によって，収集するフローサンプル情報が異なります。他機能併用時および中継条件によるフローサンプル収集内容（ヘッダ型データ）を次の表に示します。

表 20-17　他機能併用時および中継条件によるフローサンプル収集内容

併用機能および中継条件	受信指定	送信指定
VLAN （VLAN Tag の TPID 値設定）	受信した TPID※1	送信時の TPID※1
VLAN トンネリング （トンネリングポート受信）	トンネリング用 Tag 付加前の情報※2	トンネリング用 Tag 付加後の情報※1※3
VLAN トンネリング （トンネリングポート送信）	トンネリング用 Tag 削除前の情報※2※3	トンネリング用 Tag 削除後の情報※1
VLAN Tag 変換 （Tag 変換ポート受信）	変換前の Tag 情報※2	変換後の Tag 情報※1
QoS 帯域監視 （ペナルティ DSCP 書き換え）	書き換え前の DSCP 値※4	書き換え後の DSCP 値※4
QoS マーカー （DSCP 書き換え）	書き換え前の DSCP 値※4	書き換え後の DSCP 値※4
QoS マーカー （ユーザ優先度書き換え）	書き換え前のユーザ優先度※2	書き換え後のユーザ優先度※1

注※1

ヘッダ型のフレーム情報。

注※2

ヘッダ型のフレーム情報，スイッチ型の受信パケットの VLAN 情報。

注※3

VLAN Tag が 2 段以上の場合，IPv4 型，IPv6 型，ユーザ型，URL 型の情報は収集しません。

注※4

ヘッダ型のフレーム情報，IPv4 型の TOS 情報，IPv6 型の priority 情報。

(6)　カウンタサンプル収集の対象パケット

本装置でのカウンタサンプルは，送信または受信のどちらを指定しても，該当ポートのすべての送受信パケットをカウントします。

(7)　フロー統計と併用できない機能

同一ポートで，次の併用はしないでください。

- sFlow 統計の送信（egress）指定と，送信フレームを対象とするポートミラーリングのモニターポートの併用。
- sFlow 統計の送信（egress）指定と，802.1Q Tag 付与機能を使用したミラーポートの併用。

20.1.5 sFlow 統計使用時の注意事項

(1)　スタック構成時について

スタック構成時はコンフィグレーションコマンド sflow source を設定してください。または，ループバックインタフェースに IP アドレスを設定してください。

20.2 コマンドガイド

20.2.1 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 20-18　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。

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 20-19　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。

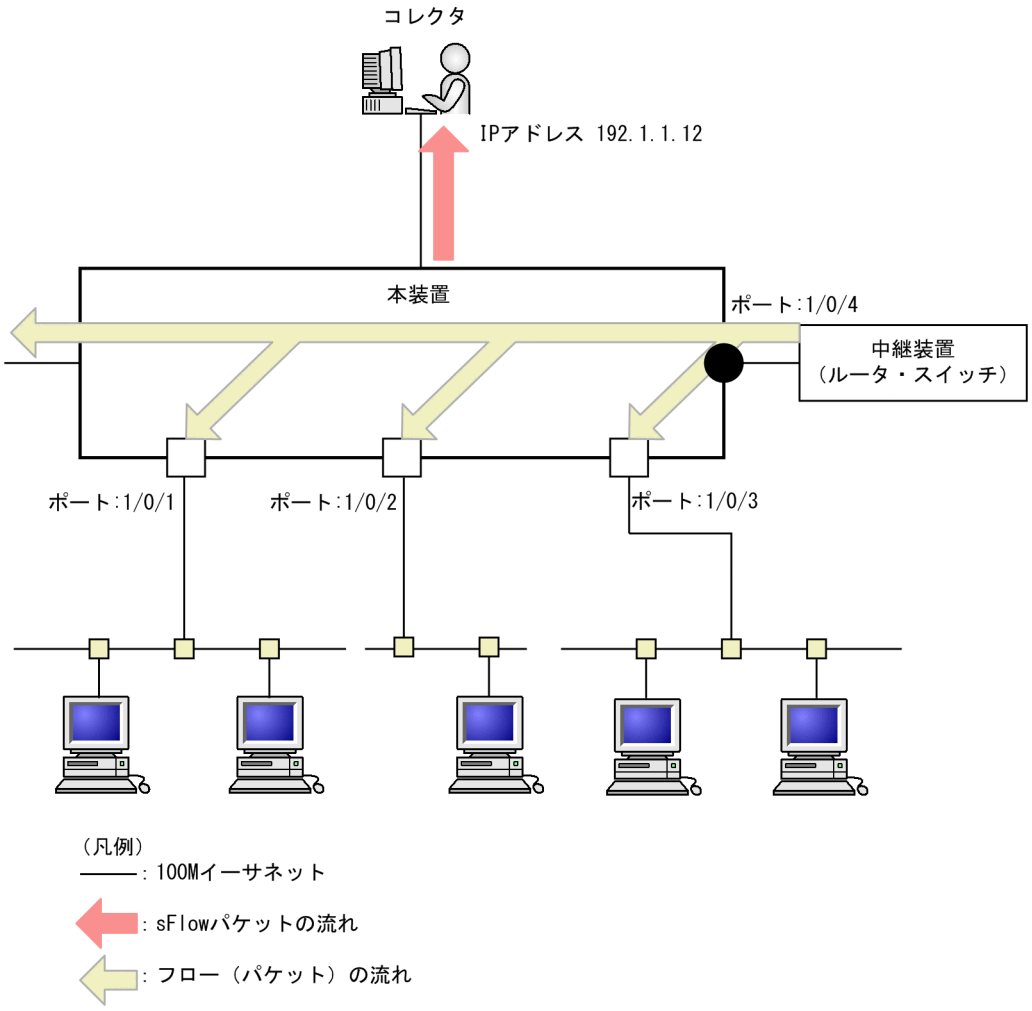
20.2.2 sFlow 統計の基本的な設定

(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 1/0/4 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 20-7　ポート 1/0/4 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 1/0/4**
   ポート 1/0/4 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 1/0/4 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］

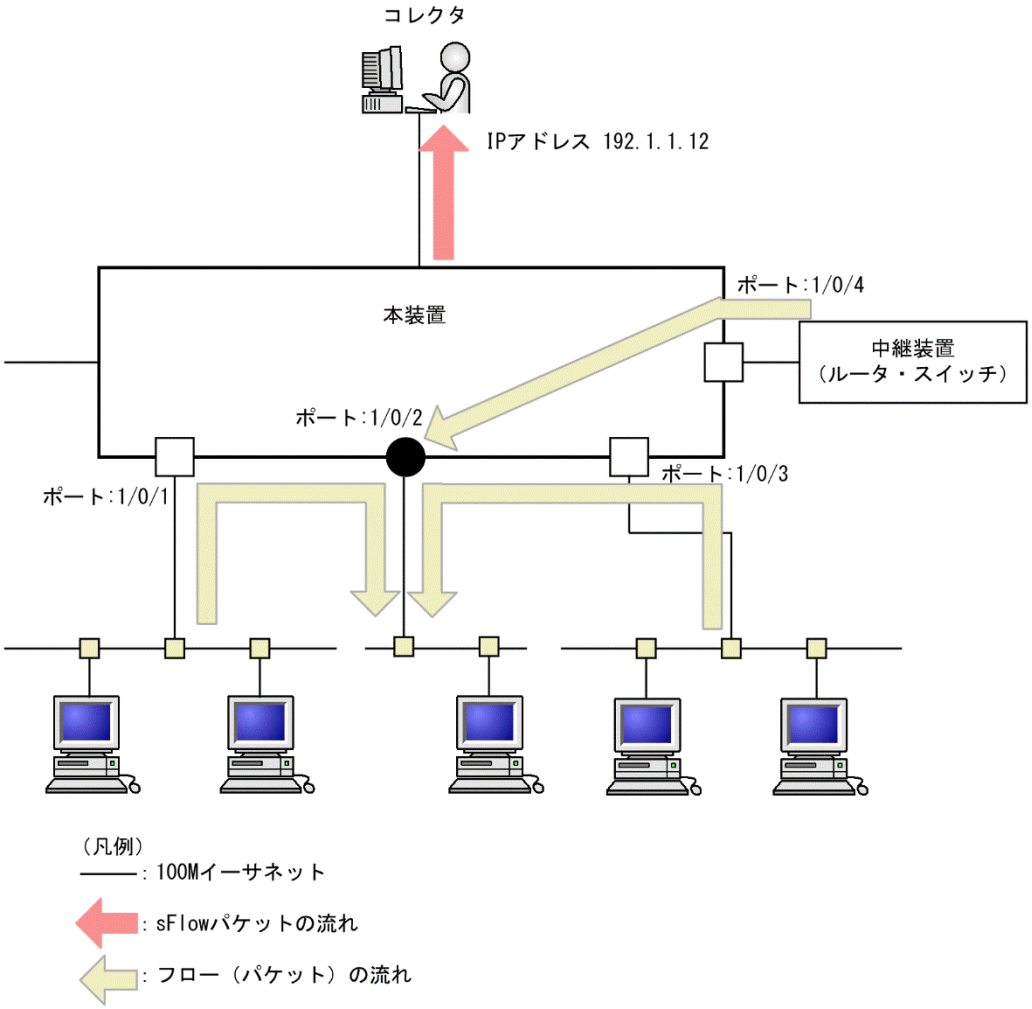
sflow sample コマンドで設定するサンプリング間隔については，インタフェースの回線速度を考慮して決める必要があります。詳細は，「コンフィグレーションコマンドレファレンス」　「sflow sample」を参照してください。

(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 1/0/2 から出て行くパケットをモニタする設定を示します。

図 20-8　ポート 1/0/2 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 1/0/2
   ポート 1/0/2 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 1/0/2 の送信パケットに対して sFlow 統計機能を有効にします。

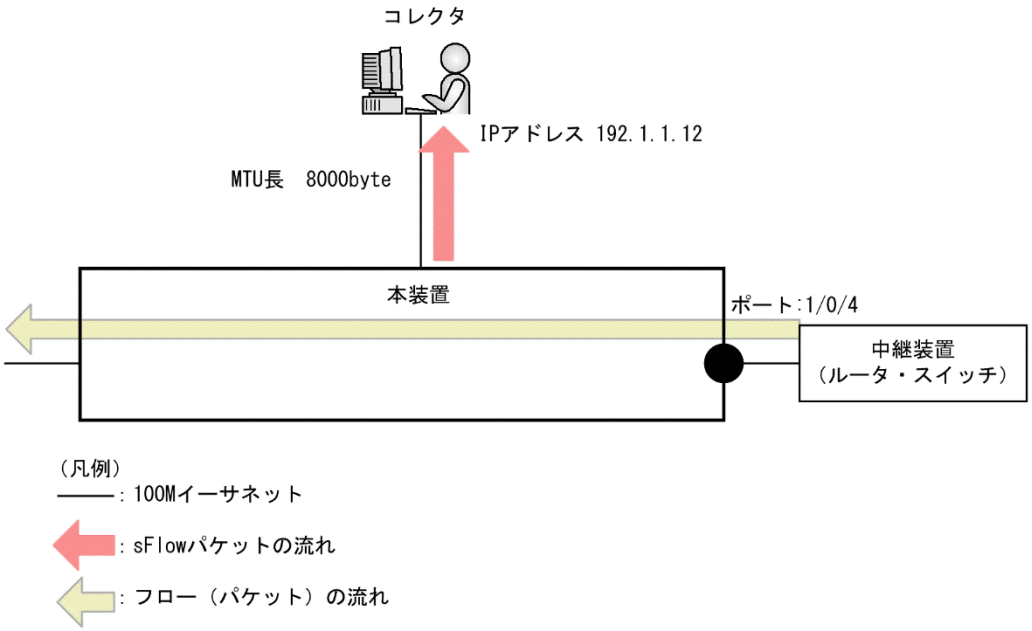
20.2.3 sFlow 統計コンフィグレーションパラメータの設定例

(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 20-9　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 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 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 1/0/4**
   ポート 1/0/4 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 1/0/4 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 VLAN 情報だけ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 switch
フローサンプルの拡張データ形式に「スイッチ」を設定します（スイッチ情報だけが取得できます)。

5. (config)# interface gigabitethernet 1/0/4
ポート 1/0/4 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 1/0/4 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)# 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。

4. (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。

5. (config)# interface gigabitethernet 1/0/4
ポート 1/0/4 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 1/0/4 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 1/0/4
   ポート 1/0/4 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 1/0/4 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。

20.2.4 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 100 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 1/0/4 とポート 1/0/5 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 20-10　show interfaces コマンドの実行結果

```
> show interfaces gigabitethernet 1/0/4
Date 20XX/12/24 17:18:54 UTC
NIF0:
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 1/0/5
Date 20XX/12/24 17:19:34 UTC
NIF0:
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/100

＝　（10.3kpps+16.8kpps）/100

＝　271※

注※

サンプリング間隔を 271 で設定すると実際は 512 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（廃棄が発生しない推奨するサンプリング間隔）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 20-11　show sflow detail コマンドの実行結果

```
> show sflow detail
Date 20XX/12/21 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: 1/0/2-4
```

21 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。

21.1 解説

21.1.1 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常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。

21.1.2 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 21-1　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

21.1.3 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，efmoam active udld コマンド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。

21.2 コマンドガイド

21.2.1 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 21-2　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。

IEEE802.3ah/UDLD の運用コマンド一覧を次の表に示します。

表 21-3　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。

21.2.2 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ことが必要です。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 1/0/1 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 1/0/1
ポート 1/0/1 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 1/0/1 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トの設定

［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トです。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トを変更すると，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ト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ト）［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。

22 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。

22.1 解説

22.1.1 概要

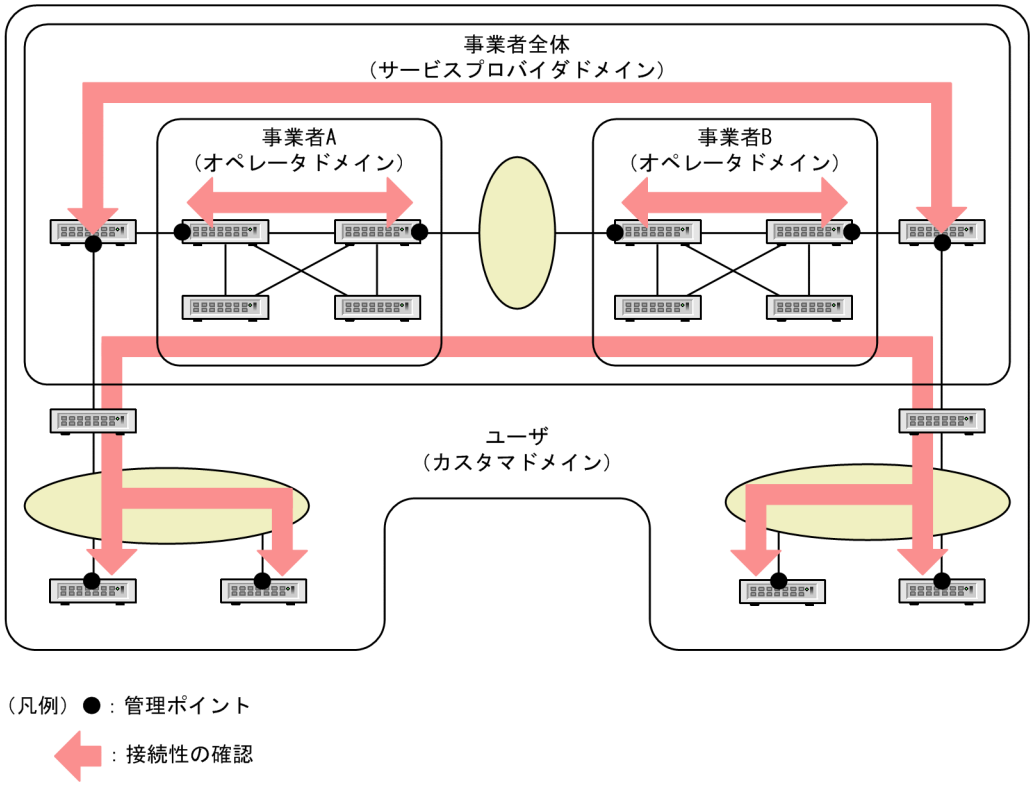
イーサネットは企業内 LAN だけでなく広域網でも使われるようになってきました。これに伴い，イーサネットに SONET や ATM と同等の保守管理機能が求められています。

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 22-1　CFM の構成例



(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 22-1　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 22-2　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。

22.1.2 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。

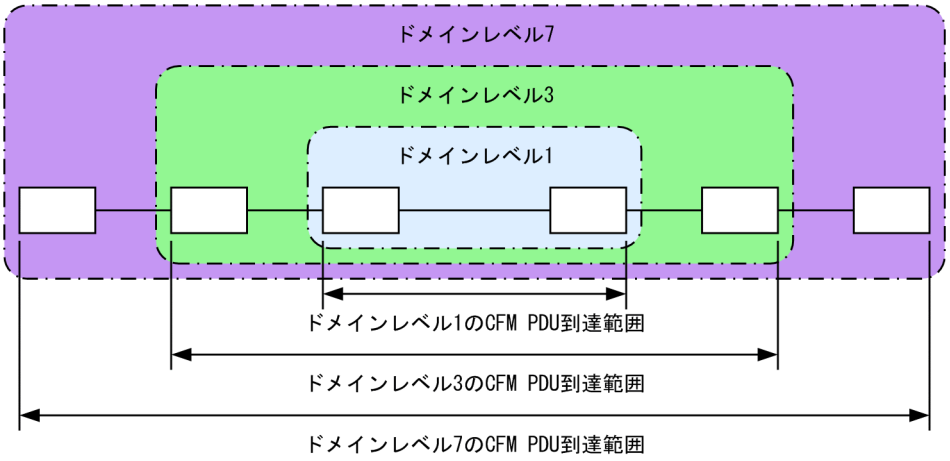
表 22-3　区分に割り当てられたドメインレベル

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）
3	
2	オペレータ（事業者）

ドメインレベル	区分
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 22-2　階層的なドメインの構成例



(2)　MA

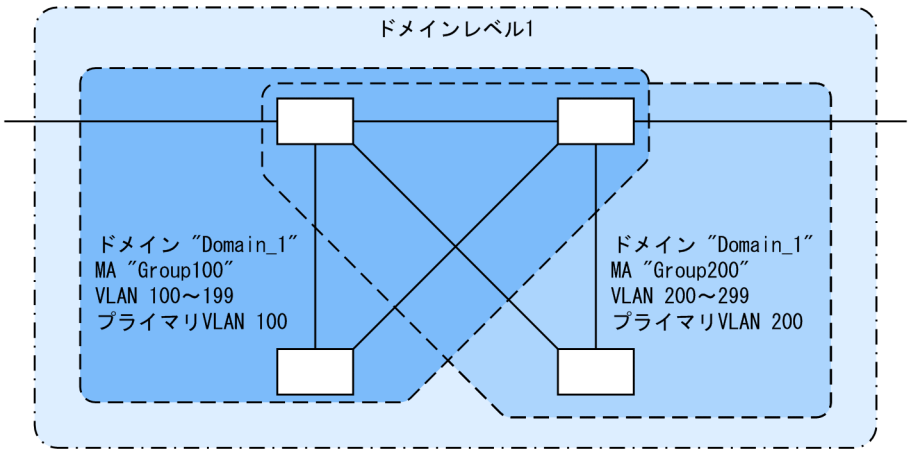
MA はドメイン内を VLAN グループで分割して管理する場合に使います。ドメインには最低一つの MA が必要です。

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 22-3　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。コンフィグ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

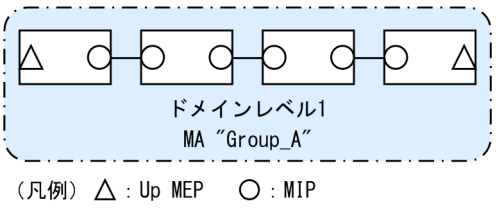
MEP はドメインの境界上の管理ポイントで，MA に対して設定します。MEP には MEP ID という MA 内でユニークな ID を設定して各 MEP を識別します。

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。

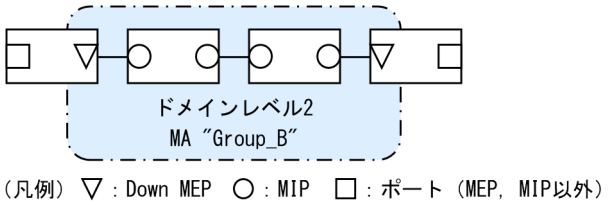
- Up MEP
  リレー側に設定する MEP です。Up MEP 自身は CFM PDU を送受信しないで，同一 MA 内の MIP またはポートを介して送受信します。
  Up MEP の設定例を次の図に示します。

図 22-4　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 22-5　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 22-6　Down MEP，Up MEP からの送信

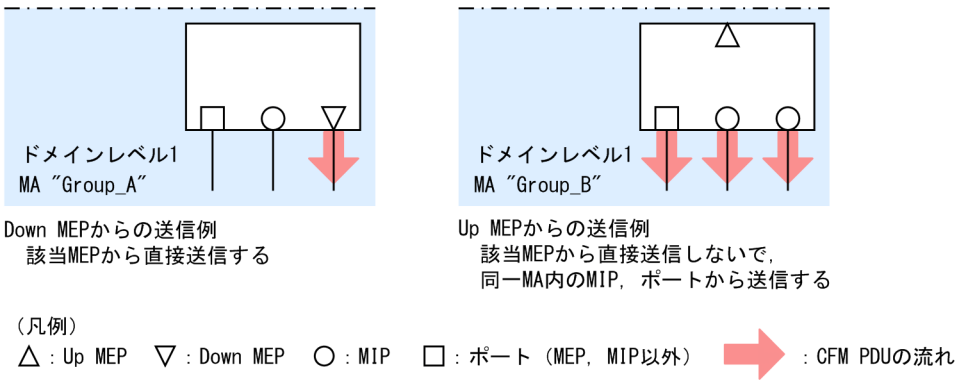
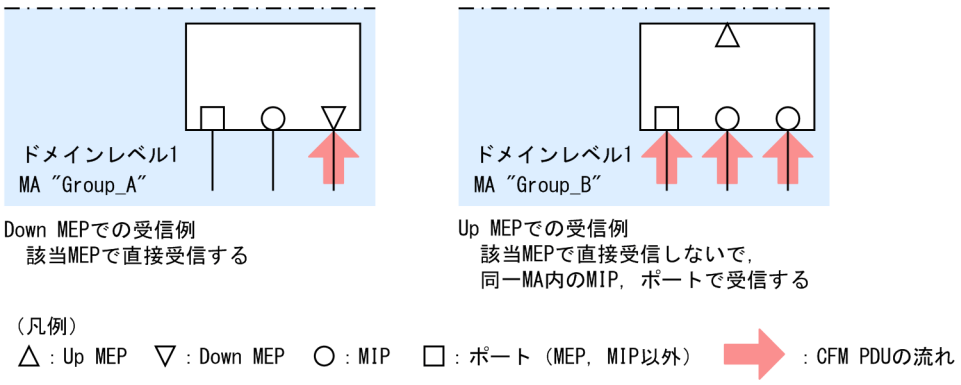
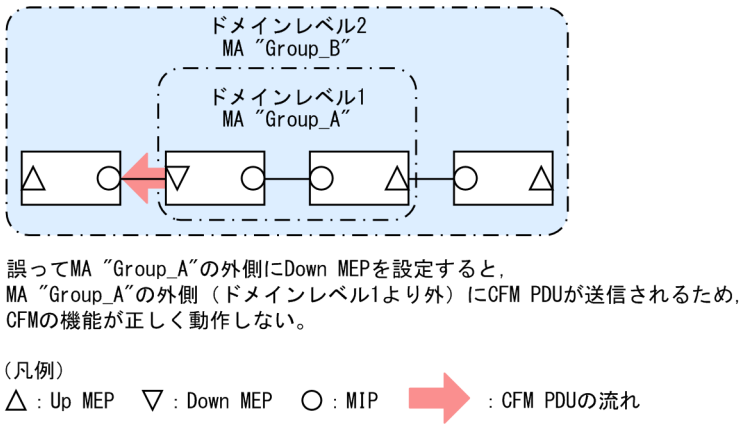


図 22-7　Down MEP，Up MEP での受信



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 22-8　誤って Down MEP を設定した例



(4)　MIP

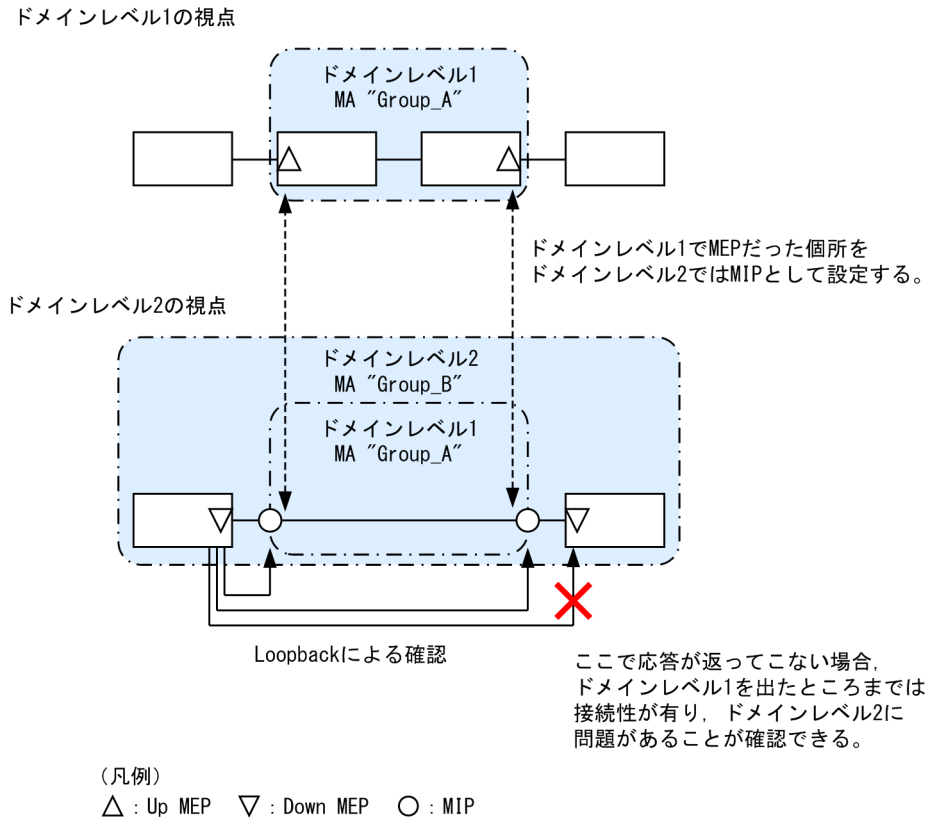
MIP はドメインの内部に設定する管理ポイントで，ドメインに対して設定します（同一ドメイン内の全 MA で共通）。階層構造の場合，MIP は高いドメインレベルのドメインが低いドメインレベルのドメインと重なる個所に設定します。また，MIP は Loopback および Linktrace に応答するので，ドメイン内の保守管理したい個所に設定します。

(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 22-9　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。

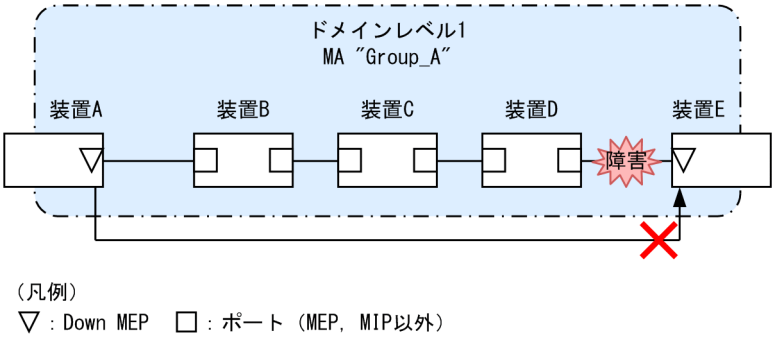
障害発生時は，ドメインレベル 2 の問題か，ドメインレベル 1 のどこかの問題かを切り分けられるため，調査範囲を特定できます。

(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。

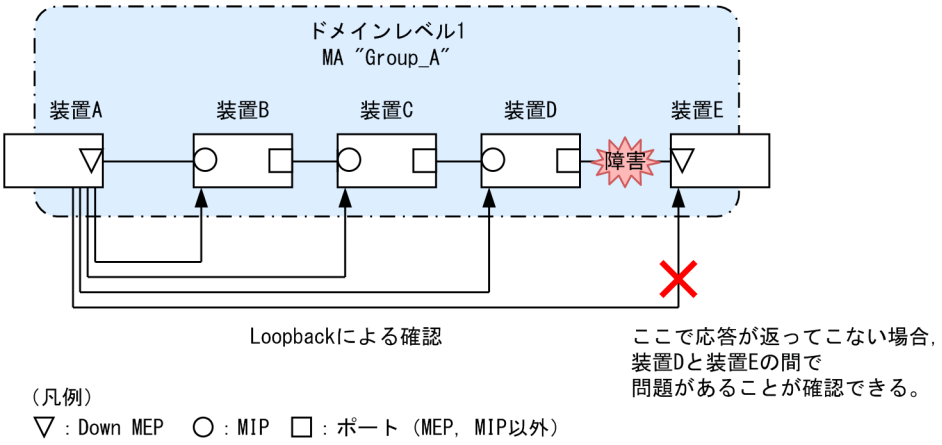
ドメイン内に MIP が設定されていない構成の例を次の図に示します。この例では，ネットワークに障害が発生した場合，装置 A，装置 E の MEP 間で通信できないことは確認できますが，どこで障害が発生したのか特定できません。

図 22-10　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，障害発生個所を特定できるようになります。

図 22-11　ドメイン内に MIP を設定した構成の例



22.1.3 ドメインの設計

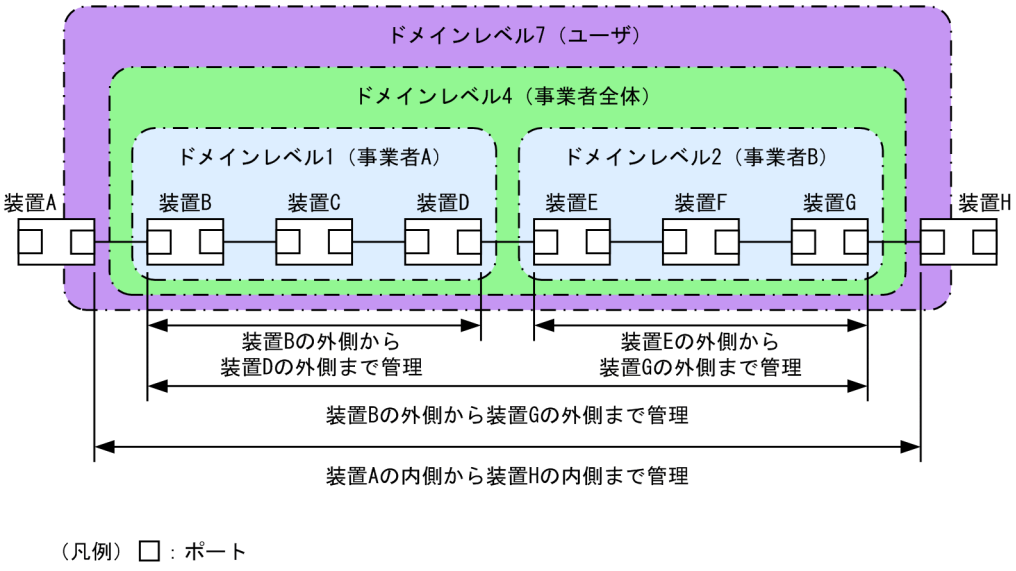
CFM を使用する際には，まずドメインを設計します。ドメインの構成と階層構造を設計し，次に個々のドメインの詳細設計をします。

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 22-12　構成例



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証するために，ユーザに提供するポートを含めた接続性を管理

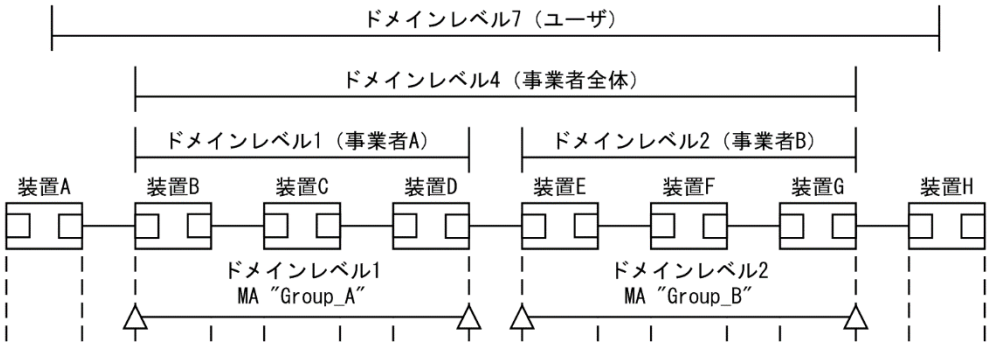
- ユーザは，事業者の提供する回線が使用できるかどうかを監視するために，事業者から提供される回線の接続性を管理

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 22-13 ドメインレベル 1，2 の設定

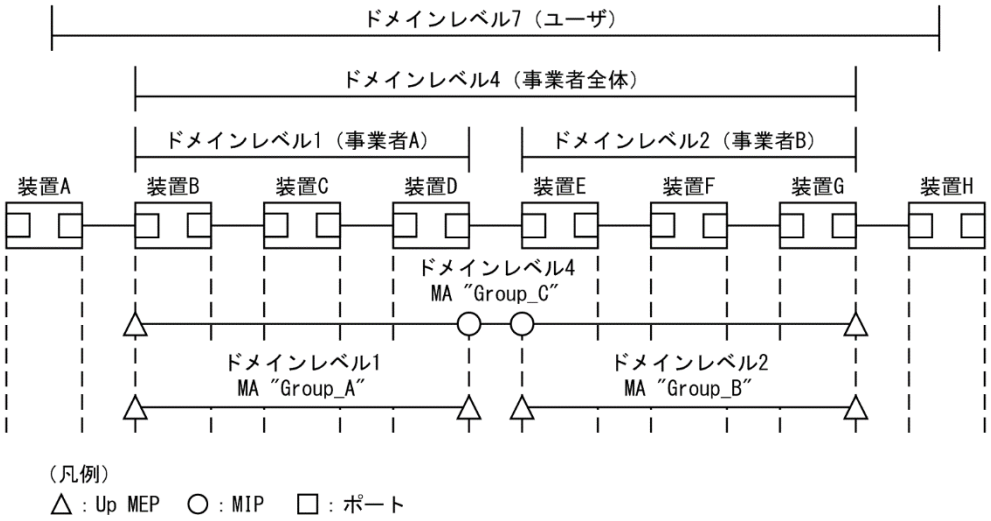


（凡例）
△：Up MEP　□：ポート

ドメインレベル 4 の設定

1. ドメインレベル 4 で MA“Group_C”を設定します。
2. 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。
3. 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。

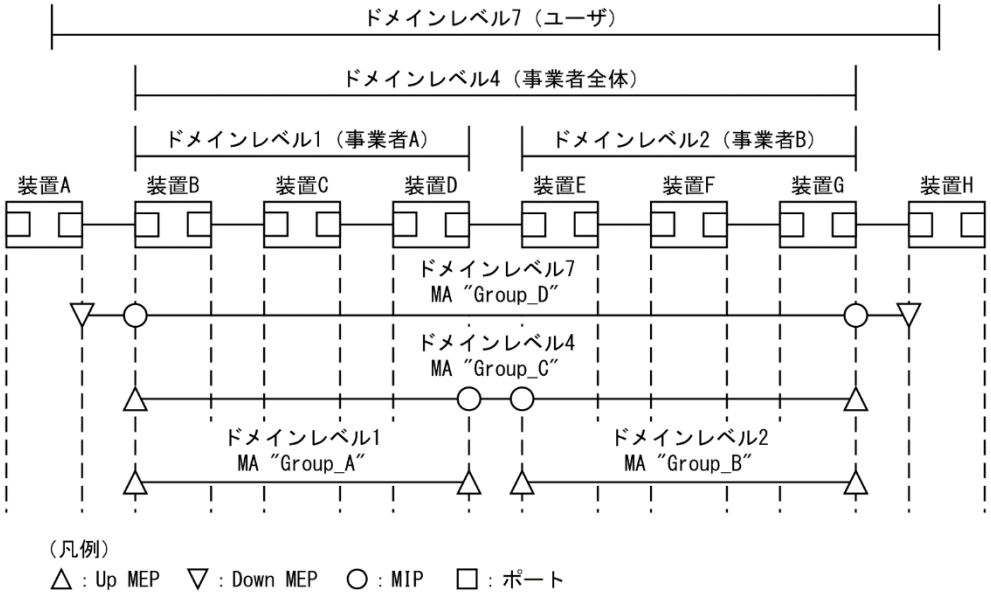
図 22-14 ドメインレベル 4 の設定



- ドメインレベル 7 の設定

1. ドメインレベル 7 で MA“Group_D”を設定します。
2. 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。
3. 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 22-15 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 22-16　MIP 設定前の構成例

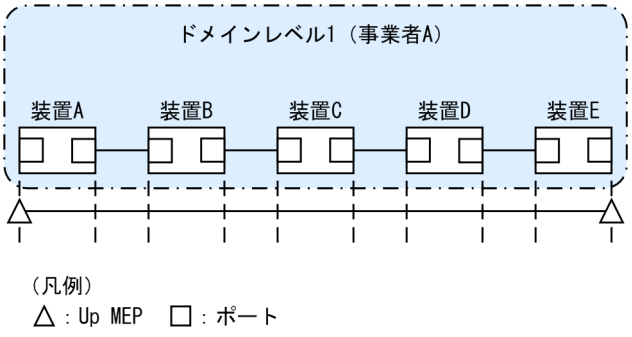
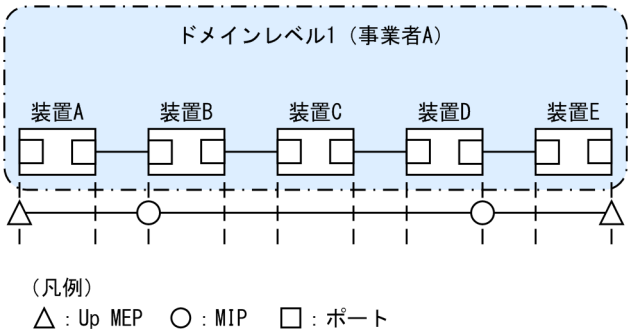


図 22-17　MIP 設定後の構成例



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。

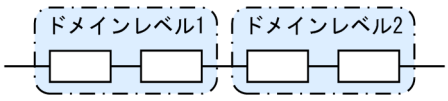
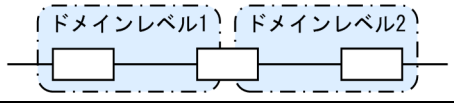
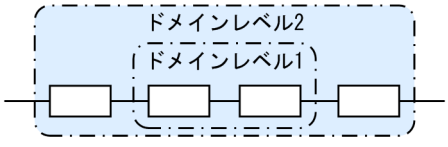
MIP を設定していない装置 C は Loopback，Linktrace の宛先として指定できません。また，Linktrace に応答しないためルート情報に装置 C の情報は含まれません。

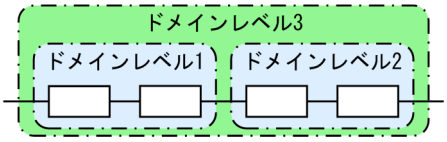
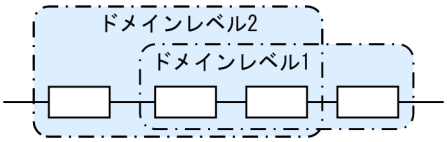
(3)　ドメインの構成例

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 22-4　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

構成状態	構成例	構成の可否
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

22.1.4 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 22-5　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。

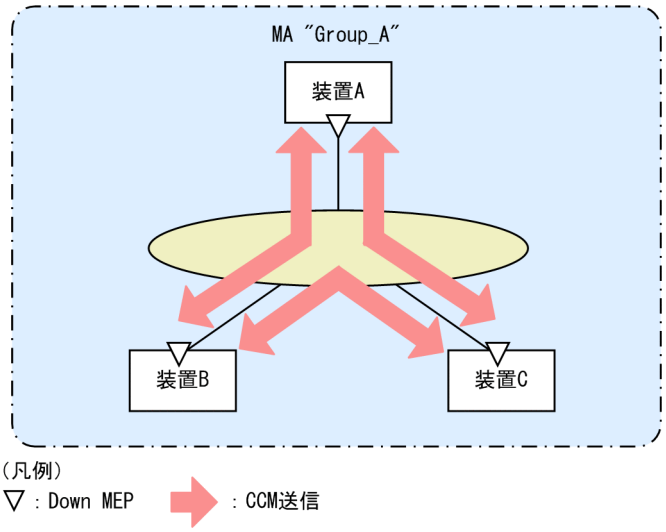
表 22-6　障害回復契機と障害回復監視時間

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。

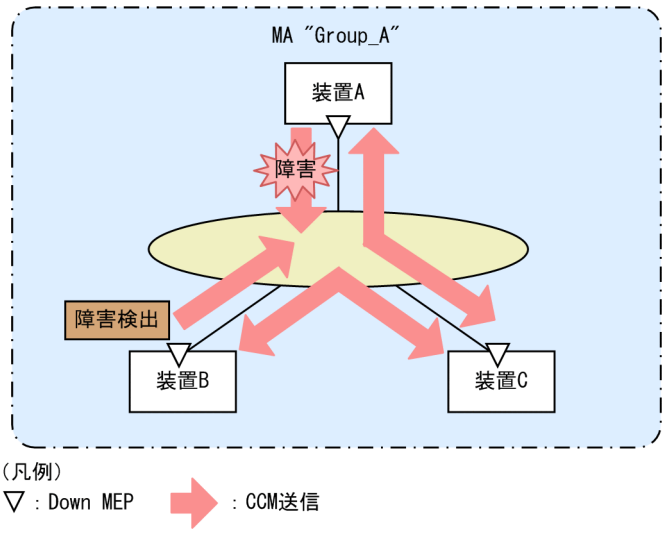
各 MEP はマルチキャストで MA 内に CCM を定期的に送信します。各 MEP の CCM を定期的に受信することで常時接続性を監視します。

図 22-18　CC での常時接続性の監視



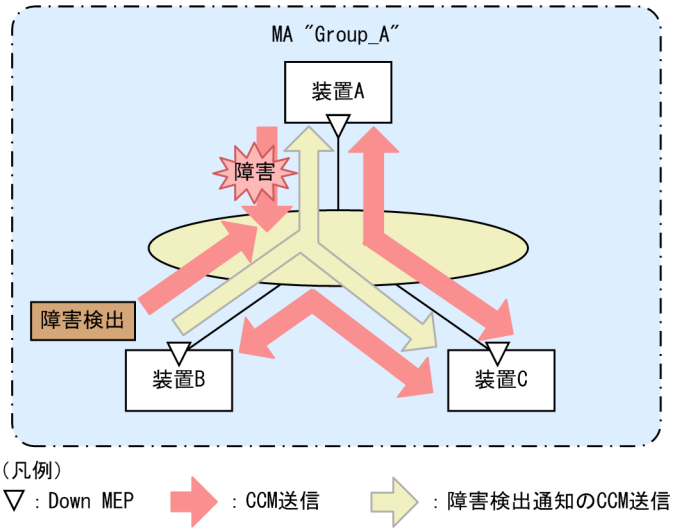
装置 A の CCM が装置の故障またはネットワーク上の障害によって，装置 B に届かなくなると，装置 B は装置 A とのネットワーク上の障害として検出します。

図 22-19　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 22-20　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。

22.1.5 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 から宛先へ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 22-21　MIP に対して Loopback を実行

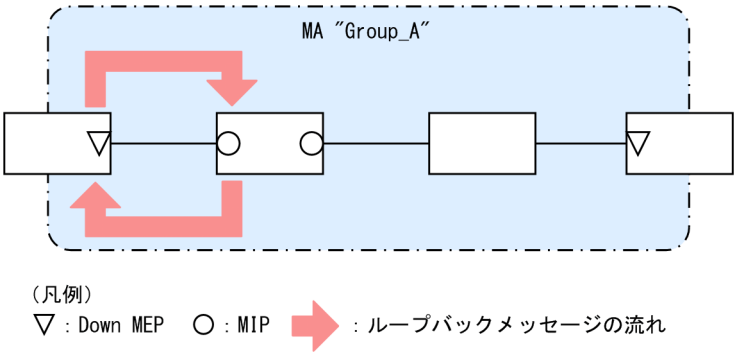
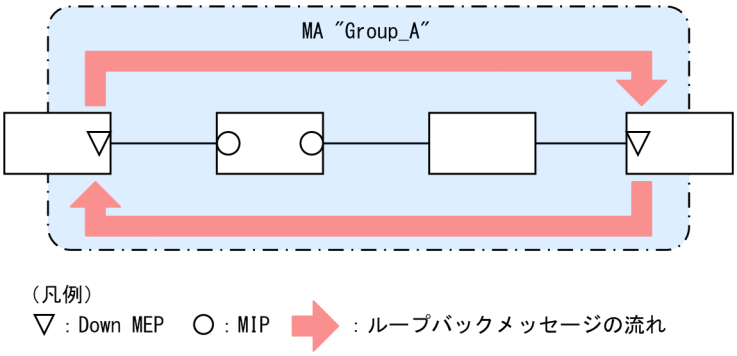


図 22-22　MEP に対して Loopback を実行



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。

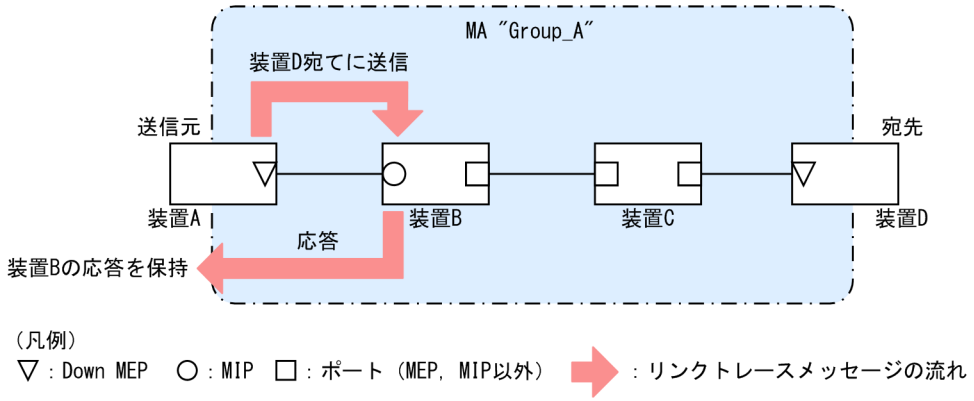
22.1.6 Linktrace

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。

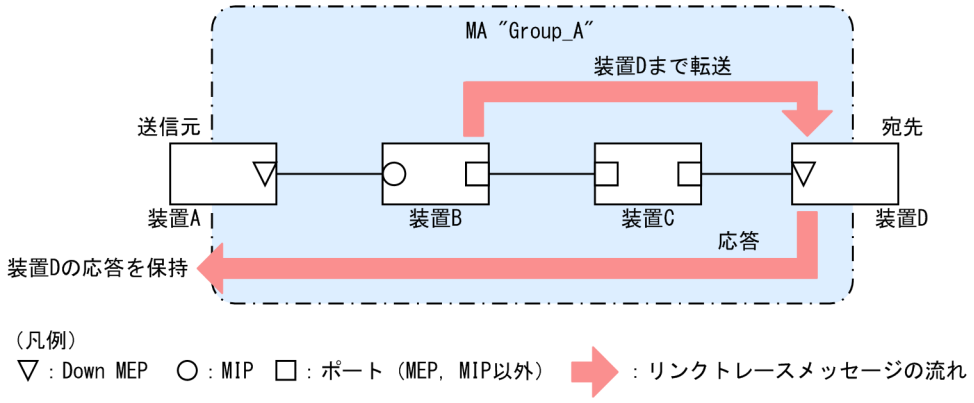
図 22-23　宛先にリンクトレースメッセージを送信



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 22-24　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 は到達したことと，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。

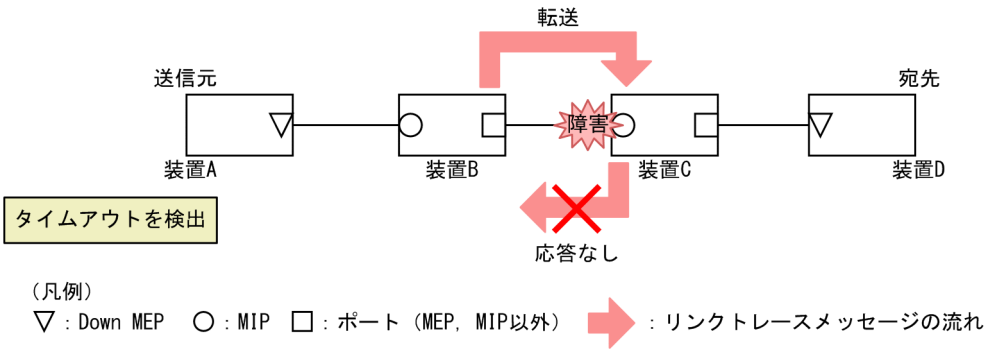
(a)　Linktrace による障害の切り分け

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めます。

● 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 22-25　Linktrace でタイムアウトを検出した例

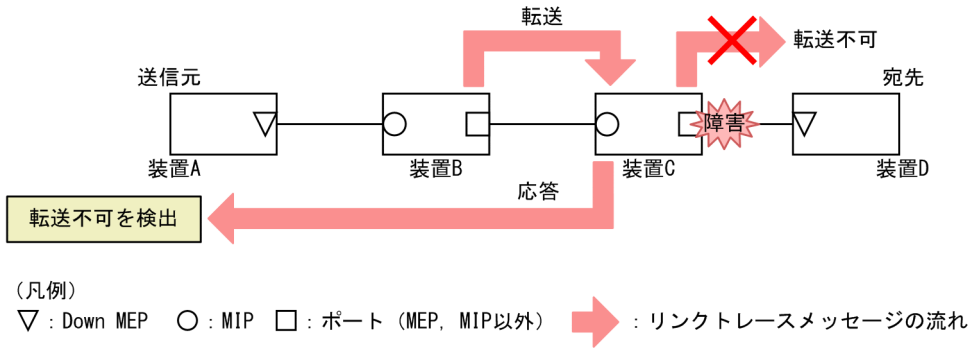


この例では，装置 A が Linktrace でタイムアウトを検出した場合，ネットワーク上の受信側のポートが通信できない状態が考えられます。リンクトレースメッセージが装置 B から装置 C に転送されていますが，装置 C が通信できない状態になっていて，応答を返さないため，タイムアウトになります。

● 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 22-26　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。

22.1.7 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 22-7　Up MEP がブロック状態の場合

機能	動作
CC	・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	・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応答する
Linktrace	・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応答する。応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 22-8　Down MEP がブロック状態の場合

機能	動作
CC	・CCM を送受信しない
Loopback	・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応答しない
Linktrace	・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応答しない

表 22-9　MIP がブロック状態の場合

機能	動作
CC	・CCM を透過しない
Loopback	・回線側から受信した自宛のループバックメッセージに応答しない ・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応答する ・ループバックメッセージを透過しない
Linktrace	・回線側から受信したリンクトレースメッセージに応答しない ・リレー側から受信したリンクトレースメッセージに応答する。応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 22-10　MEP，MIP 以外のポートがブロック状態の場合

機能	動作
CC	・CCM を透過しない
Loopback	・ループバックメッセージを透過しない
Linktrace	・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。

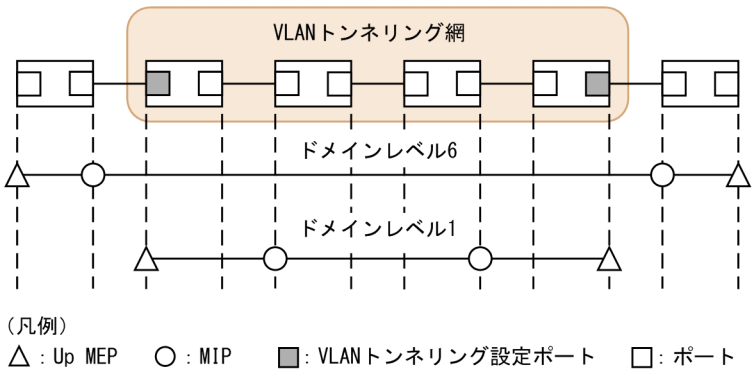
表 22-11　ドメインの設定個所別の機能の使用制限

ドメインの設定個所	機能		
	CC	Loopback	Linktrace
VLAN トンネリング網内と VLAN トンネリング網外	使用可	使用可	・VLAN トンネリング網内では使用可 ・VLAN トンネリング網外では VLAN トンネルを越えては使用不可
VLAN トンネリング網内だけ	使用可	使用可	使用可
VLAN トンネリング網外だけ	使用可	使用可	使用可

(a)　VLAN トンネリング網内と VLAN トンネリング網外で 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 CFM を使用する例を次の図に示します。

図 22-27　VLAN トンネリング網内と VLAN トンネリング網外で CFM を使用する例



VLAN トンネリング網内のドメインレベル 1 は，VLAN トン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 トンネリング網外のドメインレベル 6 は，VLAN トンネリング網外の装置だけに管

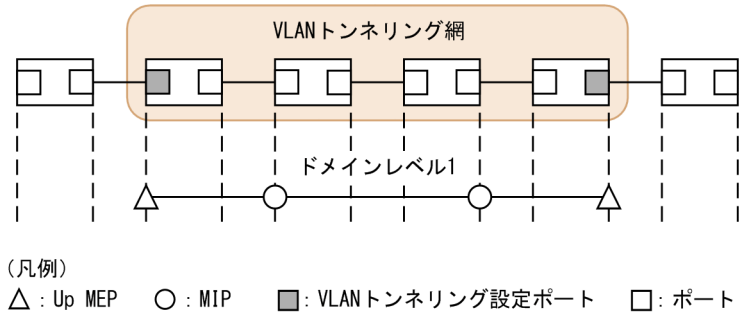
理ポイントを設定できます。VLAN トンネリング網内にはドメインレベル 6 の管理ポイントは設定できません。VLAN トンネリング網内の管理はドメインレベル 1 でします。

また，VLAN トンネリング網外のドメインレベル 6 では VLAN トンネルを越えては Linktrace を使用できません。

(b)　VLAN トンネリング網内だけで CFM を使用する場合

VLAN トン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 22-28　VLAN トンネリング網内だけで CFM を使用する例

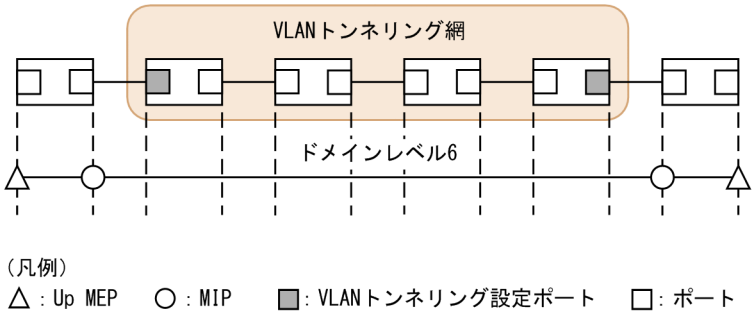


VLAN トンネリング網内のドメインレベル 1 は，VLAN トンネリング網内で任意の個所に管理ポイントを設定できます。該当ドメインでは CFM の各機能が使用できます。

(c)　VLAN トンネリング網外だけで CFM を使用する場合

VLAN トン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 22-29　VLAN トンネリング網外だけで CFM を使用する例



VLAN トンネリング網外のドメインレベル 6 は，VLAN トン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 トン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。

22.1.8 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 22-12　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。 ・MEP ID	show cfm remote-mep

データベース	内容	内容確認コマンド
	・MEP ID に対応する MAC アドレス ・該当 MEP で発生した障害情報	
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。 ・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。 ・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。

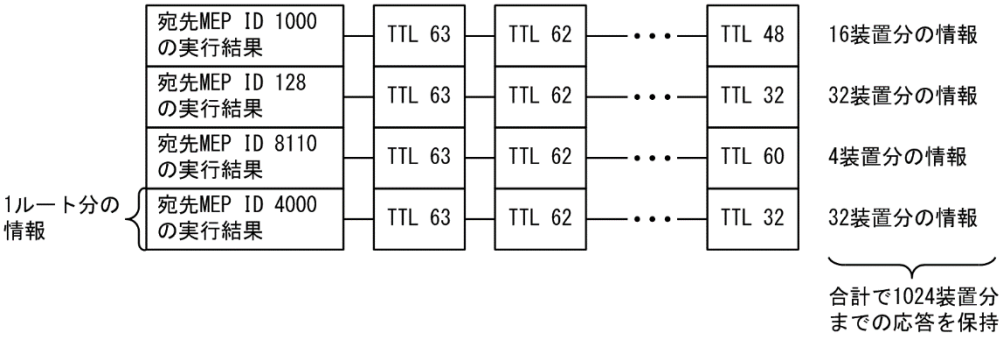
1 ルート当たり何装置分の応答を保持するかで何ルート分保持できるかが決ります。1 ルート当たり 256 装置分の応答を保持した場合は 4 ルート，1 ルート当たり 16 装置分の応答を保持している場合は 64 ルート保持できます。

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 22-30　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。

22.1.9 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 22-13　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

(a)　レイヤ 2 認証との共存

「5.2.1　レイヤ 2 認証と他機能との共存」を参照してください。

(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 96 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)　同一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

同一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）
- 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

(8) 冗長構成での CC の動作について

レイヤ 2 の冗長構成（スパニングツリー，Ring Protocol など）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，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。

22.2 コマンドガイド

22.2.1 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 22-14 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 SNMP 通知を送信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。

CFM の運用コマンド一覧を次の表に示します。

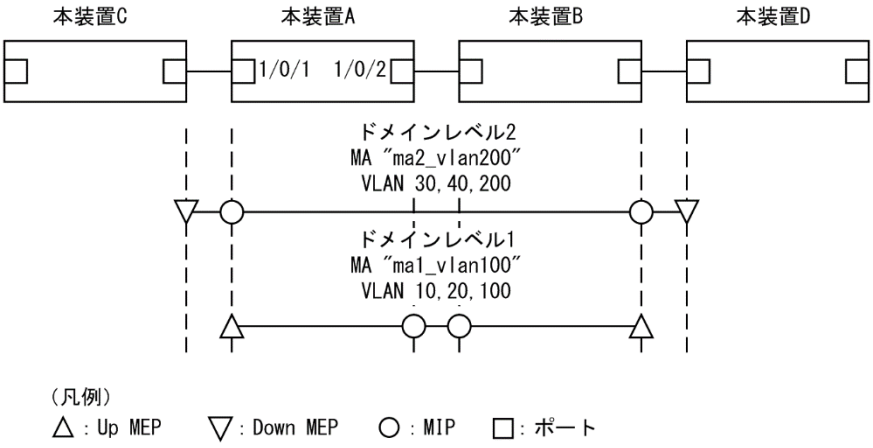
表 22-15 運用コマンド一覧

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。

22.2.2 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 22-31 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 1/0/1

```
(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 1/0/2
(config-if)# ethernet cfm mip level 1
(config-if)# exit
```

ポート 1/0/1 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 1/0/2 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 1/0/1`
   ```
   (config-if)# no ethernet cfm enable
   (config-if)# exit
   ```
   ポート 1/0/1 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。

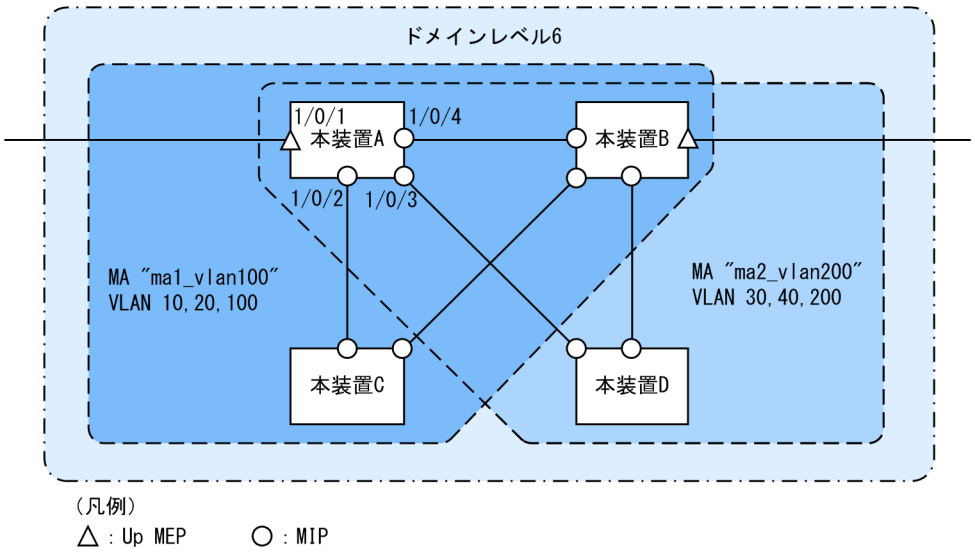
［コマンドによる設定］

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。

22.2.3 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 22-32　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，「22.2.2　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，「22.2.2　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 1/0/1
(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 1/0/2-4
(config-if-range)# ethernet cfm mip level 6

(config-if-range)# exit
ポート 1/0/1 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 1/0/2～1/0/4 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。

23 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。

23.1 解説

23.1.1 概要

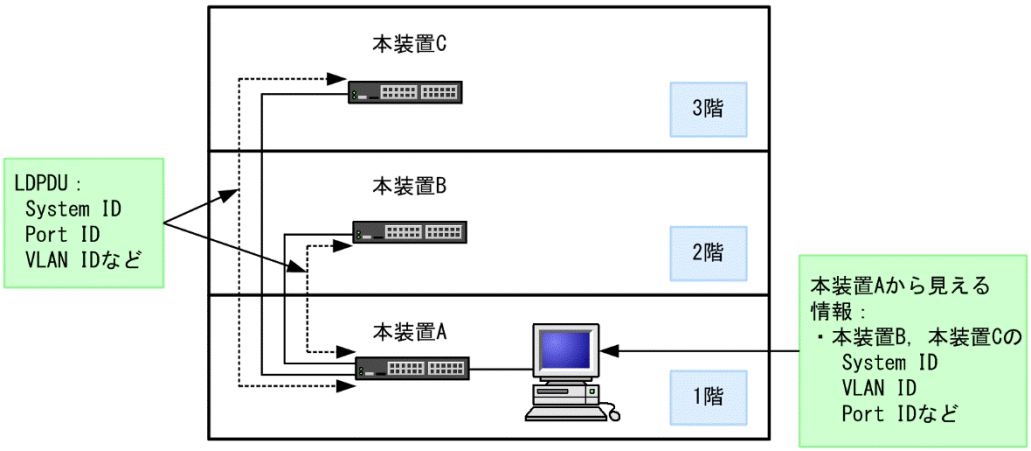
LLDP（Link Layer Discovery Protocol）は隣接する装置情報を収集するプロトコルです。運用・保守時に接続装置の情報を簡単に調査できることを目的とした機能です。

(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 23-1　LLDP の適用例



23.1.2 サポート仕様

(1)　接続できる LLDP 規格

本装置では次に示す二つの規格をサポートします。

- IEEE Std 802.1AB-2009
  本装置では，宛先 MAC アドレスが“01:80:C2:00:00:0E”だけ LLDPDU として受信できます。
- IEEE 802.1AB Draft 6

デフォルトでは IEEE Std 802.1AB-2009 で動作して，IEEE 802.1AB Draft 6 の LLDPDU だけを受信したポートからは IEEE 802.1AB Draft 6 の LLDPDU を送信します。なお，IEEE Std 802.1AB-2005 とも接続できます。規格別の受信 LLDPDU と送信 LLDPDU の関係を次の表に示します。

表 23-1　規格別の受信 LLDPDU と送信 LLDPDU の関係

受信 LLDPDU の規格		送信 LLDPDU の規格
IEEE Std 802.1AB-2009 IEEE Std 802.1AB-2005	IEEE 802.1AB Draft 6	
受信なし	受信なし	IEEE Std 802.1AB-2009※
	受信あり	IEEE 802.1AB Draft 6
受信あり	受信なし	IEEE Std 802.1AB-2009※

受信 LLDPDU の規格		送信 LLDPDU の規格
IEEE Std 802.1AB-2009 IEEE Std 802.1AB-2005	IEEE 802.1AB Draft 6	
	受信あり	IEEE Std 802.1AB-2009※

注※

System Capabilities TLV だけは IEEE Std 802.1AB-2005 の規格で送信します。

(2) サポート TLV

本装置での TLV のサポート状況を次の表に示します。

表 23-2 TLV のサポート状況

TLV name		IEEE 802.1AB Draft 6		IEEE Std 802.1AB-2009 IEEE Std 802.1AB-2005		説明
		送信	受信	送信※1	受信	
Chassis ID		○	○	○	○	装置の MAC アドレスを送信します。
Port ID		○	○	○	○	ポートの MAC アドレスを送信します。
Time To Live		○	○	○	○	本装置が送信する情報の保持時間はコンフィグレーションで変更できます。
Port Description		○	○	○	○	interface グループ MIB の ifDescr と同じ値を送信します。
System Name		○	○	○	○	system グループ MIB の sysName と同じ値を送信します。
System Description		○	○	○	○	system グループ MIB の sysDescr と同じ値を送信します。
System Capabilities		×	×	○	○	利用できる機能と有効な機能の情報を送信します。
Management Address		×	×	○	○	管理アドレスを送信します。
Organizationally-defined TLV extensions ・VLAN 情報 ・VLAN Address 情報		○	○	×	×	設定されている VLAN ID や VLAN に関連づけられた IP アドレスを送信します。
IEEE802.1 Organizationally Specific TLVs	Port VLAN ID	×	×	○	○	設定されているポート VLAN の VLAN ID 情報を送信します。
	Port And Protocol VLAN ID	×	×	○	○	設定されているプロトコル VLAN の VLAN ID 情報を送信します。
	VLAN Name	×	×	△※2	○	設定されているポート VLAN の VLAN ID，および VLAN の名前を送信し

TLV name		IEEE 802.1AB Draft 6		IEEE Std 802.1AB-2009 IEEE Std 802.1AB-2005		説明
		送信	受信	送信※1	受信	
						ます。

（凡例）　○：サポート　△：一部サポート　×：非サポート

注※1

IEEE Std 802.1AB-2009 の規格で LLDPDU を送信します。ただし，System Capabilities は IEEE Std 802.1AB-2005 の規格で送信します。

注※2

VLAN Name Length の情報を 0 で送信し，VLAN の名前は送信しません。

LLDP でサポートする情報の詳細を以下に示します。

(a)　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 23-3　Chassis ID の subtype 一覧（IEEE Std 802.1AB-2009）

subtype	種別	送信内容
1	Chassis component	Entity MIB の entPhysicalAlias と同じ値
2	Interface alias	interface MIB の ifAlias と同じ値
3	Port component	Entity MIB の portEntPhysicalAlias と同じ値，または 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	Interface name	interface MIB の ifName と同じ値
7	Locally assigned	LLDP MIB の local と同じ値

表 23-4　Chassis ID の subtype 一覧（IEEE 802.1AB Draft 6）

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：送信する subtype の種別は MAC address だけです。送信する MAC アドレスは装置 MAC アドレスを使用します。また，スタック構成時はスタックの装置 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：255 オクテット

(b)　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 23-5 Port ID の subtype 一覧（IEEE Std 802.1AB-2009）

subtype	種別	送信内容
1	Interface alias	Interface MIB の ifAlias と同じ値
2	Port component	Entity MIB の portEntPhysicalAlias と同じ値，または Entity MIB の backplaneEntPhysicalAlias と同じ値
3	MAC address	LLDP MIB の macAddr と同じ値
4	Network address	LLDP MIB の networkAddress と同じ値
5	Interface name	interface MIB の ifName と同じ値
6	Agent circuit ID	RFC3046 の Circuit ID
7	Locally assigned	LLDP MIB の local と同じ値

表 23-6 Port ID の subtype 一覧（IEEE 802.1AB Draft 6）

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 macAddr と同じ値
5	Network address	LLDP MIB の networkAddr 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：送信する subtype の種別は MAC address だけです。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：255 オクテット

(c) 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。

(d) 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：255 オクテット

(e) 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：255 オクテット

(f) 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」
  スタック構成時はマスタスイッチの sysDescr 情報を使用します。
- 受信データ最大長：255 オクテット

(g) System Capabilities（装置の機能）

利用できる機能と有効な機能を識別する情報です。この情報は規格によって subtype の有無が異なります。

IEEE Std 802.1AB-2009

subtype が定義され，subtype には chassis ID subtype を使用します。

IEEE Std 802.1AB-2005

subtype はありません。

System Capabilities についての送信内容および受信条件は次のとおりです。

- 送信
  IEEE Std 802.1AB-2005 の規格で送信します。System Capabilities TLV の送信内容を次の表に示します。

表 23-7 System Capabilities TLV の送信内容

データ名	説明	送信内容
system capabilities	機能識別子（装置が有する機能）	MAC Bridge（1）有
enabled capabilities	機能識別子のうち，有効になっている機能	MAC Bridge（1）有効

- 受信
  IEEE Std 802.1AB-2009，および IEEE Std 802.1AB-2005 の規格で受信できます。IEEE Std 802.1AB-2009 の規格では，すべての subtype について受信できます。

(h) Management Address（管理アドレス）

装置の IP アドレスや MAC アドレス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。

Management Address についての送信内容および受信条件は次のとおりです。

- 送信
  Management Address TLV の送信内容を次の表に示します。

表 23-8 Management Address TLV の送信内容

データ名	説明	設定値
management address subtype	管理アドレス種別	1：IP（IPv4 アドレス）または 2：IP6（IPv6 アドレス）
management address	管理アドレス	コンフィグレーションコマンド lldp management-address で設定したアドレスを使用します
interface numbering subtype	インタフェース番号サブタイプ	1：Unknown
OID string length	OID 情報長	0

- 受信
  すべての subtype について受信できます。LLDPDU 上に複数の Management Address TLV が付く場合は，最後の情報だけを保持します。
- 受信データ最大長
  167 オクテット

(i) Organizationally-defined TLV extensions

本装置独自に次の情報をサポートしています。

- 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。
- VLAN Address
  この情報は，該当ポートで 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。

(j) IEEE802.1 Organizationally Specific TLVs

本装置では次の情報をサポートしています。

- Port VLAN ID
  該当ポートのポート VLAN の情報です。
  アクセスポートの場合，該当するポート VLAN の VLAN ID を送信します。アクセスポート以外の場合，ネイティブ VLAN が有効なときはネイティブ VLAN の VLAN ID を送信します。受信データ最大長は，6 オクテットです。
- Port And Protocol VLAN ID
  該当ポートのプロトコル VLAN の情報です。
  プロトコルポートの場合，該当するプロトコル VLAN の VLAN ID を送信します。送信する VLAN ID の情報は，最新の状態です。プロトコル VLAN の設定がないときは，プロトコル VLAN の情報を送信しません。受信データ最大長は，7 オクテットです。
- VLAN Name
  該当ポートのポート VLAN の情報です。
  アクセスポートの場合，該当するポート VLAN の VLAN ID を送信します。トランクポートの場合，VLAN Tag の VLAN ID を送信します。また，ネイティブ VLAN が有効なときは，ネイティブ VLAN の VLAN ID も同様に送信します。アクセスポートおよびトランクポート以外の場合，各種ポートの VLAN ID を送信します。また，ネイティブ VLAN が有効なときは，ネイティブ VLAN の VLAN ID も同様に送信します。
  送信する VLAN ID の情報は，最新の状態です。また，Tag 変換を使用している場合は，変換後の VLAN ID を送信し，VLAN トンネリング機能を使用している場合は，VLAN トンネリング機能で付けた VLAN Tag の VLAN ID を送信します。受信データ最大長は，39 オクテットです。

23.1.3 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かなくなります。
- 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) 隣接装置の最大数について

隣接装置の最大収容数を超えた場合，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。

(3) スタック構成時について

スタック構成時，マスタスイッチの切り替えが発生すると，隣接装置の情報をクリアします。その後，隣接装置から LLDPDU を受信することで再学習します。

23.2 コマンドガイド

23.2.1 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 23-9 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 management-address	送信する Management Address TLV の管理アドレスを設定します。
lldp run	装置全体で LLDP 機能を有効にします。

LLDP の運用コマンド一覧を次の表に示します。

表 23-10 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。

23.2.2 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 1/0/1 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 1/0/1
   ポート 1/0/1 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 1/0/1 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。

(3) 送信する管理アドレスの設定

［設定のポイント］

管理アドレスを設定すると，設定した IP アドレスが隣接装置に通知されます。設定できる IP アドレスは，インタフェースに設定されている IP アドレスに限りません。

［コマンドによる設定］

1. (config)# lldp management-address ip 192.168.1.20
   送信する Management Address TLV の管理アドレスを 192.168.1.20 に設定します。

付録

付録A　準拠規格

付録A.1　Diff-serv

表 A-1　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.2　IEEE802.1X

表 A-2　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
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.3　Web 認証

表 A-3　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

付録A.4　MAC 認証

表 A-4　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

付録A.5　DHCP snooping

表 A-5　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.6　sFlow

表 A-6　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.7　IEEE802.3ah/UDLD

表 A-7　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.8　CFM

表 A-8　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.9　LLDP

表 A-9　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
IEEE Std 802.1AB-2009(2009 年 9 月)	IEEE Standard for Local and Metropolitan Area Networks: Station and Media Access Control Connectivity Discovery