FUJITSU

CA92344-0454-01

PRIMERGY

PRIMERGY スイッチブレード (10Gbps 18/8+2) 機能説明書

(PY-SWB105)

FUJITSU

第1章　ネットワーク設計概念

1.1　レイヤ 2 ネットワーク設計概念

1.1.1　VLAN

レイヤ2 のネットワークは、MACアドレスをもとに到達する先を制御します。
レイヤ2 のネットワークでは、VLANと呼ばれる論理的なネットワークから構成されます。
VLANを使って複数の物理的なLANから1 つの論理的なLANに構成したり、物理的に1 つのLANを複数の論理的なLANに分けたりします。各VLANにはVLAN ID（VID）をつけて管理します。

VLAN ID

各VLANには10 進数で1 から4094 までの番号をつけて管理します。これをVLAN ID といいます。同じVLAN IDを持つVLANに属している装置間では通信可能ですが、異なるVLAN ID を持つVLANに属している装置間では通信はできません。

VLANの種類

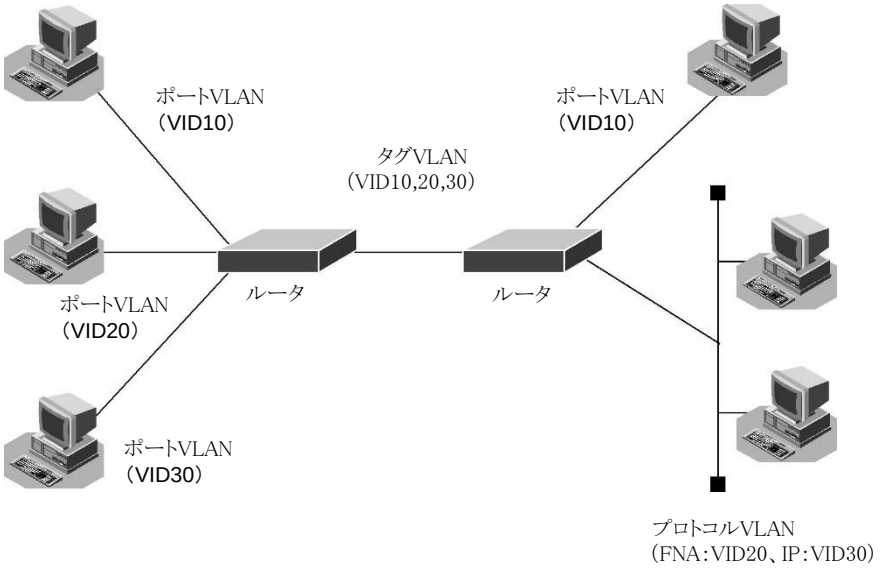
VLANには以下の3 つの種類があります。

• ポートVLAN
ETHERポートごとに「どのVLANに所属するか」を設定するものです。
そのETHERポートのデータは、すべて指定されたVLANに属します。

• タグVLAN
1 つの物理回線上に複数のVLAN を設定する場合に使用します。IEEE802.1Q で標準化された方式で、VLANヘッダをEthernet のフレームヘッダに挿入することによって、1つの物理回線上に複数のVLANを実現します。

• プロトコルVLAN
Ethernet のフレームヘッダには、フレームタイプという16 ビットのフィールドがあり、そのフレームに格納されている上位プロトコルが識別できるようになっています。たとえば、IP、IPX といった異なるネットワークプロトコルの通信をEthernetフレームのレベルで識別することができます。プロトコルVLANはこの情報を使い、ネットワークプロトコルごとに異なるVLANを定義できるようにしたものです。
たとえばIP ではサブネットワークごとにVLANを分けてルーティングを行うが、IPXプロトコルでは分割しないで全体を1 つのネットワークとして扱う、といった設定が行えます。

この3つの種類はETHERポートごとに設定を変えることができます。つまり、VLAN IDが10のVLANを、ETHERポート1ではポートVLAN、ETHERポート2ではタグVLANにするといったことができます。この場合、VLAN IDが10のVLANのデータは、ETHERポート1とETHERポート2で送受信され、ETHERポート1ではタグのない通常のフレーム、 ETHERポート2ではタグ付きのフレームとして送受信されます。



1.1.2 リンクアグリゲーション

リンクアグリゲーションとは、複数の物理回線をまとめて1本の論理回線として扱う技術です。
1本の物理回線では帯域が足りない場合、複数の物理回線をまとめて広い帯域を確保します。また、リンクアグリゲーションを構成している物理回線のうち、1本の回線が故障などの原因により通信できなくなった場合、ほかの物理回線で通信は継続できるので、冗長構成の機能もあります。
複数のVLANが含まれている場合も物理回線が1本の場合と同様に、リンクアグリゲーションで構成された論理的に1本の回線に複数のVLANが含まれる構造になります。また、STPでも1本の回線として扱い、ポートの制御などはリンクアグリゲーションの論理的な回線に対して行われます。

1.2 装置の設定の概要

ネットワークと設定の関係

本装置に設定すべき情報としては、接続する回線に関する物理的な情報、接続するネットワークに関する論理的な情報、およびデータの振り分け条件である経路情報が必ず必要となります。また、ほかに装置固有の情報や、付加的なサービスの設定を必要に応じて行います。
本装置では、これらの情報の設定に関して、大きく以下のように分類しています。

•ether定義
本装置に接続する回線に関する物理的な情報を定義する命令群です。回線の種類や速度などに関する情報を定義します。

•vlan定義
本装置のVLANに関する情報を定義する命令群です。プロトコルVLANの情報や静的な学習テーブルの情報を定義します。

•lan定義
本装置に接続するLANに関する論理的な情報を定義する命令群です。LANのIPアドレスやネットワークの情報などを定義します。また、DHCPなどのLANに固有のサービスに関してもlan定義によって定義します。

•その他の定義
装置固有の情報や付加サービスの情報を必要に応じて定義する命令群です。ネットワーク管理に関する情報や時刻情報などの定義があります。

ネットワークインタフェースの定義

データ転送時の出口となるネットワークインタフェースには、その特性や接続されている回線によっていくつかの種別があります。以下に、ネットワークインタフェースの種別について説明します。

•lo (ループバックインタフェース)
装置の内部プログラムで折り返し通信を行う場合に利用されます。

•lan (Ethernetインタフェース)
Ethernetを利用して通信する場合に利用するネットワークインタフェースです。lan定義によって設定されます。

これらのインタフェース種別にインタフェース番号を付与したものがネットワークインタフェース名となります。

例：lo0,lan0,lan1,...
lanのネットワークインタフェースはlan定義によって設定されます。lan定義の定義番号とネットワークインタフェースのインタフェース番号は1対1に対応します。

経路情報の定義

経路情報は最終的に出口となるネットワークインタフェースを決定するために必要な情報を定義するものです。本装置では出口インタフェースに対応する定義内で経路情報を設定します。たとえば、lan0から出力するための経路情報はlan0内の定義に、lan1から出力するための経路情報はlan1内の定義に分けて設定します。

第2章　機能概要

2.1 オートネゴシエーション機能

オートネゴシエーション機能とは、IEEE802.3uに規定された2装置間のプロトコルであり、優先順位に従い通信速度、通信モード（全二重／半二重）の設定を自動的に行う機能です。

• オートネゴシエーション（Auto-Nego）同士の接続は、相互に通信できるモードの中から、決められたアルゴリズムにより通信モードが設定されます。

• 固定同士の接続は、同じ通信モードのときだけ正常に通信できます。

こんな事に気をつけて

• 一方がオートネゴシエーションで、他方がFULL（全二重）の固定で接続すると、通信モードはHALF（半二重）と認識されます。この場合、エラー率が高いなど正常な通信ができないことがありますので、通信モードを正しく設定してください。

• 一方または両方の通信モードがオートネゴシエーションで、お互いが認識できない場合は、両方の通信モードを固定に設定してください。

• 一方が10M固定、他方を100M固定で誤接続すると、片方の装置だけがリンク確立したり、通信状態によってはリンクが確立と切断を繰り返したりする場合があります。 この場合は通信モードを正しく設定してください。

• 10Gポートには、速度を決定するオートネゴシエーション機能はありません。

2.2 フロー制御機能

本装置では、IEEE802.3x に基づくPause フレームによるフロー制御機能をサポートしています。
フロー制御の設定による各ポートの動作を以下に示します。

こんな事に気をつけて

フロー制御を適用した場合、接続相手が本装置の該当ポートにフレーム送信できなくなることがあります。この場合、接続相手のバッファ容量によって、本装置に設定している優先機能の優先度に関係なくフレーム廃棄されることがあります。このため、音声や画像などを使用するネットワークの場合は、フロー制御を無効にしてください。
また、接続相手によっては、データフレームの転送性能が劣化することがあります。
フロー制御で PAUSE フレームを送信するかどうかは、入力ポートの受信バッファ残量で判断されます。buffermode qos や ratecontrol 等で出力キューの長さが制限されているポートに転送されるフレームは出力キュー側で廃棄されるため、入力ポートの受信バッファには溜まりません。結果として、フレームが廃棄されるにも関わらず Pause フレームは送信されません。フロー制御を確実に行うためには buffermode max に設定し、ratecontrol の設定がされたポートに転送されることもないようにしてください。

<固定モードの場合>

フロー制御設定		通信モード	システム動作	
送信	受信		送信方向	受信方向
Off 設定	Off 設定	全二重固定	Pause フレーム送出なし	Pause フレーム受信時は、フロー制御を実行しない（※ 1）
On 設定	Off 設定	全二重固定	フロー制御のため Pause フレームを送信する。	Pause フレーム受信時は、フロー制御を実行しない（※ 1）
Off 設定	On 設定	全二重固定	Pause フレーム送出なし	Pause フレーム受信時は、フロー制御を実行する。
On 設定	On 設定	全二重固定	フロー制御のため Pause フレームを送信する。	Pause フレーム受信時は、フロー制御を実行する。

※ 1）Pause フレーム受信時は無視する。

2.3 フォワーディングモード変更機能

本装置では、スイッチングの方式として、カットスルーモードとストアアンドフォワードモードを選択することができます。

カットスルーモード

本装置にパケットの先頭部分が入力した後に転送先のポートからパケットを送出します。パケットの全体が入力するのを待たずに転送が行われるため、転送に伴うパケットの遅延(レイテンシ)を最小限に抑えることができます。

ストアアンドフォワードモード

本装置にパケットの全体が入力した後に転送先のポートからパケットを送出します。

こんな事に気をつけて

カットスルーモードを選択した場合には、レイテンシが短縮できる半面、エラーパケットを中継してしまいます。ストアアンドフォワードモードの場合はエラーパケットが入力されても中継しませんが、半面レイテンシはパケットデータを蓄積する分だけカットスルーモードより長くなります。

2.4 MAC アドレス学習/MAC フォワーディング機能

本装置では、MACアドレス学習機能として以下の機能をサポートしています。・

MACアドレス学習基本機能

受信パケットの送信元MACアドレスをダイナミックに学習して、FDB（Forwarding Data Base）に登録する機能です。登録したMACアドレスは、エージングアウト時間まで保持し続けます。エージングアウト時間は構成定義コマンド　で変更できます（初期値は300秒）。ポートがリンクダウンした場合は、FDB上の該当ポートから学習したエントリを削除します。

MACアドレス自動学習停止機能

構成定義によって、装置単位でダイナミックなMACアドレスの学習を停止する機能です。

FDBクリア機能

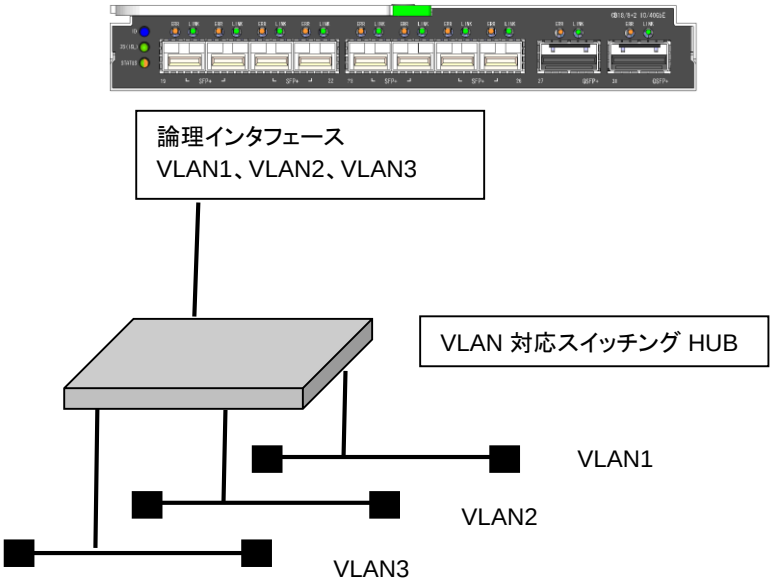
ダイナミックに学習したFDBエントリを削除する機能です。ポート単位、MACアドレス単位など条件指定することもできます。

スタティックMACフォワーディング機能

特定のあて先アドレスを持つフレームをVLANごとに指定したポートへ中継できる機能です。あて先アドレスにはユニキャストアドレスが指定できます。

2.5 VLAN 機能

VLAN機能とは、物理的なLANを仮想的な複数のLANに分割し、ポート、MACアドレス、プロトコルなどでグループ化を行う機能です。



装置内VLAN

VLANは、タギング方式と呼ばれるVLANグループ識別方法を用いた通信方式を規定しています。
タギング方式とは、フレームにVLANタグを付与することでそのフレームがどのVLANに属するのかを識別する方法です。識別子として定義されたものをVLAN ID といい、VLANを1つ定義した場合、それに対応するVLAN IDも1つ割り当てます。本装置でサポートするVLAN機能は、IEEE802.1q に準拠しています。
本装置は、VID=1に、すべてのポートがVLAN1のタグなしとして初期設定されていますが、各ポートを特定のVLANのタグ付きまたはタグなしに設定を変更することができます。

VLANとネットワークアドレス

VLAN機能を使用した場合、ブリッジング通信はそのVLAN内に閉じたものになります。したがって、VLANを定義するということは、MACアドレスのレベルでブロードキャストフレームが届く範囲（ブロードキャストドメイン）を制限するということになります。
また、これをネットワーク層の位置から考えると、以下の2つのことができます。

- 各物理ポートに、VLANタグを使用して複数のネットワークアドレスを対応させる。
- 複数の物理ポートを束ねたものに、1 つのネットワークアドレスを割り当てる。

VLAN種別

本装置がサポートするVLAN機能では、以下の2 つの単位でVLANを分けることができます。

•ポートVLAN

ポート単位でグループ化を行う機能です。すべてのネットワークプロトコルのアドレスを付与することができます。

•プロトコルVLAN

特定のプロトコルに基づいてポートをグループ化する機能です。プロトコルVLANで指定可能なプロトコルの種類は以下のとおりです。

- IP
- IPv6

また、フレームタイプを直接指定することによって、任意プロトコルのプロトコルVLANを作成することができます。

例）IPX（Ethernet Ⅱ形式EtherType 値[0x8137,0x8138] 指定）、

VLANタグとポートの関係

VLAN機能を使用する場合、あらかじめVLAN内のポートに、フレームを送信するときにVLANタグを付与するか定義しておきます。付与するかどうかは、各ポートの先にあるノードがVLANタグを識別できるかどうかによって決まります。

VLAN機能を使用している場合、本装置の各ポートの先に接続されたセグメントは、以下の3 つのどれかに属しています。

• アクセスリンク

VLANタグなしのフレームだけが流れる区間です。VLANタグを理解できないエンドノードが接続されます。

• トランクリンク

VLANタグ付きフレームだけが流れる区間です。タグ付きVLAN機能をサポートしている装置どうしは、通常トランクリンクで接続します。VLANタグを理解できないエンドノードは接続されません。

• ハイブリッドリンク

VLANタグ付きのフレームとVLANタグなしのフレームの両方が流れる区間です。ここには、複数のVLANが存在し、それぞれのVLANにとってアクセスリンクまたはトランクリンクとなります。ただし、特定のプロトコルに注目した場合、ハイブリッドリンクをアクセスリンクとして運用できるVLANは1 つだけです。たとえば、1 つのハイブリッドリンク上に2 つのVLANがアクセスリンクとして運用している場合に、IP プロトコルに注目すると、そのうちの1 つしか認識することができません。

こんな事に気をつけて

• 特定のプロトコルに対して、2 つ以上のVLANをアクセスリンクとして運用する場合、それぞれのVLANから送信されるフレームにはVLANタグが付与されていないため、属するVLANを識別することができません。

• スパニングツリー機能と併用する場合、ブリッジフレームおよびルーティングフレームはスパニングツリーの制　限に従います。

・プロトコルVLAN定義を装置に設定可能な上限を超える設定をした場合、上限を超えたプロトコルVLAN定義、およびプロトコルVLAN定義に指定したVLAN IDは無効となり、無効とされたVLAN IDに所属するすべてのポートは利用できなくなります。なお、プロトコルVLAN定義の装置に設定可能な上限は16個です。

同一ポート上での VLANの混在

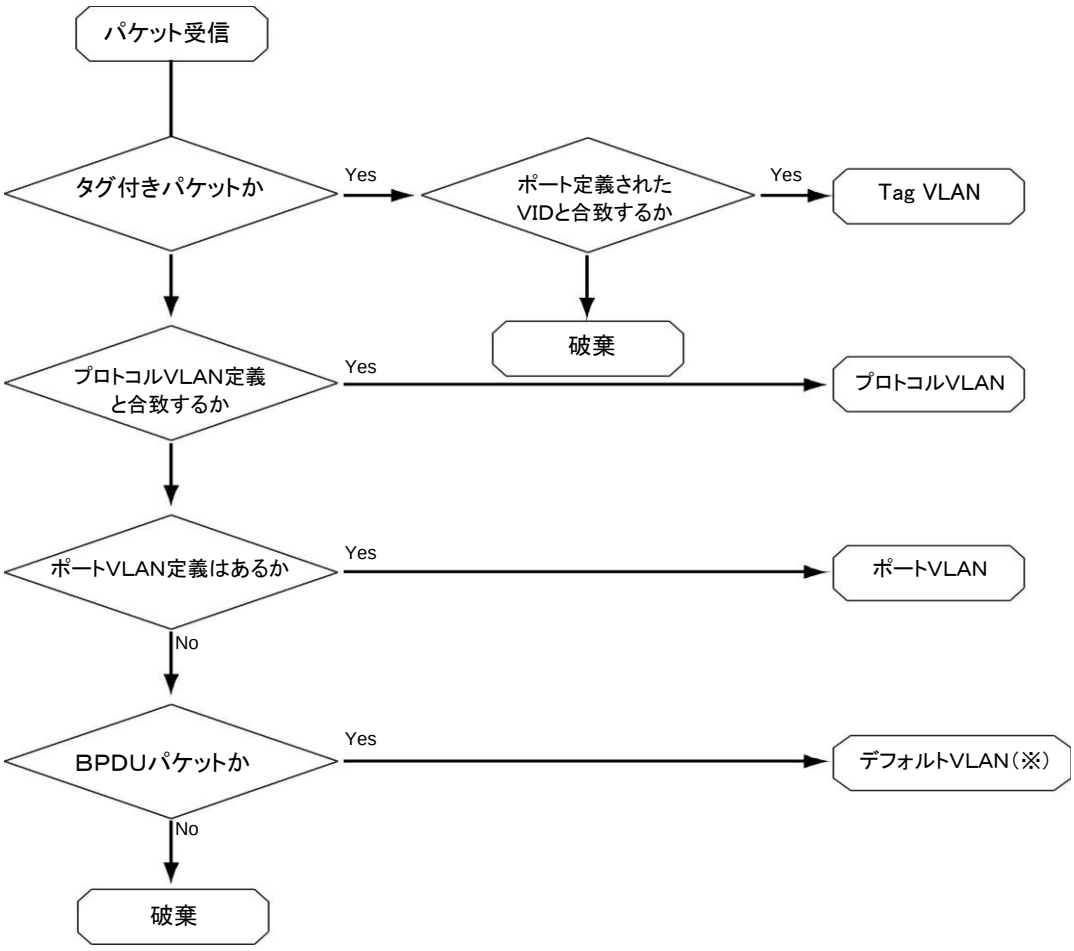
同一ポート上で使用できるVLANの組み合わせを以下に示します

○　：混在できる、×：混在できない

VLAN種別	ポートVLAN（untagged）	プロトコルVLAN	Tag VLAN（Tagged）
ポートVLAN（untagged）	×	○	○
プロトコルVLAN	○	○	○
Tag VLAN（Tagged）	○	○	○

パケット受信時のVLAN判定

VLANを設定したポートでパケットを受信した場合、受信したパケットの所属するVLANの判定を以下の順序で行います。



※）本装置では、構成定義でTag VLAN／プロトコルVLANが定義され、かつ、ポートVLAN（untagged）が未設定のポートに対しては、BPDUパケットを受信するために装置内でデフォルトVLANを作成します。

パケット送信時のVLANタグ

パケット送信時のVLANタグの扱いは、送信するポートのTagged／Untagged設定に従って、Taggedポートの場合はVLANタグを付与し、Untaggedポートの場合はVLANタグを付与しないで送信します。

VLANトランク機能

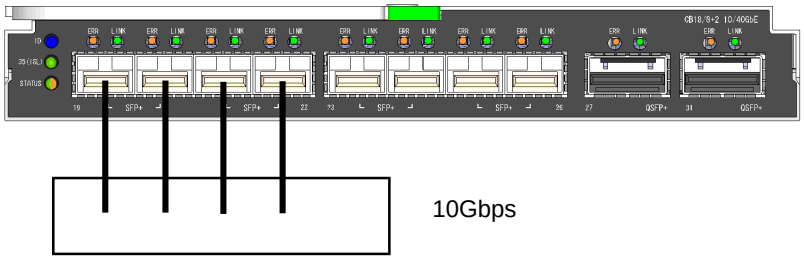
VLANトランク機能とは、VLANタグの付与および削除が可能なスイッチがVLAN間の通信を行う際に使用する機能です。複数のVLANに属するポートからルーティングするために、ほかのレイヤ3スイッチへ中継します。ポートでは、どのVLANに属しているかを認識するためにVLANタグを付け、レイヤ3スイッチでVLANタグ付きフレームを受け取り、ルーティングして中継します。

装置間VLAN

VLANが装置間をまたぐ場合、フレームにVLANタグを付けてどのVLANからきたフレームかを区別します。これによって、たとえばVLAN Aどうし、VLAN Bどうしは、それぞれ同じスイッチングHUBに接続されているように通信することができます。また、VLANトランク機能を使用することによって、通常2本必要な伝送路が本装置間を1本で接続することができます。

2.6 リンクアグリゲーション機能

リンクアグリゲーション機能とは、複数のポートを多重化し、1 本の高速リンク（トランク・グループ）として扱うための機能です。この機能を使用すると、多重化されたリンク（メンバポート）の1 本が故障した場合に、そのトラフィックをほかのメンバポートに分散することによって、リンクの冗長性を高めることができます。リンクアグリゲーション機能は、マルチリンクイーサまたはポート・トランキングとも呼ばれます。また、メンバポートを構成する場合は、1～10本のポートで構成します。
すべてのメンバポート同じVLAN構成となるよう設定してください。



40Gbps 帯域仮想リンク

トランク・グループへのトラフィックは、送信パケットのMACアドレスまたは、IPアドレスで判断し、負荷分散します。
以下の方式から選択して指定することができます。

- 送信先MACアドレスと送信元MACアドレスを元にした負荷分散
- 送信先MACアドレスを元にした負荷分散
- 送信元MACアドレスを元にした負荷分散
- 送信先IPアドレスと送信元IPアドレスを元にした負荷分散
- 送信先IPアドレスを元にした負荷分散
- 送信元IPアドレスを元にした負荷分散

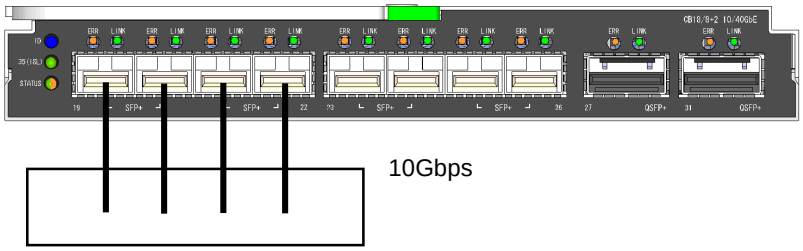
トランク・グループを通信可能とさせるまでの最小メンバポート数を指定することができます。
トランク・グループのメンバポートが指定した数だけ有効となるまでトランク・グループの通信を抑止します。
たとえば、リンクダウンしたメンバポートなどは有効なポートに含まれません。
冗長構成などでトランク・グループを必要な帯域が確保できるまで通信させたくない場合に使用します。
なお、この機能はLACPと併用することができます。

こんな事に気をつけて

- 多重化されたポートは、論理的な 1 本のポートとして扱われます。STP や VLAN 機能を併用した場合も同じです。
- STP のコスト値は、メンバポートの帯域およびメンバー数より算出し、コスト値を割り当てます。縮退／復旧によってコストが変わることはありません。

2.6.1 LACP 機能

LACP機能とは、IEEE802.3 準拠のLACPを利用したリンクアグリゲーションです。LACPを取り付けたシステム間で実現可能な最大レベルのリンクアグリゲーションを継続的に提供します。
LACPの利用によってリンクアグリゲーションの整合性確認や、リンクの正常性確認、障害検知の確度を向上できます。



40Gbps 帯域仮想リンク

導入のメリット

• 隣接装置と整合性を確認するので、たとえばポートを差し間違えていたといったようなミスがあった場合でも、プロトコルレベルで一本一本正しいリンク先に接続されていることを確認しながら通信を開始します。そのため誤った接続先へ通信してしまうことがありません。
• 隣接装置からのLACPパケットが一定時間受信されない場合は、リンク異常と判断するので、装置ポートの異常検出範囲を超えたリンクの障害検知が可能です。

こんな事に気をつけて

• LACPを利用したリンクアグリゲーションは、接続先もLACPを有効にする必要があります。リンクアグリゲーション動作モードにstatic を指定したなどのLACP以外のリンクアグリゲーションとは接続できません。
• リンクアグリゲーション動作モードにpassive を指定して、接続先も同様にpassive とするとリンクアグリゲーシ ョンは構成されません。どちらか一方はactive と指定してください。双方をactive と指定してもかまいません。
その他の注意事項については、「2.6 リンクアグリゲーション機能」を参照してください。

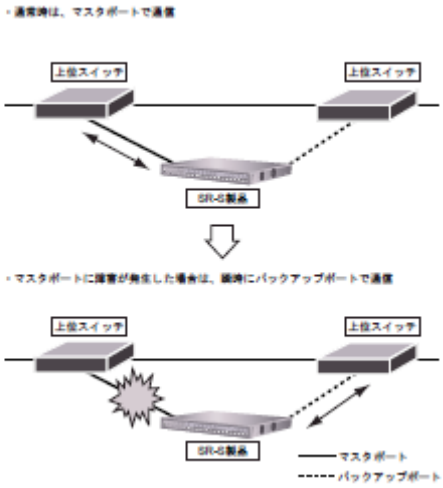
2.7 バックアップポート機能

バックアップポート機能とは、2 つのポートをグループ化し、片方のポートをマスタポート（優先ポート）、もう一方のポートをバックアップポート（待機ポート）として管理し、つねにどちらか一方のポートだけを稼動させる機能です。

稼動中のポートになんらかの障害が発生した場合に、もう一方の待機ポートを瞬時に稼動ポートに切り替えることで、ネットワーク障害の影響を最小限に抑えることが可能です。

グループポートが共にリンクアップしている状態で、マスタポートを必ず優先使用するモードと、先にリンクアップしたポートを使用するモードの選択が可能です。

また、バックアップポートとしてリンクアグリゲーションを使用することも可能です。



こんな事に気をつけて

- バックアップポート機能では、障害発生時に稼動ポートを瞬時に切り替えることが可能ですが、各種プロトコルを使用した場合、通信が復旧するまでに各プロトコルでの復旧時間が必要となります。
- リンクアグリゲーションと併用した場合で、そのリンクアグリゲーションがバックアップ構成として不整合な設定 であった場合は、リンクアグリゲーションとしても無効となります。
- 待機ポートの待機状態をoffline と設定した場合、待機ポートはリンクダウンしているため、回線抜けなどの異常が発生しても検出はできません。切り替わり動作後に異常検出となります。

2.8 STP 機能

STP 機能とは、異なるLANを接続し、MACフレームを中継する機能です。
本装置では、以下の機能をサポートしています。

2.8.1 STP

スパニングツリー機能とは、物理的にループを構成するブリッジ構成で、複数ある経路のうちの1 つだけを通信経路とし、論理的にツリー構造のネットワークを構成する機能です。この機能を使用することによって、システムダウンにつながるようなフレームのループは発生しません。また、使用している経路上になんらかの障害が発生した場合は、自動的にほかの経路を用いてツリー構造を再構成するため、障害に強いネットワークが構築できます。

ヒント 以下にスパニングツリーを構成するうえで重要な語句を説明します。

◆ スパニングツリーを構成するブリッジ

- ルートブリッジ

システム中で最小のブリッジ識別子を持つブリッジをルートブリッジと言います。ルートブリッジはツリー構造の頂 点に位置し、システム中に1 台だけ存在します。

- 代表ブリッジ

1 つのLANに接続された複数のブリッジの中で、最小のルートパスコストを持つブリッジ（ルートブリッジに近い）をそのLANの代表ブリッジと言います。ルートブリッジは接続されているすべてのLAN上で代表ブリッジとなります。

◆ スパニングツリーを構成するブリッジのポート

- ルートポート

フォワーディング状態のポートであり、各ブリッジで最小のルートパスコストのポートがルートポートとなります。ルートポートは、それぞれのブリッジに必ず1つ存在します。

- 代表ポート

フォワーディング状態のポートです。1 つのLAN上に複数接続したポートの中に1 つだけ存在します。ルートブリッジのすべてのポートは、接続されたLAN上の代表ポート（代表ブリッジ）となります。

- ブロッキングポート

ブロッキング状態のポートであり、MACフレームは中継しません。ルートポートでも代表ポートでもないポートがブロッキングポートとなります。

＜フレームの中継動作＞

- フォワーディング

MACフレームを中継します。また、MACアドレス情報の学習を行います。

- ブロッキング

MACフレームは中継しません。また、MACアドレス情報の学習を行いません。

◆ ツリー構造を構成するための要素

• ブリッジ識別子

ブリッジ識別子は、最小のブリッジプライオリティ（任意に指定）とポート番号のポートが持つMACアドレスの2 つのフィールドから構成されます。ブリッジ識別子とルートパスコストにより、構成するツリー構造の各ブリッジの優先度を決めます。同じ値のブリッジプライオリティが設定されたブリッジは、MACアドレスにより識別されますが、通常はブリッジプライオリティ＝ブリッジ識別子となります。

ブリッジプライオリティ	MACアドレス
2オクテット	6オクテット

• ルートパスコスト

各経路にコストが割り当てられると、各ブリッジはそのブリッジからルートブリッジへ達するいくつかの経路にそれぞれ対応して、1 つまたは複数のコストを持ちます。この中で最小のコストをブリッジでのルートパスコストと言います。

• 構成BPDU

論理的なツリー構造を構成するためにブリッジ間でやり取りされるブリッジ・プロトコル・データ・ユニット（Bridge Protocol Data Unit）です。ルートブリッジに接続しているすべてのネットワークに、構成BPDUを定期的に送出します。

＜ポートによる構成BPDUの制御＞

- 代表ポート

構成BPDUを定期的に送信します。

- ルートポート

構成BPDUを受信しますが、送信しません。

- ブロッキングポート

構成BPDUを受信しますが、送信しません。

• STPドメイン

1 台のルートブリッジを頂点として、スパニングツリーが動作しているエリアをSTPドメインと言います。構成BPDUの送受信をポートごとに停止できるブリッジは、構成BPDUの送受信を停止することにより、そのポートを境界にSTPドメインを分離することができます。

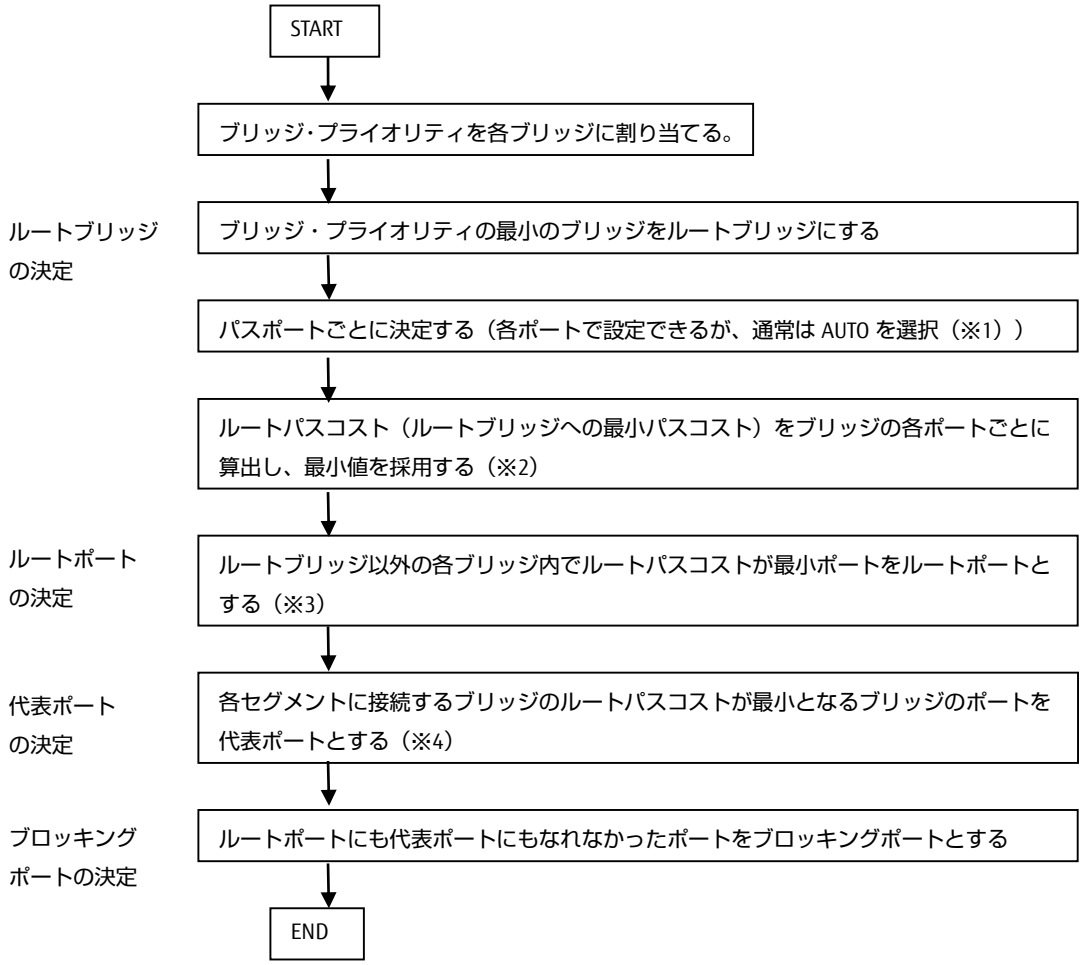
ドメインを分離する設定にしたポートはSTP動作を行わず、ツリーを構成しません。

ポートの種類と状態を以下に示します。

	ポート状態	ＭＡＣフレームの中継	ＭＡＣアドレスの学習	構成ＢＰＤＵの送受信	備考
代表ポート	フォワーディング状態	する	する	定期的に送信する	LAN上に１つ存在 ルートブリッジは すべてのポート
ルートポート	フォワーディング状態	する	する	受信する 送信しない	ルートブリッジ以外 のブリッジに必ず１つ 存在
ブロッキングポート	ブロッキング状態	しない	しない	受信する 送信しない	代表ポート、 ルートポート 以外のポート
	リスニング状態	しなし	しない	受信する 送信する	
	ラーニング状態	しない	する	受信する 送信する	

ルートポート・代表ポート・ブロッキングポートの決定手順

各種ポートの決定手順を以下に示します。



※1）AUTO 選択時のデフォルトコスト値を以下に示します。

伝送速度	デフォルトパスコスト
10G	2000
40G	200

リンクアグリゲーションの場合は、伝送速度が 10G/40G の場合は 200 になります。

※2）・ルートパスコストは、ルートブリッジからの経路で構成 BPDU パケットが入力するポートのパスコストの合計であり、最小値を採用します。

・ルートブリッジのパスコストは 0 です。

※3）・ルートポートは、ブリッジごとに 1 つ存在します。

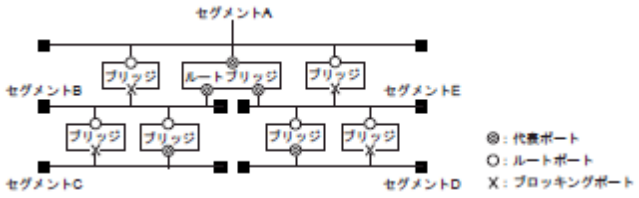
・ルートパスコストが同じ場合、ポート識別子が小さいポートを採用します。

※ 4）・代表ポートは、セグメントごとに 1 つ存在します。

・最小値となるポートが 2 ポート以上ある場合、ブリッジプライオリティが小さいブリッジのポートを採用します。

スパニングツリーでのフレームと構成BPDUの流れ

以下のような構成（ポート状態）になるように、各ブリッジのブリッジプライオリティ、パスコストを設定した場合のフレームと構成BPDUの流れについて説明します。



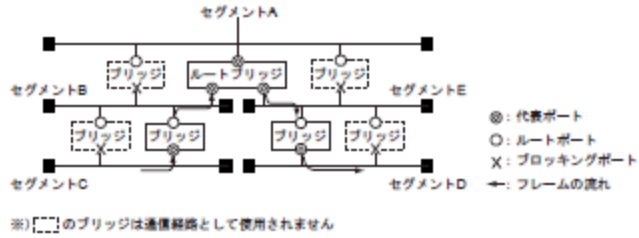
スパニングツリーでのフレームの流れ

ノードから発信したフレームは、そのセグメント上の代表ポートを持つブリッジ（代表ブリッジ）が中継します。フレームを受け取った代表ブリッジは、あて先MACアドレスにより、どのセグメントに中継するかを判断し（MACアドレス学習機能）、該当するセグメントにルートポートを介してフレームを中継します。ブロッキングポートを介してフレームは中継しません。

その先のブリッジでも同様に中継しますが、ルートブリッジがフレームを受け取った場合、代表ポートを介して次のセグメントにフレームを中継します（ルートブリッジのポートはすべてのLANに対して代表ポートです）。

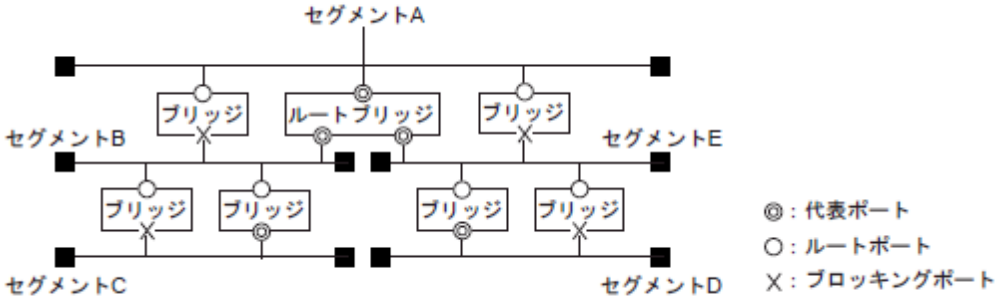
そのため、その先でフレームを中継するブリッジはルートポートでデータを受け取り、代表ポートを介して次のセグメントにフレームを中継します。ルートポートを持つブリッジがセグメント上に複数存在する場合、経路をブロッキングポートで1 つに制限し、ルートブリッジ方向またはほかの経路に再びフレームは中継しません。

上の図のセグメントCからセグメントDへの通信のフレームの流れを以下の図に示します。セグメント上は、図のような通信経路だけとなり、フレームはループしないであて先に中継します。



スパニングツリーでのフレームと構成BPDUの流れ

以下のような構成（ポート状態）になるように、各ブリッジのブリッジプライオリティ、パスコストを設定した場合のフレームと構成BPDUの流れについて説明します。

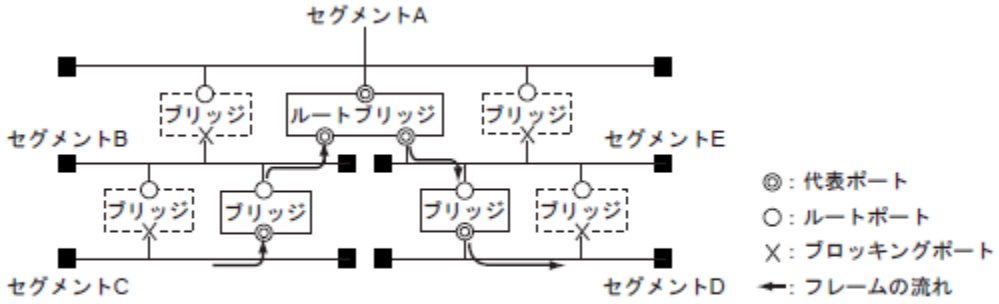


スパニングツリーでのフレームの流れ

ノードから発信したフレームは、そのセグメント上の代表ポートを持つブリッジ（代表ブリッジ）が中継します。フレームを受け取った代表ブリッジは、あて先MACアドレスにより、どのセグメントに中継するかを判断し（MACアドレス学習機能）、該当するセグメントにルートポートを介してフレームを中継します。ブロッキングポートを介してフレームは中継しません。

その先のブリッジでも同様に中継しますが、ルートブリッジがフレームを受け取った場合、代表ポートを介して次のセグメントにフレームを中継します（ルートブリッジのポートはすべてのLANに対して代表ポートです）。そのため、その先でフレームを中継するブリッジはルートポートでデータを受け取り、代表ポートを介して次のセグメントにフレームを中継します。ルートポートを持つブリッジがセグメント上に複数存在する場合、経路をブロッキングポートで1 つに制限し、ルートブリッジ方向またはほかの経路に再びフレームは中継しません。

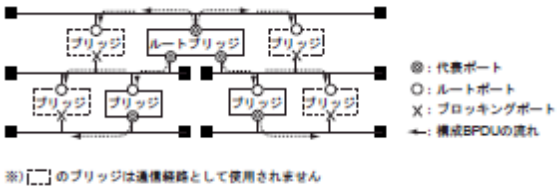
上の図のセグメントCからセグメントDへの通信のフレームの流れを以下の図に示します。セグメント上は、図のような通信経路だけとなり、フレームはループしないであて先に中継します。



※）[ ] のブリッジは通信経路として使用されません

スパニングツリーでの構成BPDUの流れ

ルートブリッジは、Hello タイム（1 ～ 10 秒（推奨値2 秒））間隔で接続しているすべてのネットワークに構成BPDUを送出します。構成BPDUは、グループMACアドレス800143000000 を持っており、それぞれのブリッジはこのグループMACアドレスを認識します。このとき、代表ブリッジはパスコストとタイミング情報を更新し、構成BPDUを下流へ転送します。構成BPDUはルートブリッジから発信され、ツリー構造に沿ってすべてのネットワークに行き渡ります。スパニングツリー構成は、構成BPDUの代表ブリッジからの定期的な送信により維持されます。



ツリー構造の再構成

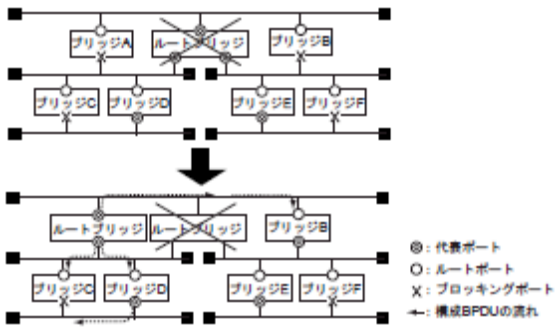
スパニングツリーのツリー構造は、構成BPDUで維持します。以下のような原因により、タイマ値STP bridge Max age（推奨値20 秒）以内に、この構成BPDUが下流のブリッジに届かなかった場合、ブリッジは障害と判断し、ツリー構造を再構成します。

- ルートブリッジがダウンし、システム全体で構成BPDUの受信が停止
- ツリー構造の上流に位置するブリッジがダウンし、その下流で構成BPDUの受信が停止

以下の図でルートブリッジがダウンした場合のツリー構造の再構成について説明します。

新ルートブリッジの決定

ルートブリッジがダウンした場合、システム中でルートブリッジの次に小さいブリッジプライオリティを持つブリッジが新ルートブリッジとなります。新ルートブリッジは、接続した各LANに構成BPDUを送信し、それを受け取った各ブリッジにより、ツリー構造を再構成します。以下の図では、ブリッジAが新ルートブリッジに切り替わることを示しています。



ブロッキングポートの中継可能状態への変化

ツリー構造の再構成にともない、ブロッキングしているポートが中継できる状態に変化します。しかし、すべてのブリッジに新しい構成BPDUが届いていない状態で、1 部のブリッジのポート状態が変化すると、ループ状態となることがあります。そのため、ポートがブロッキング状態からフォワーディング状態に切り替わる間、中間的なポート状態を置き、すべてのブリッジのツリー構成情報を更新し、ツリー構造が確立するのを待ちます。ブロッキング状態からフォワーディング状態に切り替わるまで以下の2 つの中間状態があります。それぞれの中間状態の待ち時間STP bridge forward delay（推奨値15 秒）でポート状態が変化します。

＜中間状態＞

• リスニング状態

MACフレームを中継しません。また、MACアドレス情報の学習を行いません。構成BPDUを受信します。必要であれば送信します。

• ラーニング状態

MACフレームを中継しませんが、MACアドレス情報の学習は行います。構成BPDUを受信します。必要であれば送信します。

したがって、以下のブリッジBのブロッキングポートは、フォワーディング状態になる前に、リスニング、ラーニング状態で構成BPDUを下流へ送信します。

ポート状態変化の待ち時間

ポートがブロッキング状態からフォワーディング状態に切り替わる待ち時間の合計は、以下の式により算出できます。待ち時間のパラメタに、推奨値を採用する場合は、約50 秒（20 ＋ 15 × 2）でフォワーディング状態に切り替わります。

ツリー構造の確立

ツリー構造の再構成によって、ポート状態が変化したブリッジは、構成変更を通知する構成BPDUを、ルートポートを介して上流ブリッジに送信します。構成変更通知BPDUはツリー構造に沿って上流ブリッジに中継され、最終的にルートブリッジまで中継されます。

構成変更通知BPDUを受信したルートブリッジは、定期的に送信している構成BPDUの中の構成変更フラグをONにして各ブリッジに送信します。構成変更フラグがONとなった構成BPDUを受信したブリッジは、MACアドレス学習テーブルのエントリ（通常は5 分でタイムアウト）を早めに削除するために、各エントリのタイムアウト値をSTP bridge forward delay（転送遅延）に変更し、学習テーブルを短時間で更新します。以上の動作でツリー構造は動的に再構成します。

スパニングツリー機能を利用したネットワーク設計

スパニングツリーでのパラメタ

スパニングツリーでは、設計したツリー構成やツリー性能を実現させるために、いくつかのパラメタをブリッジに設定します。このパラメタにより、ツリー構成とツリー性能を決定します。

＜ツリー構成を決定するパラメタ＞

以下のパラメタにより、ツリー構成を決定します。

パラメタ	設定対象	備考
ブリッジプライオリティ（STP bridge priorty）	ブリッジごと	ブリッジごとに設定し、小さい値を設定したブリッジを優先経路として使用します。ルートブリッジとなるブリッジには、システムの中での最小値を設定します。
ポート識別子（STP port identifier）	ポートごと	ルートパスコストとブリッジ識別子の判断がつかない場合は、ポート識別子のし異彩ポートが代表ポートとなります。ただし、ブリッジ識別子には、MAC アドレスが含まれているため、ポート識別子で代表ポートが決定することはほとんどありません。
パスコスト（STP port path cost）	ポートごと	ルートポート（上流ブリッジへの経路）を決めます。パスコストとブリッジプライオリティにより代表ポート（代表ブリッジ）を決めます。ブリッジでポートごとに設定し小さい値のルートが選択されます。伝送速度の遅いルートは高いコストを設定し、バックアップ用にします。パスコストは、デフォルト値（1000÷伝送速度 Mbps）を用いることをお勧めします。

＜ツリー性能を決定するパラメタ＞

以下のパラメタにより、ツリー性能（障害時のルート変更時間など）を決定します。

パラメタ	設定対象	備考
Hello タイム（STP bridge hello time）	ブリッジごと	ルートブリッジがツリー構成を確認するために発信する構成 BPDU の送出間隔です。推奨値は 2 秒です。
最大寿命 (STP bridge Max age)	ブリッジごと	構成 BPDU が届かなくなったためにツリーの再構成を始めるタイマ値です。ツリー構成の末端のブリッジに届くまでの遅延時間により異なりますが、推奨値は 20 秒です、同じタイミングで再構成するために、同じネットワーク内のブリッジは同じパラメタで設定します。
転送遅延 (STP bridge forward delay)	ブリッジごと	ブロッキング状態からフォワーディング状態に切り替わるまでの中間状態での待ち時間です。 この時間が短い場合、リスニング状態でツリー構成全体の同期がとれなくなります。 ラーニング状態では、MAC アドレス学習テーブルの学習が不十分なために、すべてのポートに中継してします場合やループ状態になる場合があります。また、時間が長い場合は、ツリーの再構成に必要とする時間が長くなります。推奨値は 15 秒です。

＜その他のパラメタ＞

パラメタ	設定対象	備考
STP ドメインの分離 (STP domain Separation)	ポートごと	ブリッジの各ポートに、STP ドメインを分離するかどうかを設定します。 STP ドメインを分離すると、そのポートから構成 BPDU の送信を停止します。 STP ドメインを分離する設定にしてポートは STP ツリーを構成しません。 ただし、構成 BPDU 以外のフレームは中継します。 ON：STP ドメインを分離しない、 OFF：STP ドメインを分離する、で設定します。

スパニングツリーでのネットワーク設計のポイント

スパニングツリー機能を使用して、ツリー構成を設計するポイントを以下に説明します。

＜ルートブリッジの決定のポイント＞

まず、ルートブリッジを決め、システム内で最小のブリッジプライオリティを設定します。ルートブリッジはツリー構造の頂点に位置し、トラフィックが集中する傾向にあるため、ルートブリッジを決める場合は以下の点に注意してください。

• 各セグメントのトラフィックが均一になるようにバックボーン（FDDI など）に近いブリッジをルートブリッジとします。

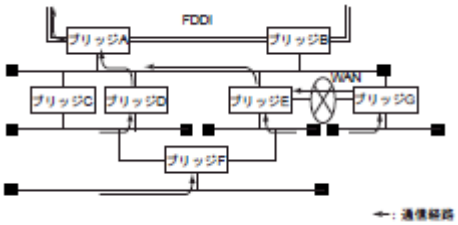
• むだなトラフィックがルートブリッジを経由しないようにエンドノートの配置に注意します。たとえば、常に通信しているような端末や大量のトラフィックを通信する端末はルートブリッジを経由しないように配置します。

＜ルートブリッジの障害時の対応＞

障害が起き、ルートブリッジがダウンすると、ツリーは新ルートブリッジで再構成します。ただし、新ルートブリッジの位置により、ツリー構成がすべて変わる場合があります。そのため、ルートブリッジの障害を想定し、ツリー構成の変更が小さい新ルートブリッジを決め、システム中で2 番目に小さいブリッジプライオリティを設定します。

スパニングツリーでのツリー構成の設計

スパニングツリー機能を使用するツリー構成の設計について、以下の構成例を用いて説明します。



＜ツリー構成範囲の決め方＞

ブリッジの中でツリー構成（スパニングツリー動作範囲）に組み込むブリッジを決めます。まず、ブリッジEからWANの先に位置するブリッジGは、ツリー構成に含む必要もなく、WAN回線上に余計なトラフィック（構成BPDU）を流さないために、ブリッジEのWAN側のポートでSTP ドメインを切り離します。なお、FDDIの先にはツリー構成に入るブリッジが存在しないため、ブリッジA、ブリッジBのFDDI ポートもSTP ドメインを切り離します。

＜ルートブリッジの決定（ブリッジプライオリティの設定）＞

ツリー構成を設計する場合は、まずルートブリッジを決める必要があります。上の図のネットワーク構成では、ブリッジAとブリッジBがバックボーンとなるFDDI に接続しており、ブリッジAをルートブリッジに、ブリッジBをルートブリッジ障害時の新ルートブリッジになるように設計します。よって、ブリッジAに1 番小さなブリッジプライオリティを、ブリッジBに2 番目に小さいブリッジプライオリティを設定します。

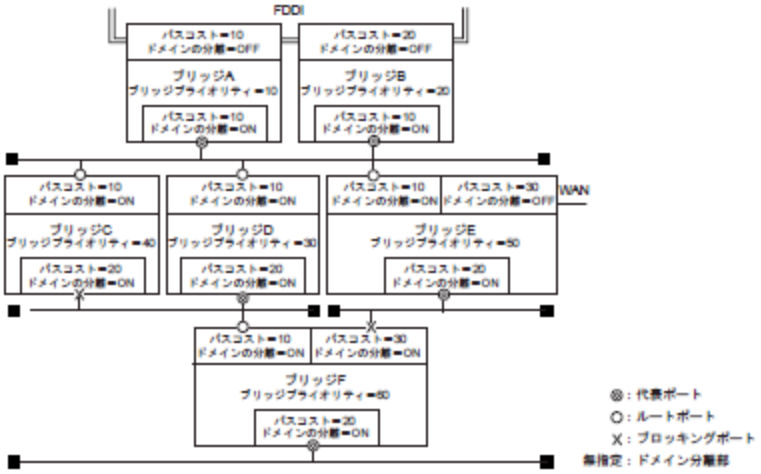
その他のブリッジは実現する通信経路を考慮し、ルートブリッジに近い上流ブリッジより、小さな値を設定します。

＜ポートの設計（パスコストの設定）＞
各ブリッジのポートごとにパスコストを設定し、ブリッジのポート状態を設計します。ルートパスコストがポート状態を確立します。ルートパスコストは以下の計算により算出できます。

＜ルートパスコストの算出＞
　各ブリッジのポートごとに「代表コスト＋パスコスト」を算出し、各ブリッジ中で最小の値をそのブリッジのルートパスコストとします。

・代表コスト
そのポートが接続しているLAN上の代表ブリッジのルートパスコストです。構成BPDUの受信により、各ポートに自動的に設定されます。設計上でルートパスコストを意識することは困難です。そのため、設計段階ではルートパスコストを使用せず、ブリッジプライオリティとパスコストでポート状態を設計します。たとえば、LAN上に2 台のブリッジが存在した場合、経路とするブリッジの方を他方のブリッジよりブリッジプライオリティを低く設定します。ブリッジの中で経路となるポートには、そのブリッジの中で低いパスコストを設定します。

＜各ブリッジの設定状態＞
以下に、実際にブリッジに設定した各パラメタの値を示します。
ブリッジF の左ポートのパスコストが10 ＋ 10 ＝ 20、右ポートのパスコストが10 ＋ 30 ＝ 40 により、ブリッ ジFの左ポートがルートポートとなります。



こんな事に気をつけて

スパニングツリー機能を使用する場合は、以下の点に注意してください。

• 複数支線の構成時の留意点

以下のように2 台のブリッジ間に複数の支線が接続する構成の場合は、支線ごとに中継するブリッジを選択することはできません。

代表ポート（各支線に中継するポート）は、以下の順序で決めます。

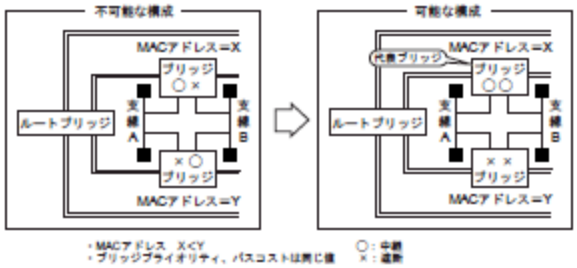
（1）ルートパスコストの低いブリッジ

（2）ブリッジ識別子（ブリッジプライオリティ＋MACアドレス）

ただし、複数のMACアドレスを持つ場合は装置の代表MACアドレスを使用します。

（3）ポート識別子（ポートプライオリティ＋ポート番号）

したがって、以下のように2 台のブリッジ間に複数の支線が接続する構成の場合は、2 台のブリッジに同じブリッジプライオリティ／パスコストを設定できます。しかし、同じMACアドレスは使用できないため、同じブリッジ識別子は設定できません。どちらかが代表ブリッジになり、すべての支線を中継します。



• 国際標準からのツリー構成

国際標準では、ツリー構成の段数は最大7 段をお勧めしています。これは、各性能に関するパラメタを推奨値（デフォルト値）で運用した場合にシステムがどのような条件で運用しても、スパニングツリー機能が正常に動作することを保証できる値です。

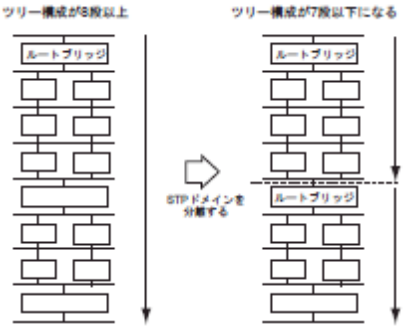
推奨値の最大7 段は、以下の式より算出できます。

```
最大寿命÷（Hello タイム＋構成メッセージの最大遅延時間）＋1
＝20÷（2＋1）＋1
≒7
```

ツリー構成の段数が7 段を超える場合は、以下の2つの対応方法があります。

- 構成するすべてブリッジの最大寿命を長くします。
- STPドメインを分離します。

前者は変更規模が大きくなり構成を変更する時間が長くなるため、後者での対応をお勧めします。



2.8.2 RSTP

STP の問題点として、最大で50 秒の通信断が発生してしまう場合があります。その問題点を克服するために開発されたプロトコルがRSTP（ラピッドスパニングツリープロトコル）です。RSTPを使用するとスパニングツリーの再計算は1秒程度となり、瞬断レベルでの切り替えが可能になります。また、RSTP は IEEE802.1w として標準化されており、従来のSTP（IEEE802.1d）とは互換性があります。そのためSTP との混在環境でも問題なく動作します。

RSTPでのポートの役割

STP では各ポートの役割が以下のようになっています。

- 指定ポート
- ルートポート
- ブロッキングポート

RSTP では指定ポートおよびルートポートは、STP の場合と同じ役割として使われます。ブロッキングポートは、以下の2 つの役割に分けて使われます。

- 代替ポート

代替パスを提供するポート。ルートポートの次にコストが小さいポートで、ルートブリッジへの代替パスのポートになります。

- バックアップポート

指定ポートが指定している経路の代替パスのポートです。1 つのスイッチで同一セグメントに対して2 つ以上の接続を持つ場合に、その代替パスとして提供されます。

代替ポートおよびバックアップポートは、通常ブロッキング状態となります。

RSTPでのポートの状態

STP では、ブロッキング状態、リスニング状態、ラーニング状態およびフォワーディング状態という4 つのポート状態があります。ブロッキング状態とリスニング状態ではどちらもMACフレームの中継は行いません。両者の違いは、ブロッキング状態ではBPDUの送信を行わないの対して、リスニング状態ではBPDUの送信を行うという点のみです。

RSTP では、ブロッキング状態とリスニング状態をまとめてディスカーディング状態としています。

2.8.3 MSTP

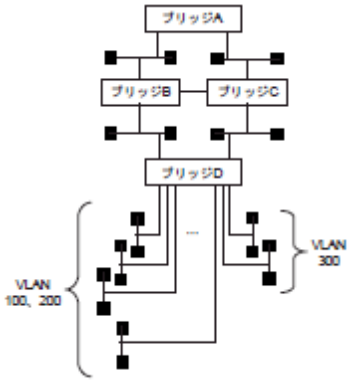
物理的にループしているネットワークでも、VLANの構成によっては、論理的にループしない場合があります。
STP ではループと判断して、一方のLANを通信に使わないで動作しますが、MSTP ではVLAN単位に扱うことができるため、STP よりも効率的にネットワーク内のデータを流すことができます。
以下のようなVLAN環境下でVLAN単位でフレームの制御を行う場合を考えます。

- ブリッジA～C

すべての接続ポートでVLAN100 および200、またはVLAN300 をタグVLANとしている。

- ブリッジD

ブリッジB、Cに接続しているポートは、VLAN100 および200、またはVLAN300 をタグVLANとしている。
端末側は、ポートごとにVLAN設定が異なる場合に、MSTP を使用してVLAN単位でロードバランシング（ブリッジA- ブリッジB間は1Gで、ブリッジA- ブリッジC間は100Mのような場合）を行う



インスタンス0

- ブリッジの優先順位　　：A→B→C→D

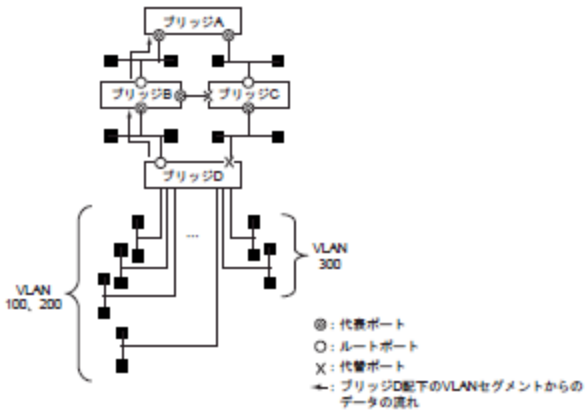
インスタンス1

- ブリッジの優先順位　　：A→B→C→D
- VLAN割り当て　　：100、200

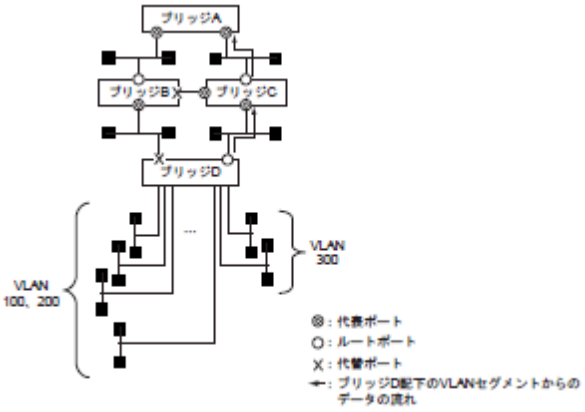
インスタンス2

- ブリッジの優先順位　　：A→C→B→D
- VLAN割り当て　　：300

インスタンス1でのスパンニングツリーとVLAN100、200のデータの流れ

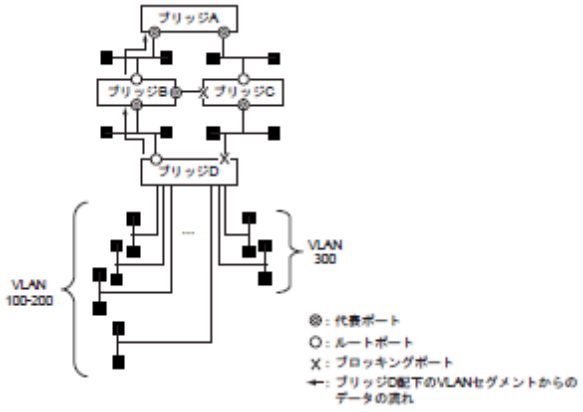


インスタンス2 でのスパンニングツリーとVLAN300のデータの流れ



MSTP を使用すると、「インスタンス1 でのスパンニングツリーとVLAN100、200 のデータの流れ」、「インスタンス2 でのスパンニングツリーとVLAN300 のデータの流れ」のようにVLAN単位でのロードバランシングか可能ですが、STP のみの場合は、以下のようにVLANに関係なくスパニングツリーが作成されるためデータが偏ります。

STPを使った場合のVLAN100および200、またはVLAN300を使用したフレームの流れ



2.9 LLDP 機能

LLDP（Link Layer Discovery Protocol）とは、自装置情報を広報することにより隣接装置の把握や接続状態の確認などを目的とした隣接探索プロトコルです。
LLDP情報は、同一物理LANに接続された装置にだけ届き、ルータを超えた先には届きません。
本装置のLLDP機能はIEEE802.1AB に準拠し、以下に示す機能を提供します。

- 自装置情報をLLDPで送信
- LLDPで受信した隣接装置情報を保持
- LLDPに関する情報をMIBとして管理し、SNMP機能でMIBを取得
- 隣接情報が更新されたことをSNMPトラップで通知
- LLDP設定情報、自装置情報、隣接装置情報、統計情報を表示

本装置から送信するLLDP情報には以下に示す情報を含めます。オプション情報は、送信しないように指示することができます。なお、1500バイト以上の情報は送信できないので、この場合には不要なオプション情報は送信しないようにしてください。特に、CEE機能使用時には、1500バイトを越えると、CEEの動作に必要な情報が送信されなくなるので注意してください。実際に送信される内容は、コマンドやWeb 画面で確認できます。

- 装置識別情報（代表MACアドレス） （必須）
- 物理ポート識別情報（ifIndex MIB） （必須）
- 保持時間情報（TTL） （必須）
- 物理ポート解説情報（ifDescr MIB） （オプション）
- 装置名称情報（sysName MIB） （オプション）
- 装置解説情報（sysDescr MIB） （オプション）
- 装置主要機能情報（スイッチ／ルータ） （オプション）
- 物理ポート管理アドレス情報（MAC/IPv4/IPv6）（オプション）
- ポートVLAN ID 情報（オプション）
- プロトコルVLAN ID 情報（オプション）
- VLAN名称情報（オプション）
- プロトコルVLAN種別情報（オプション）
- 物理ポート設定情報（オプション）
- 物理ポート電源供給情報 （オプション）
- リンクアグリゲーション情報（オプション）
- 最大フレームサイズ情報（オプション）

隣接装置から受信したLLDP情報は、LLDP情報に含まれている保持時間が経過するまで保持します。保持している隣接情報は、コマンドやWeb 画面で確認できます。

本装置で保持できる隣接情報の最大数を以下に示します。最大保持数を超えたために保持できなかった情報は破棄し、統計情報に破棄したことを計数します。

条件	保持数
装置全体での最大保持数	510
1ポートでの最低保障保持数	1
装置全体での共有保持数	476
1ポートでの最大保持数 (※)	477

※）1ポートで共用分をすべて保持した場合（ほかのポートでは1 台分しか保持できない）

2.10MAC フィルタ機能

MACフィルタ機能では、本装置を経由するパケットをMACアドレス、パケット形式、VLAN ID、COS値、IPアドレス、ポート番号などの組み合わせで制御することによって、ネットワークのセキュリティを向上させたり、ネットワークへの負荷を軽減することができます。

本装置を通過したパケットがACL 内の"acl mac" 定義、"acl vlan" 定義、"acl ip" 定義、"acl ip6" 定義、"acl tcp" 定義、"acl udp" 定義、および"acl icmp" 定義に該当した場合にMACフィルタ処理が動作します。

MACフィルタの条件

以下の条件を指定することによって、パケットデータの流れを制御できます。

• パケット入力ポート

フィルタ処理の対象となるパケット入力ETHERポート

• 動作

フィルタ処理の対象となるパケットが入力ETHERポートに入力された場合の動作（遮断または透過）

• ACL番号

MACフィルタの条件となるパケットパターンを定義したACL 番号

MACフィルタ機能の適用範囲

MACフィルタ機能では、ACL で指定したパケットパターンのフィルタを以下の単位で適用指定できます。

• ETHERポート

ether コマンドで設定します。ETHERポートに対して、指定したACL のパケットパターンに一致した入力パケットに対して、フィルタ処理を実施します。

• VLAN

vlan コマンドで設定します。VLANに属するETHERポートに対して、指定したACL のパケットパターンに一致した入力パケットに対して、フィルタ処理を実施します。同一VLAN内のすべてのETHERポートに適用する場合に使用します。

装置に設定可能な上限

装置に設定可能な上限を以下の表に示します。

1 ～ 4 の項目毎に設定可能上限数と優先度が設けられており、コマンドにより上限数を超えた設定がされた場合、優先度の低いコマンドの最後方の定義番号から無効になります。

優先度に関して、下表の 1 項を例に挙げると、"macfilter", "vlan macfilter", "lan ip filter" それぞれのコマンドで 50 個ずつ (定義番号は 0 ～ 49)、合計 150 個の定義を設定した場合、"macfilter" と "vlan macfilter" の定義は全て有効ですが、"lan ip filter" は 0 ～ 27 までの定義番号の定義が有効で、28 ～ 49 の定義番号の定義は無効となります。

項	コマンド	優先度	設定可能上限数
1	macfilter vlan macfilter lan ip filter	高 低	128
2	qos aclmap vlan qos aclmap	高 低	128
3	ip6filter vlan ip6filter lan ip6 filter	高 低	128
4	ip6qos aclmap vlan ip6qos aclmap	高 低	128

こんな事に気をつけて

プロトコルVLAN機能と併用した場合、プロトコルVLANとして認識されるフレームへのMACフィルタ機能は無効となります。

なお、プロトコルVLANとして認識されるフレームについては“vlan protocol”コマンド項目を参照してください。

2.11QoS 機能

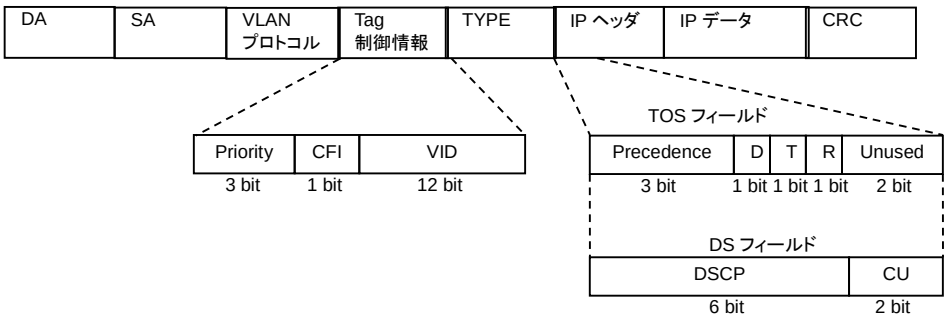
Qos機能とは、優先制御や優先制御の書き換えを行って、通信の品質を確保する機能です。本装置の優先制御機能には、ACLを使わない機能と、ACLを使った機能があります。
以下に、ACLを使わない基本的な優先制御機能から説明します。

2.11.1 優先制御機能

優先制御機能とは、パケットをキューイングし、対応付けされたキューの優先度に従って出力する機能です。優先制御機能は、入力パケットに対するユーザプライオリティの決定、ユーザプライオリティに対する本装置内部のキューへの対応付け、キューの優先制御の各機能から構成されています。

入力パケットに対するユーザプライオリティは、IEEE802.1pに準拠したCoS、およびタグなし受信パケットに対するデフォルトプライオリティで決定されます。また、qos classificationコマンドを用いると、IPv4のTOSフィールドの上位3bit（IP Precedence）やIPv6のTCの上位3bitを用いてユーザプライオリティを決定することが可能になります。qos classificationを有効化した場合、TOSもしくはTCの上位3bitによるユーザプライオリティ付けがCoSやタグなし受信パケットに対するデフォルトプライオリティによるユーザプライオリティ付けよりも優先されるようになります。

たとえば下記のIPパケットを運ぶVLANタグ付きフレームは、qos classificationを有効化した場合はTOSフィールドのPrecedence（=DSCPの上位3ビット）でユーザプライオリティが決定し、qos classificationが無効化されている場合はCoS（Tag制御情報のPriority）でユーザプライオリティが決まります。



ユーザプライオリティ付けされたパケットは、そのプライオリティに対応付けられた出力ポート（自装置あてポート含む）の複数のキューにキューイングされます。キューの数は4個で、ユーザプライオリティ値と本装置内部のキューの対応付けは変更可能です。キューはそれぞれ0～3の優先度を持っており、数字が大きくなるにしたがって優先度が上がります。

キューイングされたパケットはキューの優先制御方式に従って出力されます。優先制御方式はStrict Priority Queuing（Strict）、もしくはWeihted Round Robin(WRR) または Weighted Deficit Round Robin（WDRR）から選択します。

ユーザプライオリティ値と優先度の関係

本装置の初期設定および優先制御を行う場合のユーザプライオリティ値と装置内部のキューの推奨設定を、以下に示します。

ユーザプライオリティ値 （Traffic type）	本装置内部の キューの初期設定	優先制御を行う場合のキュー設定 （推奨）
0(Best Effort)	1	1
1(Background)	0	0
2(予備)	0	0
3(Excellent Effort)	1	1
4(Controlled Load)	2	2
5(Video)	2	2
6(Voice)	3	3
7(Network Control)	3	3

ユーザプライオリティを割り当てる設定

順位	入力パケットのプライオリティの 決定方法	有効とする設定
1	TOS	qos classification ip tos on
1	TC	qos classification ip6 tc on
2	CoS	VLAN Tag制御情報上位3ビット(プライオリティ)による。
2	Tagなし受信パケット	qos priority <queue_priority>

優先制御の処理方法

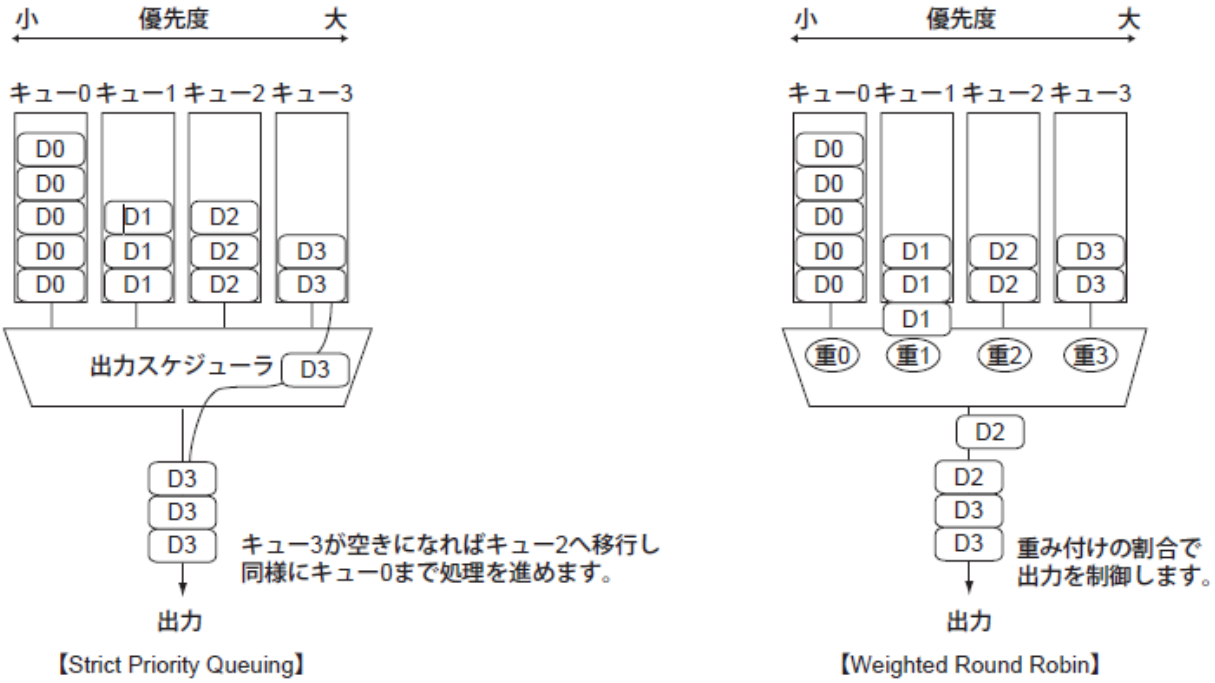
優先制御の処理には、Strict、WRR、WDRRのいずれかを設定します。

・Strict　：優先度の高いキューのフレームを最優先に処理します。

・WRR　：キューごとに一定の数値（出力比）を設定し、相対的な優先制御を行います。たとえば、キュー3 に10 を、キュー0 に1 を設定した場合、キュー3 とキュー0 は10：1 の割合で処理が行われます。

・WDRR　：キューごとに一定の数値（出力比）を設定し、相対的な優先制御を行います。WRRはパケット数を制御するのに対し、WDRRはデータ量を制御します。

以下に、Strict WRRの処理例を示します。



2.11.2 ACL を用いた優先制御機能

本装置は、ACLを用いて優先制御を行うこともできます。ACLを用いると、本装置を経由するパケットのMACアドレス、パケット形式、VLAN ID、COS値、IP アドレス、ポート番号などの組み合わせに基づいて出力ポートキューの割り当てを決定したり、DSCPのような優先制御情報を書き換えることができます。

ACLを用いて優先制御する場合は、優先制御の対象とするパケットを指定するACLの定義を行います。本装置は"acl mac" 定義、"acl vlan" 定義、"acl ip" 定義、"acl ip6" 定義、"acl tcp" 定義、"acl udp" 定義、および "acl icmp" 定義を設定し優先制御することができます。そして入力ポートに対して、定義したACLのACL番号と、そのACLに適合するパケットに対するアクションを指定します。アクションとしては出力キューの指定とDSCP(differentiated services codepoint)フィールドの書き換えがあります。
DSCPを用いてパケットの優先度制御を行いたい場合には、ACL定義でDSCPを指定し、そのDSCPに対する出力キューと優先制御のアルゴリズムを指定します。優先制御のアルゴリズムとしてはWRR、WDRRとStrictを選択可能です。DSCPに対してある最低限確保したい帯域幅を割り当てたい場合はWRRまたはWDRR、優先度の高いキューのフレームを最優先に割り当てたい場合はStrictを選択できます。
DSCPフィールドの書き換えを行う機能については、DSCP値書き換え機能の章をご覧ください。本装置のDSCP書き換え機能は、RFC2474：Definition of the Differentiated Services Field（DS Field）in the IPv4 and IPv6 Headersに準拠しています。

装置に設定可能な上限

装置に設定可能な上限を以下の表に示します。
1 ～ 4 の項目毎に設定可能上限数と優先度が設けられており、コマンドにより上限数を超えた設定がされた場合、優先度の低いコマンドの最後方の定義番号から無効になります。
優先度に関して、下表の 1 項を例に挙げると、"macfilter", "vlan macfilter", "lan ip filter" それぞれのコマンドで 50 個ずつ (定義番号は 0 ～ 49)、合計 150 個の定義を設定した場合、"macfilter" と "vlan macfilter" の定義は全て有効ですが、"lan ip filter" は 0 ～ 27 までの定義番号の定義が有効で、28 ～ 49 の定義番号の定義は無効となります。

項	コマンド	優先度	設定可能上限数
1	macfilter vlan macfilter lan ip filter	高 低	128
2	qos aclmap vlan qos aclmap	高 低	128
3	ip6filter vlan ip6filter lan ip6 filter	高 低	128
4	ip6qos aclmap vlan ip6qos aclmap	高 低	128

こんな事に気をつけて

プロトコルVLAN機能と併用した場合、プロトコルVLANとして認識されるフレームへのQoS機能は無効となります。なお、プロトコルVLANとして認識されるフレームについては“vlan protocol”コマンド項目を参照してください。MACフィルタ機能と併用する場合、MACフィルタ機能に該当したパケットに対するQoS機能は無効となります。

2.12IGMP スヌープ機能

IGMPスヌープ機能とは、送信元が送出したIGMPパケットを確認して、受信者の存在するポートへマルチキャストパケットを転送する機能です。

• 送信元

本装置に接続している端末またはマルチキャストルータ

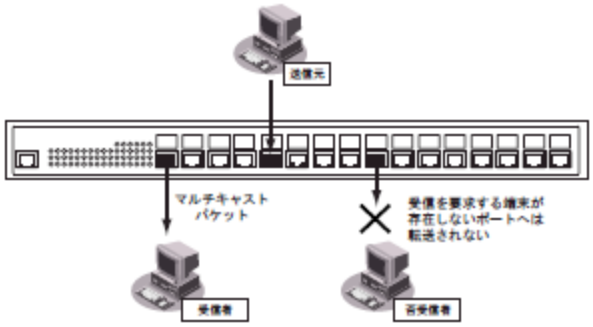
• 受信者が存在するポート

マルチキャストグループアドレスのリスナが存在しているポートまたはマルチキャストルータが接続されたポート

本機能を利用することによって、期待しないマルチキャストパケットを端末が受信しなくなり、端末の負荷を低減することができます。

本装置のIGMPスヌープ機能では、IGMPプロトコルのバージョン1、2、3 をサポートしています。

以下に、IGMPスヌープ機能の動作について示します。



本装置のポートで、マルチキャストルータが接続されたマルチキャストルータポートまたはリスナが存在するポートとして認識される条件を、以下に示します。

ポート	認識される条件
マルチキャスト ルータポート	マルチキャストルータポート設定（vlan <vlan_id> igmpsnoop router）によって、以下の条件で認識されます。 ・autoを指定した場合 IGMP Queryパケットを受信した場合、そのポートがマルチキャストルータポートと認識されます。 ・yes<port_no>を指定した場合 設定により指定されたポートは起動時にマルチキャストルータポートとして認識されます。さらに、autoを指定した場合と同様に、IGMP Query packetを受信したポートもマルチキャストルータポートとして認識されます。
リスナポート	IGMP Membership Reportパケットを受信したポートがリスナポートとして認識されます。

マルチキャストグループアドレスをあて先に持つパケットを受信した場合、本装置はマルチキャストルータポートおよびリスナポートにのみ、そのパケットを転送します。

こんな事に気をつけて

• IGMPを利用しないでマルチキャスト通信を行っている場合は、通信ができなくなる可能性があります。

• IGMPスヌープが有効である装置と接続するポートは、構成定義でマルチキャストルータポートとして設定してください。

• マルチキャストルータが2 台以上接続される場合は、マルチキャストルータポートを構成定義で設定してください。マルチキャストルータポートが正しく認識されなくなり、マルチキャストルータの先に接続される端末がマルチキャストパケットを受信できなくなる場合があります。

• 本装置では、一度登録されたグループアドレスはリスナ端末が存在しなくなった場合でもエントリ自体を消去しないで、出力ポートの情報のみを消去します。不要なグループアドレスが登録されている場合はclear igmpsnoop groupコマンドで消去することができます。

• 最大登録可能なマルチキャストグループアドレス数を超えた場合、超えたアドレスはすべて同一VLAN内にフラッディングされます。扱われるグループアドレスが最大登録可能数を超える場合は、IGMPスヌープ機能は利用しないでください。

• IPv4マルチキャスト以外の通信（例：IPv6 通信）を利用するネットワークでは利用できません。IGMPスヌープ機能は有効にしないでください。

• 本装置では224.1.1.1 と225.1.1.1 や224.1.1.1 と225.129.1.1 のようにIP アドレスの下位23 ビットが同じアドレスについては、同一アドレスとして認識されます。そのため、これらのアドレスで待ち合わせする異なるリスナ端末が存在した場合でも両方のアドレスあてのパケットが転送されます。

• IGMPスヌープの送信元アドレスは通常設定する必要はありません。送信元アドレスが0.0.0.0 であるIGMPパケットを認識できない装置が存在する場合のみ設定してください。なお、IGMPスヌープ装置を複数台接続する場合、IGMPスヌープの送信元アドレスは同一VLAN内で2 台以上設定しないでください。

• マルチキャストルータが接続されないネットワークでは、vlan igmpsnoop querier コマンドでQuerier 動作を無効としないでください。

・IEEE802.1Qトンネルポートの所属するVLAN IDのIGMPスヌープ機能は無効となります。

2.13MLD スヌープ機能

MLDスヌープ機能とは、送信元が送出したMLDパケットを確認して、受信者の存在するポートへIPv6マルチキャストパケットを転送する機能です。

• 送信元

本装置に接続している端末またはマルチキャストルータ

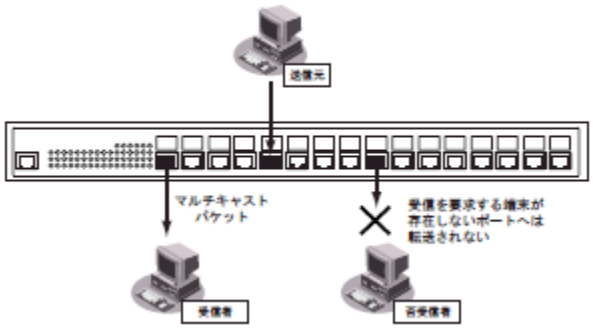
• 受信者が存在するポート

マルチキャストグループアドレスのリスナが存在しているポートまたはマルチキャストルータが接続されたポート

本機能を利用することによって、期待しないIPv6マルチキャストパケットを端末が受信しなくなり、端末の負荷を低減することができます。

本装置のMLDスヌープ機能では、MLDプロトコルのバージョン1をサポートしています。

以下に、MLDスヌープ機能の動作について示します。



本装置のポートで、マルチキャストルータが接続されたマルチキャストルータポートまたはリスナが存在するポートとして認識される条件を、以下に示します。

ポート	認識される条件
マルチキャストルータポート	マルチキャストルータポート設定（vlan <vlan_id> mldsnoop router）によって、以下の条件で認識されます。 ・autoを指定した場合 MLD Queryパケットを受信した場合、そのポートがマルチキャストルータポートと認識されます。 ・yes<port_no>を指定した場合 設定により指定されたポートは起動時にマルチキャストルータポートとして認識されます。 さらに、autoを指定した場合と同様に、MLD Query packetを受信したポートもマルチキャストルータポートとして認識されます。
リスナポート	MLD Membership Reportパケットを受信したポートがリスナポートとして認識されます。

マルチキャストグループアドレスをあて先に持つパケットを受信した場合、本装置はマルチキャストルータポートおよびリスナポートにのみ、そのパケットを転送します。

こんな事に気をつけて

•MLDを利用しないでIPv6マルチキャスト通信を行っている場合は、通信ができなくなる可能性があります。

• MLDスヌープが有効である装置と接続するポートは、構成定義でマルチキャストルータポートとして設定してください。

• マルチキャストルータが2 台以上接続される場合は、マルチキャストルータポートを構成定義で設定してください。マルチキャストルータポートが正しく認識されなくなり、マルチキャストルータの先に接続される端末がマルチキャストパケットを受信できなくなる場合があります。

• 本装置では、一度登録されたグループアドレスはリスナ端末が存在しなくなった場合でもエントリ自体を消去しないで、出力ポートの情報のみを消去します。不要なグループアドレスが登録されている場合は、clear mldsnoop groupコマンドで消去することができます。

• 最大登録可能なマルチキャストグループアドレス数を超えた場合、超えたアドレスはすべて同一VLAN内にフラッディングされます。扱われるグループアドレスが最大登録可能数を超える場合は、MLDスヌープ機能は利用しないでください。

• IPv4マルチキャストの通信を利用するネットワークではIGMPスヌープも有効にしてください。

• IPv6マルチキャスト以外の通信を利用するネットワークでは利用できません。MLDスヌープ機能は有効にしないでください。

• 本装置ではIPv6アドレスの下位32ビットの値が同じアドレスについては、同じアドレスとして認識されます。そのため、これらのアドレスで待ち合わせする異なるリスナ端末が存在した場合でも両方のアドレスあてのパケットが転送されます。

• MLDスヌープの送信元アドレスは通常設定する必要はありません。送信元アドレスが :: であるMLDパケットを認識できない装置が存在する場合のみ設定してください。なお、MLDスヌープ装置を複数台接続する場合、MLDスヌープの送信元アドレスは同一VLAN内で2 台以上設定しないでください。

• マルチキャストルータが接続されないネットワークでは、vlan mldsnoop querier コマンドでQuerier 動作を無効としないでください。

•IEEE802.1Qトンネルポートの所属するVLAN IDのMLDスヌープ機能は無効となります。

2.14EHM 機能

End-Host-Mode (EHM)では、アップリンクポート間でフレームの転送を行わないことで STP 等のプロトコルを用いることなくフレームのループが発生しないことを保証します。

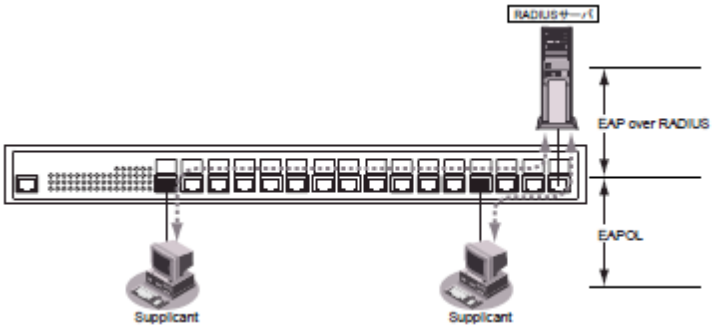
通常のスイッチモードと End-Host-Mode とは、boot-system mode コマンドで指定した後に再起動することで切り替えることができます。End-Host-Mode と通常のスイッチモードはそれぞれ独立した構成定義を持っています。

こんな事に気をつけて

- STP(スパニングツリー)機能を使用できません。
- コネクションブレードと ToR (Top-of-Rack)スイッチとの間で複数の接続を行う場合は、パケットの重複を防ぐためコネクションブレードと ToR スイッチの双方でリンクアグリゲーションを設定することをお勧めします。

2.15IEEE802.1X 認証機能

IEEE802.1X 認証機能とは、外部に設置したRADIUSサーバによって認証を行います。
本装置では、IEEE802.1X に準拠した認証機能（802.1X認証）をサポートしています。
認証機能は、認証方式「EAP-MD5」、「EAP-TLS」、「EAP-TTLS」、「PEAP」に対応しています。認証を行うための認証データベースとして、自装置内のAAA機能を用いたローカル認証と、外部にRADIUSサーバを設置したリモート認証が利用できます。ローカル認証を利用する場合は「EAP-MD5」のみで認証を行います。リモート認証を利用する場合は、ローカル認証に比べてより安全な「EAP-TLS」および「EAP-TTLS」などで認証を行います。
本機能を利用することで、認証許可のないSupplicant の通信（認証要求を除く）をすべて遮断し、認証されたSupplicant 以外からのネットワークへの不当アクセスを防止します。
RADIUSサーバに属性を設定することによって、認証時、Supplicant をVLANに対応付けます。RADIUSサーバからVLAN ID が通知されなかった場合、"ether dot1x vid" コマンドで設定されたVID を割り当てます。
本装置で動作確認が取れているRADIUSサーバは、富士通製「Safeauthor V3.5」です。
本装置では、1 つの物理ポートで複数の端末を認証できます。この場合、本装置の物理ポートにスイッチングHUBなどを接続し、そこに複数の端末を接続して、それぞれの端末で認証を行う運用が可能です。
1 つの物理ポートで複数の端末を認証する場合、“EAPOL 開始”メッセージを送信するサプリカントソフトを使用してください。“EAPOL開始”メッセージを送信しないサプリカントソフトでは認証が開始されません。本装置で動作確認が取れているサプリカントソフトは、富士通製「Systemwalker Desktop Inspection 802.1X サプリカント」 です。



こんな事に気をつけて

- 本機能を利用するポートでは、事前にVLANを設定できません。認証成功端末が認証成功時に割り当てられたVLANで通信します。

以下に、各EAPの認証方式と特徴を示します。

認証方式	特徴
EAP-MD5	・ ID、パスワードベースの認証規格である。 ・ ユーザ自身がパスワードを変更できるなど、管理者の負荷を軽減できる。
EAP-TLS	・ 証明書内の情報（サブジェクト）による認証ができる。 ・ クライアント（ユーザ端末）とサーバの双方に登録されたデジタル証明書による双方向承認ができる。 ・ 期限切れのユーザ側証明書のチェックおよび拒否ができる。 ・ 証明書執行情報（CRL）を反映し、失効した証明書のアクセス拒否できる。
EAP-TTLS	・ ID,パスワードベースの認証規格である。 ・ ユーザ端末側で証明書が不要である。 ・ 導入時のコスト負担が少なく、高いセキュリティレベルを維持できる。
PEAP	・ ID,パスワードベースの認証規格である。 ・ ユーザ端末側で証明書が不要である。 ・ 導入時のコスト負担が少なく、高いセキュリティレベルを維持できる。 ・ ユーザ自身がパスワードを変更できるなど、管理者の負荷を軽減できる。

VLAN ID 通知のための属性

リモート認証時にSupplicantへ割り当てるVLAN IDをRADIUSサーバへ設定する際の属性情報を以下に示します。

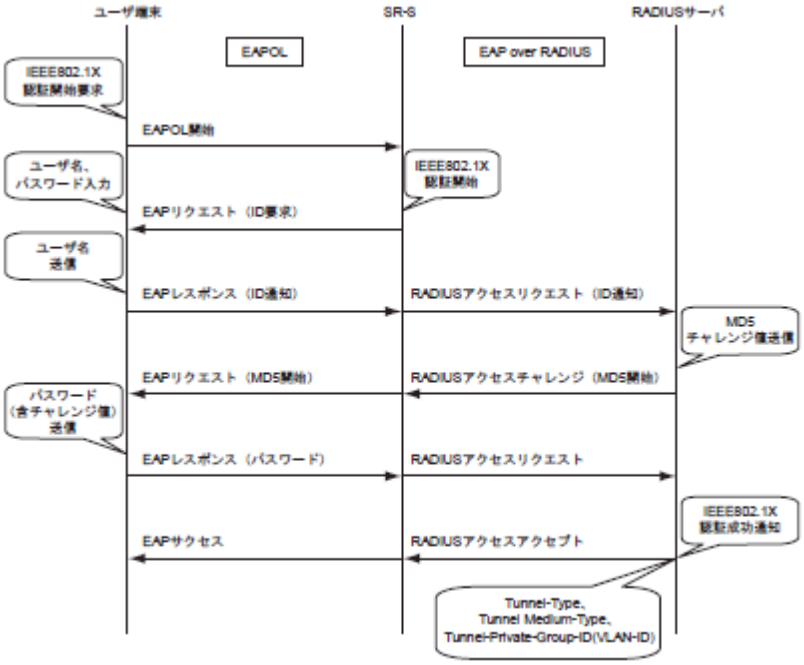
名前	番号	属性値（※）
Tunnel-Type	64	VLAN（13）
Tunnel-Media-Type	65	802（6）
Tunnel-Private-Group-ID	81	VLAN ID（10 進数表記をASCII コードでコーディング

※）（）内の数字は属性として設定される 10 進数の値

EAP-MD5認証

EAP-MD5 認証とは、ユーザ端末とRADIUS サーバ間で共通のパスワードを持つことによって、認証する方式です。チャレンジ・レスポンスをやり取りし、MD5 ハッシュ関数によって暗号化して、RADIUSサーバがユーザの認証を行います。ローカル認証時は「RADIUSサーバ」の代わりに本装置内の「AAA機能」が利用されます。

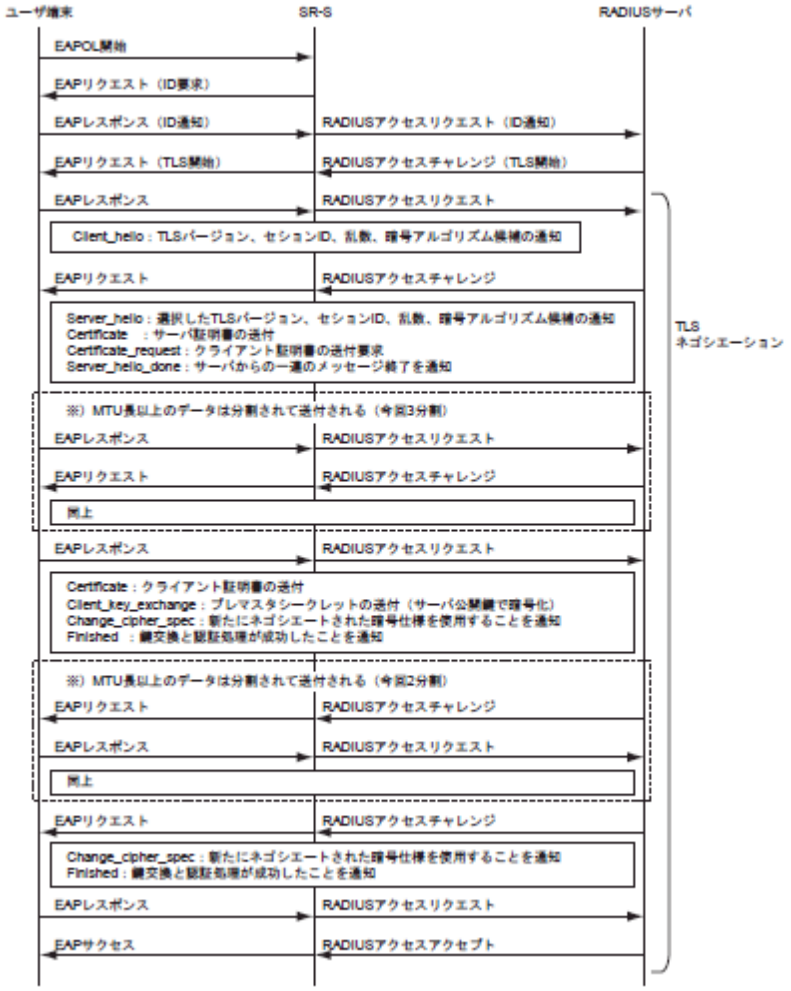
IEEE802.1X 機能のEAP-MD5認証のシーケンスを以下に示します。



EAP-TLS 認証

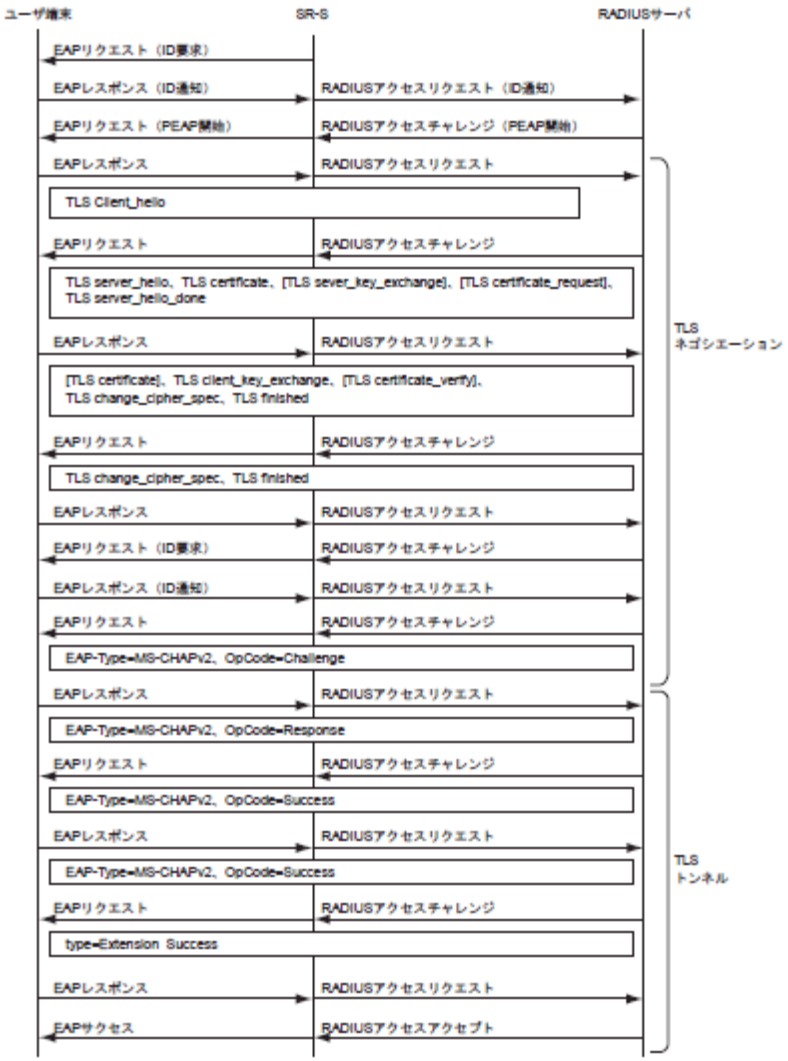
EAP-TLS認証とは、ユーザ端末とRADIUSサーバの双方に証明書を持つことによって、認証する方式です。

IEEE802.1X 機能のEAP-TLS認証のシーケンスを以下に示します。



PEAP認証（EAP-TTLS認証も同様）

PEAP認証とは、RADIUSサーバのみに証明書を持つことによって、認証する方式です。IEEE802.1X機能のPEAP認証のシーケンスを以下に示します。



2.16ゲスト VLAN 機能

ゲストVLAN機能とは、認証許可のない端末を検知したときに、特別なVLAN（ゲストVLAN）への接続を許可する機能です。
本機能を利用して、認証許可のない端末を接続拒否することなく別のVLANへと収容することで、認証許可のない端末のネットワーク利用を制限するといった運用ができるようになります。

こんな事に気をつけて

- ゲストVLAN機能とdot1x 認証を併用する場合は、EAP認証の途中で認証が成功となることがあるため、それに対応できないサプリカントは正常に動作しないおそれがあります。

2.17ブロードキャスト／マルチキャストストーム制御機能

ブロードキャスト／マルチキャストストーム制御機能とは、障害によってブロードキャスト／マルチキャストのパケットがネットワークを大量に流れ、それ以外のパケットの通信を阻害しないように、パケットを制御する機能です。

本装置は、しきい値を設定し、パケットをポート単位で制御します。パケットの流量がしきい値を超えた場合は、パケットを破棄またはポートを閉塞し、流量を制限します。

こんな事に気をつけて

パケットの流量がしきい値を超えポート閉塞した場合、ポート閉塞を解除するには、online コマンドによる閉塞解 除の指定が必要となります。

1518byte を超えるタグなしフレーム、または 1522byte を超えるタグ付きフレームに対して、ブロードキャスト/マルチキャストストーム制御が行われません。

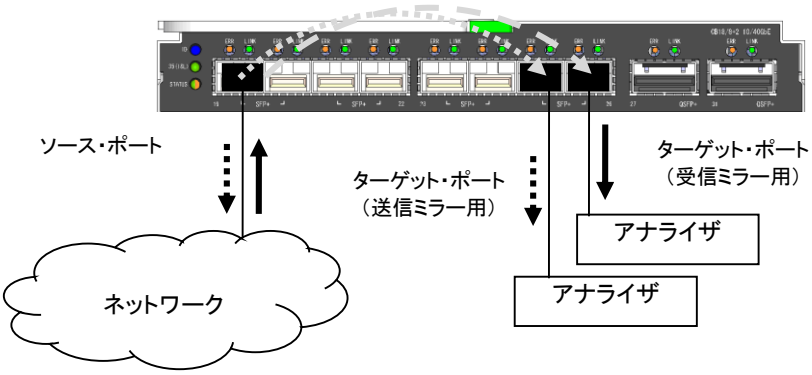
2.18ポート・ミラーリング機能

ポート・ミラーリング機能とは、指定したターゲット・ポートから、指定したソース・ポートの受信／送信／送受信トラフィックを監視する機能です。

ポート・ミラーリング機能を使用する場合は、まず、ターゲット・ポートに、LANアナライザなどトラフィックの状況を監視するプローブ装置を接続し、接続したターゲット・ポートと監視するソース・ポートを指定します。

本装置では複数のソース・ポートを指定することができます。ただし、複数ポートを指定する際には、対象となるソース・ポートのトラフィックの合計が、ターゲットポートの帯域を超えないようにしてください。

なお、、ソース・ポートのフロー制御を有効に設定していた場合、ソース・ポートの通信帯域がターゲット・ポートの通信帯域を超えると、ソース・ポートのフロー制御が動作し、実通信側にも影響を及ぼしますので、注意してください。



こんな事に気をつけて

ミラーのターゲットポートは装置で1ポートしか設定できません。

ミラーのターゲットポートは運用ポートとしても使用可能です。

ミラーのターゲットで指定したポートをソースとして指定することはできません。

ミラーのソースポートがターゲットポートに対して複数ある場合、ターゲットポートの帯域を超えた分のパケットは廃棄されます。

ソースポートのSTP機能でのポート状態がフォワーディング以外の場合も、ターゲットポートにパケットがミラーリングされます。STP、RSTP、MSTP状態とミラーされるフレームの関係は下記のようになります。複数のソース　　のミラーが可能な場合は、それぞれの状態に応じたトラフィックがミラーされます

ソースポート(MSTP の場合対象 VLAN 内)の状態	フレーム種類	ターゲットポート転送
ディセーブル	BPDU 以外	転送されない
	BPDU	転送されない
ブロッキング、リスニング (RSTP/MSTP ではディスカーディング)	BPDU 以外	転送されない
	BPDU	転送される
ラーニング	BPDU 以外	転送されない
	BPDU	転送される
フォワーディング	BPDU 以外	転送される
	BPDU	転送される

ターゲットポートに出力されるパケットのVLANタグの有無とその内容については、実際にソースポートで送受信されたパケットと異なる場合があります。
ターゲットポートに出力されるパケットは以下のようになります。

-送信パケットをミラーリングする場合以下の条件により異なります。

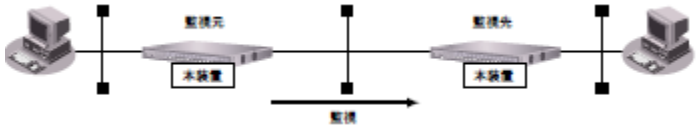
- 装置自発フレームの場合、ソースポートの VLAN 設定に基づいてタグが付けられ、ターゲットポートより出力されます。
- 装置自発フレーム以外の場合、必ずタグがつきます。
  タグ付き送信パケットの場合、そのパケットの VLAN タグが付けられてターゲットポートより出力されます。
  タグ無し送信パケットの場合、Protocol-Based VLAN, Port-Based VLAN 等により適切に VLAN タグが付けられてターゲットポートより出力されます。

-受信パケットをミラーリングする場合
ターゲットポートに出力されるパケットのVLANタグの有無は、入力時のパケットと一致します。

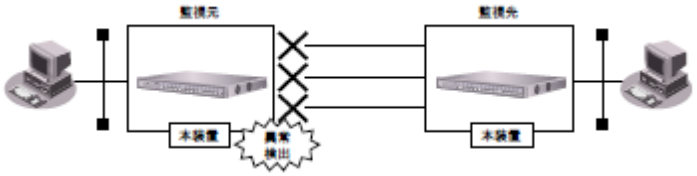
DSCPやip precedenceの書き換えを行いつつ受信フレームミラーリングを行う場合、変更後のフレームではなく変更前のフレームがミラーされます。

2.19ether L3 監視機能

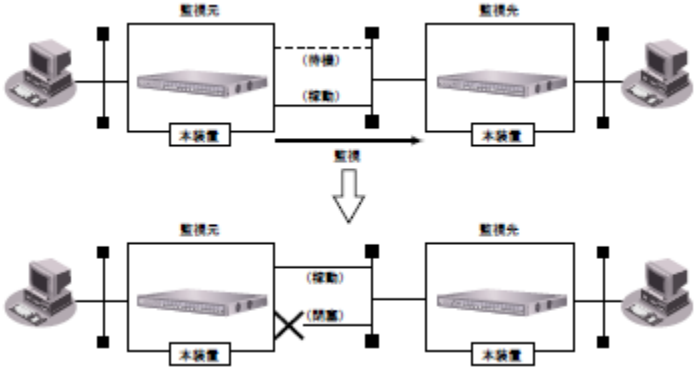
ether L3監視機能とは、ある特定のノード（装置）に対して、ICMP ECHOパケットを送受信することによりそのノードの生存を確認する機能です。監視相手装置が自装置と複数の装置を経由して繋がっている場合などでは、その経路上での障害を検出および監視しているポートを閉塞することができます。また、リンクアグリゲーション機能や、バックアップポート機能と併用することがきます。
定義反映時、監視ポートが リンクダウン状態だった場合でも、監視を開始します。



• リンクアグリゲーション機能を使用してether L3 監視
リンクアグリゲーション機能を使って監視をしている状態で、異常を検出してポートを閉塞させる場合、メンバポートすべてが閉塞されます。



• バックアップポート機能を使用してether L3 監視
バックアップポート機能を使って監視を行う場合、稼動ポートで監視を行うように設定してください。
待機ポートでether L3 監視機能を設定した場合は、監視を行いません。待機ポートが稼動ポートに切り替わったときに監視を開始します。また、異常を検出したとき、監視しているポートを閉塞させる場合、待機ポートが稼動ポートに切り替わることで、ネットワーク障害の影響を最小限に抑えることができます。
定義反映時、監視ポートが リンクダウン状態だった場合、マスタポートを必ず優先使用するモードになっていれば、マスタポートが監視を開始します。先にリンクアップしたポートを使用するモードになっていれば、監視を設定したポートが監視を開始します。

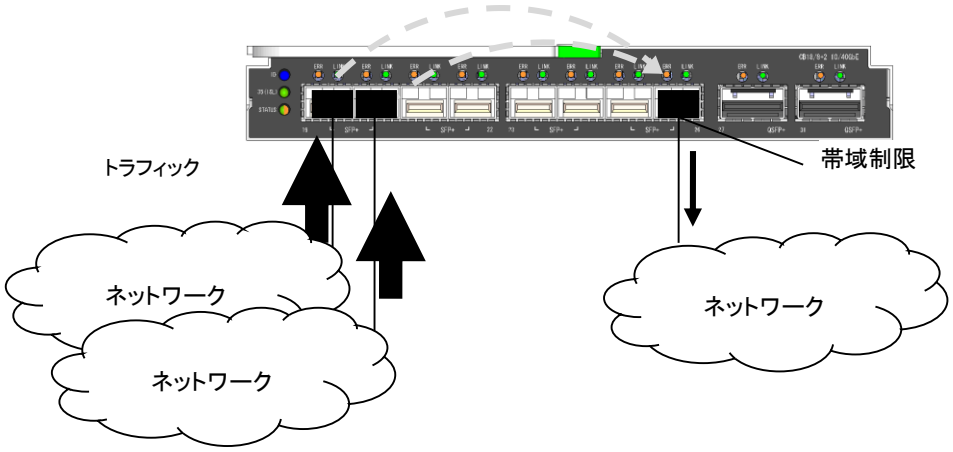


こんな事に気をつけて

• STP機能と併用する際には、監視タイムアウトを長めに設定してください。
• 閉塞状態になったポートは、online コマンドの閉塞解除指定でポート閉塞を解除してください。
• 監視対象ポートが認証ポートの場合、監視は行いません。

2.20出力レート制限機能

出力レート制御機能とは、大量のトラフィックが後続のネットワークに流れないよう、出力ポートの流量を制限する機能です。



本装置は、出力の制限値を設定し、帯域幅をポート単位で制御します。トラフィックの帯域幅がしきい値を超えた場合は、帯域幅を超えるトラフィックが破棄されます。

こんな事に気をつけて

WRR および WDRR を用いた優先制御機能と出力レート制御機能を併用することはできません。

2.21ポート閉塞機能

ポート閉塞機能とは、物理ポートのリンクダウン状態（ポート閉塞状態）をonlineコマンド発行によるオペレータ指示があるまで保持する機能です。

障害要因によって、物理ポートのリンクアップ、リンクダウンが繰り返し発生する可能性があります。そのような場合、本装置は意図的にリンクダウン状態（ポート閉塞状態）を継続させることで、冗長経路が存在する場合は、安定した通信を保つことができます。

ポート閉塞状態への遷移は、以下で制御します。

- offlineコマンド発行による手動閉塞
- 通信制御機能の連携動作による自動閉塞
- 接続ポートのリンク状態変化による自動閉塞

こんな事に気をつけて

- offline コマンドは、管理者クラスだけ発行可能です。
- 閉塞状態となったポートは、online コマンドの閉塞解除指定でポート閉塞を解除してください。
- 構成定義を変更した場合、変更内容によっては閉塞が解除される場合があります。

offline コマンド発行による手動閉塞

Ethernet ポート制御コマンドであるoffline コマンドを発行することによってポートを閉塞状態とします。

通信制御機能の連携動作による自動閉塞

ブロードキャスト／マルチキャストストーム制御機能などを使用した場合に、ポート閉塞状態への遷移指定が可能です。本装置でポート閉塞状態への遷移をサポートしている通信制御機能は以下のとおりです。

- バックアップポート機能
- ブロードキャスト／マルチキャストストーム制御機能
- ether L3監視機能

接続ポートのリンク状態変化による自動閉塞

接続ポートのリンク状態の変化を契機にポートを閉塞状態にすることを可能にします。

本装置でポート閉塞状態への遷移が可能なリンク状態変化は以下のとおりです。

- 起動時閉塞

装置起動時および動的定義反映時にポートを閉塞状態とします。

- リンクダウン回数による閉塞

構成定義で指定した回数分リンクダウンを検出した場合に、ポートを閉塞状態とします。

- リンクダウンを契機にしたほかのポートの連携閉塞（リンクダウンリレー閉塞）

リンクダウン時に、構成定義で指定した連携ポートを同時に閉塞状態とします。

また、リンクアップ状態へ復旧した場合に、連携ポートを同時に閉塞解除することも可能です。

2.22IP 経路制御機能

IP 経路情報は、ルーティングテーブルで管理され、IP パケットの転送先の判断に使用します。
IP 経路情報は、以下の機能で制御します。
• インタフェースの障害検出による経路制御機能
• スタティックルーティング機能

ここでは、IP 経路情報の種類、管理方法およびIP 経路情報を制御する機能について説明します。

2.22.1 IP経路情報の種類

IP 経路情報は、以下に示す情報で分類されます。
• インタフェース経路（IPv4）
インタフェースに割り当てたIPv4 ネットワークまたはIPv4 アドレスを示します。 ループバックインタフェースに割り当てたIPv4 アドレスは、ホストルート（32 ビットネットワークマスク）として管理されます。
• インタフェース経路（IPv6）
インタフェースに割り当てたIPv6 プレフィックスを示します。構成定義としてIPv6 プレフィックスを設定したときや、Router Advertisement Message でIPv6 プレフィックス情報を受信したときに生成されます。ループバックインタフェースに割り当てたIPv6 アドレスは、ホストルート（128 ビットネットワークマスク）として管理されます。
• RA経路（IPv6）
受信したRouter Advertisement（RA）Messageの情報に基づき、生成されるデフォルトルートを示します。
• スタティック経路（IPv4/IPv6）
構成定義として設定し、装置に保持される経路情報を示します。

IP 経路情報は、以下に示す優先度値で管理されます。

●ＩＰｖ4

ＩP経路情報	優先度値
インタフェース経路	0(固定)
スタティック経路	1(変更可)

●ＩＰｖ6

ＩP経路情報	優先度値
インタフェース経路	0(固定)
スタティック経路	1(変更可)
RA経路	12(固定)

2.22.2 IP経路情報の管理

IP 経路情報は、ルーティングプロトコルの経路テーブルとルーティングテーブルで管理されます。
以下に、2 つのテーブルについて説明します。

ルーティングテーブル

ルーティングテーブルは、IP 経路情報の中から選択した優先経路（ベストパス）で構成されます。また、ルーティングテーブルで管理するIP 経路情報の中で、インタフェース経路を除いたものをルーティングエントリ数として管理します。
ルーティングエントリは、装置ごとに最大エントリ数を規定し、最大エントリ数を超えた経路情報は破棄されます。
なお、IPv4 とIPv6 では、別々に管理されます。

こんな事に気をつけて

ルーティングテーブルで、ルーティングエントリの最大値を超えて受信したIP 経路情報は破棄され、登録されません。また、IP 経路情報によっては、最大エントリ数に満たない場合でも登録できないことがあります。経路登録に失敗した場合は、登録に失敗したことを示すシステムログが記録されます。ネットワーク構成および経路情報を見直したうえで、装置の再起動を行ってください。

2.22.3 インタフェースの障害検出による経路制御機能

インタフェースの障害検出（ハードウェアによる異常検出など）により、インタフェース経路情報をルーティングテーブルから削除することができます。このインタフェース経路の削除により、スタティックルーティング機能で作成されるIP 経路情報（同じあて先の経路情報）への切り替えを行うことができます。
また、インタフェースの障害検出は、スタティックルーティング機能で使用するインタフェースの異常として通知され、スタティックルーティング機能の中で経路切り替えを行うことができます。

2.22.4 スタティックルーティング機能

スタティック経路を使用し、以下の機能と組み合わせることにより、IP 経路情報を制御します。

- インタフェースの障害検出による経路制御機能

インタフェースの障害検出により、該当インタフェースを出口とするスタティック経路をルーティングテーブルから削除することができます。

- 優先経路制御機能

同じあて先の経路に対して、優先度（distance）によって、ルーティングテーブルに追加するIP 経路情報を選択することができます。優先度が小さいほど優先経路と扱われ、優先経路だけをルーティングテーブルに反映します。また、この優先経路が無効となった場合、次の優先経路に切り替えることができます。

2.23IPv6 機能

IPv6 とは、現在、主に利用されているIP（IPv4）を置き換えるための次世代インターネットプロトコルです。本装置では、IPv6 パケットでのホスト機能動作を行うことができます。
本装置がサポートしているIPv6 ホスト機能は、以下のとおりです。

- 静的な経路設定
- Router Advertisement Message 受信によるアドレスの自動設定
- Router Advertisement Message 受信によるデフォルト経路の自動設定
- Router Advertisement Message 受信によるND情報の自動設定
- ソースアドレスの自動選択

また本装置では、IPv4 パケットだけでなくIPv6 パケットも転送することができます。
本装置がサポートしているIPv6 ルータ機能は、以下のとおりです。

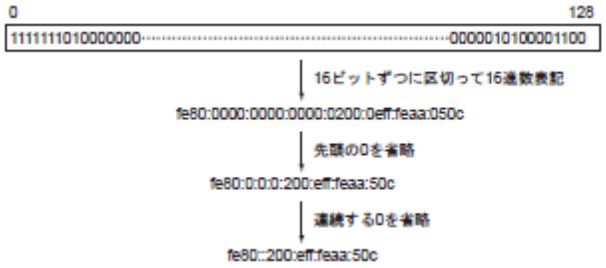
- 静的または動的な経路設定
- パケットフィルタリング

こんな事に気をつけて

- IPv6ホスト機能時は、ICMPv6リダイレクトメッセージは送信しません。
- IPv6ルーティング機能を使用する場合、プレフィックス長が65 ～ 127 の経路情報をルーティングテーブルに登録することはできません。

IPv6 アドレスの表記方法

128 ビットのIPv6 アドレスを表記する場合は、そのアドレスを「:」（コロン）で16 ビットずつに区切って、その内容を16 進数で記述します。個々の16 進数の値について先頭の0 は省略することができます。連続して0が続く場合は、1 つのIPv6 アドレスの表記で1 回限り「::」で省略することができます。



IPv6 アドレス体系

IPv6 アドレスは、IPv4 アドレスがネットワーク部とホスト部に分離することができるように、プレフィックスとインタフェースID に分離することができます。一般的には、プレフィックスのビット長（プレフィックス長）は64ビットで利用されます。
プレフィックス長を含めてアドレス表記をする場合は、プレフィックス長はアドレスの後ろに「/」で区切って付与します。

IPv6 で利用することができるアドレスは、IPv4 と同様に、先頭のビット数によって利用方法が決められています。本装置で利用できるアドレスは以下のようなものがあります。

• Global Unicast Addresses
通常利用するアドレスです。一般的には、契約したISP から割り当てられたアドレスや、IPv6 ルータから受信したRouter Advertisement Message 情報を元に自動生成されたアドレスとなります。

• Link-Local Unicast Addresses（fe80::/64）
link 内（ルータを介さないで通信できる範囲）だけで有効な特別なアドレスです。このアドレスは先頭の10ビットが1111 1110 10 で始まります。通常は11 ビット目から64 ビット目まではすべて0 となります。

• Multicast Addresses
マルチキャストアドレスです。先頭の8 ビットが1111 1111 となります。

静的または動的な経路設定

IPv6 のネットワークとルーティングの概念は、IPv4 の場合とほぼ同じです。装置が持つ経路情報に従って転送先を決定します。この経路情報を装置に持たせる方法として、静的な経路設定（スタティックルーティング）と動的な経路設定（ダイナミックルーティング）があります。
スタティックルーティングとは、経路情報を構成定義として設定し、利用します。この経路情報は構成定義を変更しない限り変更されることはありません。
ダイナミックルーティングとは、ルーティングプロトコルを利用する通信によって、ネットワーク上のほかのノードから経路情報を学習して利用します。本装置はダイナミックルーティングをサポートしません。

Router Advertisement Message 受信によるアドレスの自動設定

本装置では、Router Advertisement Message の受信機能をサポートしています。
Router Advertisement Message には、そのネットワークで利用するプレフィックス情報が含まれています。プレフィックス情報を受信した場合、有効期限を管理するためのプレフィックスリストを生成し、インタフェース IDを付加したIPv6 アドレスを自動設定します。
受信したプレフィックス情報は、show ipv6 ra prefix-list コマンドで参照できます。また、自動設定したIPv6 アドレスは、show ipv6 route またはshow interface コマンドで参照できます。

こんな事に気をつけて

•1つのインタフェースで複数のプレフィックス情報を受信する場合は、自動生成の設定を必要な数だけ追加してください。
•有効期限が365 日を超えたプレフィックス情報（無期限は除く）を受信した場合、365 日の有効期限として動作します。
•プレフィックス情報のプレフィックス長が64 以外の場合、そのプレフィックス情報は破棄されます。
•プレフィックス情報のオンリンクフラグと自動アドレス生成フラグが設定されている場合、IPv6 アドレスをインタフェースに設定します。

Router Advertisement Message 受信によるデフォルト経路の自動設定

Router Advertisement Message を受信した場合、送信ルータのリンクローカルアドレスを中継ゲートウェイとするデフォルト経路を設定します。
複数のルータよりRouter Advertisement Message を受信した場合、デフォルトルータとして利用できるデフォルトルータリストを生成し、この一覧の中でパケットが到達可能なルータをデフォルトルータとして設定します。
生成したデフォルトルータリストは、show ipv6 ra default-router-list コマンドで参照できます。また、show ipv6 route コマンドで、設定されたデフォルトルータを参照できます。

こんな事に気をつけて

•複数ルータからRouter Advertisement Message を受信した場合、ルータプレファレンスによる優先制御は動作しません。この場合、最初に受信したルータをデフォルトルータとします。
• Router Advertisement Message によるデフォルト経路の優先度値は12 で設定します。
スタティックのデフォルト経路と混在運用する場合、スタティック経路の優先度値を変更してください。

Router Advertisement Message 受信による ND 情報の自動設定

Router Advertisement Message には、通信時に使用する隣接情報（ND情報）が含まれています。Router Advertisement Messageを受信し、受信メッセージに含まれているND情報と本装置で保持しているND情報が異なる場合は、ND情報の更新が行われます。
以下に、本装置で保持しているND情報とその初期値を示します。

- 隣接装置の到達性についての有効期間（初期値は30 秒）
- 隣接装置の到達性確認を行うNeighbor Solicitation（NS）Messageの送信間隔（初期値は1 秒）
- 最大ホップ数（初期値は64）
- 受信ネットワーク上で推奨するMTU長（初期値は1500 バイト）

ソースアドレスの自動選択

IPv6 では、インタフェースに複数のIPv6 アドレスが割り当てられることが一般的です。本装置から通信を始め、アプリケーションによって明示的にソースアドレスを指定しない場合は、複数のIPv6 アドレスの中から一定のルールに基づいてアドレスの選択を行います。

本装置がサポートするソースアドレスの選択ルールは、以下のRFCおよびドラフトに準拠します。

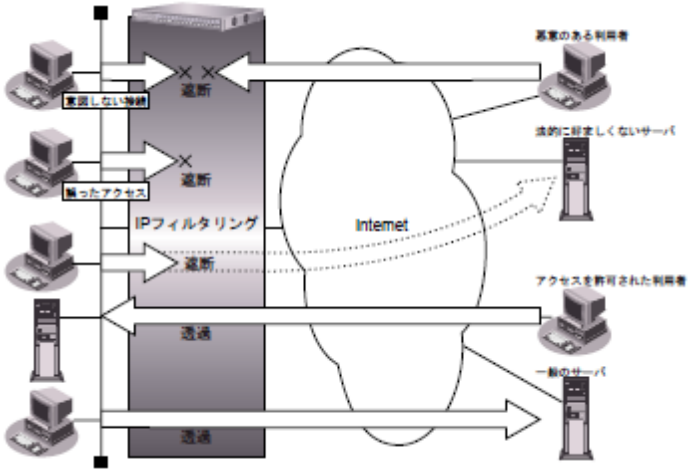
- RFC3484：Default Address Selection for Internet Protocol version 6 （IPv6）

2.24IP フィルタリング機能

本装置は、IP フィルタリング機能やパスワードの設定などを使って、ネットワークのセキュリティを向上させることができます。

IP フィルタリング機能とは、本装置を経由して送受信するパケットをIP アドレスやポート番号などで制御することによって、ネットワークのセキュリティを向上させることができます。

本装置では、本装置に入力されたパケットが指定されたACL 定義の“acl ip”定義および、“acl tcp”定義または“acl udp”または“acl icmp”定義に該当した場合にIP フィルタリング処理を行います。



ネットワークのセキュリティを向上させるには、以下の要素について考える必要があります。

•ネットワークのセキュリティ方針

•スイッチ以外の要素（ファイアウォール、ユーザ認証など）

こんな事に気をつけて

•本装置などのスイッチでは、コンピュータウィルスの感染を防ぐことはできません。パソコン側でウィルス対策ソフトを使用するなど、別の手段が必要です。

接続形態に応じてセキュリティ方針を決める

インターネットに接続する場合でもLANどうしを接続する場合でも、データの流れには「外部から内部へ」、「内部から外部へ」という2 つの方向があります。セキュリティ方針を決める場合は、2 つの方向について考慮する必要があります。

● **「外部から内部へ」流れるデータに対するセキュリティ方針の例**

特定のパケットを受け取らないようにする。

非公開ホストへのアクセスを拒否する。

内部ユーザによる不要なアクセスを防ぐ。

● **「内部から外部へ」流れるデータに対するセキュリティ方針の例**

法的に問題のあるサイトなどへのアクセスを制限する。

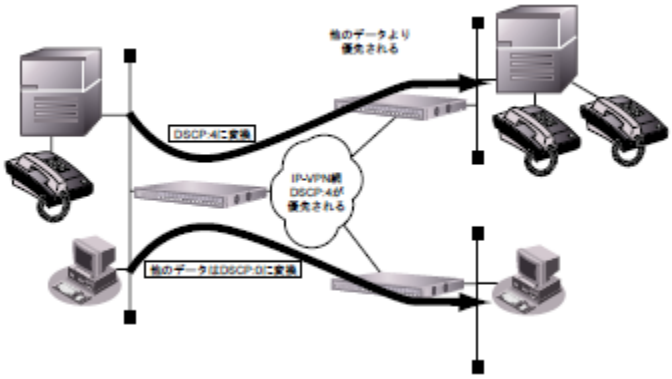
内部ユーザによる不要なアクセスを防ぐ。

補足　IPフィルタリングは「外部から内部へ」流れるデータに対してのみ機能します「内部から外部へ」流れるデータおよび内部にあるパソコン間データ（LAN　内のデータ）に対しては機能しません。

2.25DSCP 値書き換え機能

DSCP値書き換え機能とは、指定するIP パケットのDSCP値を書き換える機能です。IP-VPN 網を使って音声やレスポンスが要求されるデータのDSCP値を変更して送信することにより、IP-VPN 網内の遅延を減らすことができます。DSCP値でパケット優先制御を行うキャリアVPNサービス（スーパーVPNなど）と接続する場合に有効な機能です。
本装置でサポートしているDSCP値書き換え機能は、以下のRFC（Request For Comments）に準拠しています。

• RFC2474：Definition of the Differentiated Services Field（DS Field）in the IPv4 and IPv6 Headers



DSCP値書き換え機能は、IPv4［RFC791］ で定義されている IP パケットヘッダにある8 ビットのType Of Service（TOS）フィールドおよびIPv6 パケットヘッダにある8 ビットのTraffic Class フィールドのうち、DSCPフィールドを制御することができます。

• RFC791 Internet Protocol
• RFC2460 Internet Protocol,Version 6 （IPv6）Specification

Bits 0-5: DSCP
Bits 6-7: Currently unused

書き換え条件では、送信先IP アドレス、あて先ポート番号、送信元IP アドレス、送信元ポート番号、およびプロトコル番号を指定できます。この条件に一致するパケットのDSCP値を書き換えて送信します。複数の条件と一致する場合は、定義番号が小さい方の条件を使用します。
書き換えの対象とならなかったパケットのDSCP値は書き換えられません。
本装置では、本装置に入力されたパケットが、指定されたACL 定義の"acl ip" 定義（IPv6 の場合はacl ip6 定義：および、"acl tcp"、"acl udp" または"acl icmp" 定義に該当した場合にDSCP値書き換え処理を行います。

DSCPの書き換えを行う場合、出力キューの決定方法は2通りの方法が選択できます。1つはパケットに対するユーザプライオリティとキューの対応関係のみに基づいて決定する方法で、この場合DSCP書き替えは出力キューの決定に影響しません。ユーザプライオリティはqos classification機能を用いた場合のTOSもしくはTCの上位3bit（書き換え前のDSCPの上位3bit）によるユーザプライオリティ、IEEE802.1pに準拠した

CoS、タグなし受信パケットに対するデフォルトプライオリティの優先順位で決定されます。もう1つはchangeQueue機能を用いる場合で、この場合は書き換え後のDSCPに従って出力キューが決定されます。書き換え後のDSCPに対応する出力キューは、そのDSCPの上位3bitをユーザプライオリティとした場合に対応する出力キューとなります。出力キューに対する優先制御アルゴリズムと優先度を指定することで、書き替えたDSCPのトラフィックに対して設定したい優先制御を適用することができます。

こんな事に気をつけて

プロトコルVLAN機能と併用した場合、プロトコルVLANとして認識されるフレームへのQoS機能は無効となります。

なお、プロトコルVLANとして認識されるフレームについては“vlan protocol”コマンド項目を参照してください。

また、IP・MACフィルタが適用されたパケットに対しては、ACLを利用するQoSは無効となります。

2.26RADIUS 機能

RADIUS機能は、AAA（Authentication, Authoraization, Accounting）情報の管理を外部サーバ（RADIUSサーバ）を利用して行う機能です。複数の装置で同じAAA情報が必要な場合や、大量のユーザ情報を管理する場合など、ユーザの認証情報や設定情報、ユーザごとの接続時間を集約して管理することができます。
本装置では、RADIUSクライアント機能をサポートしています。
RADIUSクライアント機能は、以下のRADIUSサポート機能からAAAを経由して利用されます。

以下に、それぞれの機能で利用可能なAAA情報を示します。

RADIUS サポート機能	認証方式 （authentication）	ユーザ情報 （authoraization）	アカウンティング （accouning）
IEEE802.1X 認証	EAP-MD5 認証、EAP-TLS認証 EAP-TTLS認証、PEAP認証	使用しません	・送受信オクテット数 ・送受信パケット数 ・接続時間
ARP認証	PAP認証／CHAP認証（※）	使用しません	使用しません
DHCP MACアドレスチェック	PAP認証／CHAP認証（※）	使用しません	使用しません

※）ユーザ名はMACアドレス（区切り文字なしHEX12 文字）、
　　パスワードはMACアドレスを使った認証となります。

本装置のRADIUSクライアント機能は、複数台のRADIUSサーバを使用したバックアップ構成または負荷分散構成が可能です。

RADIUSサーバとして定義された認証サーバおよびアカウンティングサーバは、alive状態とdead状態を持ちます。
それぞれの状態の意味は以下のとおりです。
• alive 状態
サーバが使用可能である状態です。優先度が高い（定義上の数値が小さい）サーバから優先して使用されます。同じ優先度のサーバが複数存在する場合は、ランダムにサーバが選択されます。
• dead 状態
サーバあてのリクエストがタイムアウトしたことにより、そのサーバの使用を一時的に停止している状態です。ほかにalive 状態のサーバが存在する場合、定義した優先度の値は使用されません。
復旧待機時間で指定した時間が経過すると、自動的にalive 状態に復旧します。
認証またはアカウンティングを行う場合、すべてのサーバがdead 状態になると、ランダムに1つのサーバで試行し、応答の得られたサーバはalive 状態に復旧します。

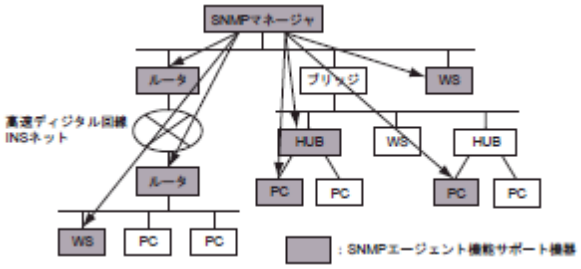
こんな事に気をつけて

• RADIUSプロトコルの制約で、同時に認証およびアカウンティングが行える数は256 です。同時に257 以上の認証とアカウンティングを行った場合は、両方とも失敗します。
• RADIUSクライアント機能を定義しても、同じグループのユーザ情報は利用されます。AAAグループにRADIUSクライアント機能（aaa radius）とユーザ情報（aaa user）の両方を定義した場合、RADIUSクライアント機能で認証が行われます。RADIUSクライアント機能で認証が成功した場合はユーザ情報は利用されませんが、認証に失敗した場合は、次にユーザ情報で認証を行います。

2.27SNMP 機能

SNMP（Simple Network Management Protocol）とは、IP 層およびTCP層レベルの情報を収集、管理するためのIP 管理用のプロトコルです。
SNMP機能では、管理する装置をSNMPマネージャ、管理される装置をSNMPエージェントと言います。
SNMP機能でネットワークを管理する場合、管理する側はSNMPマネージャ機能を、管理される側はSNMPエージェント機能をサポートしている必要があります。
SNMPマネージャ機能は、ネットワーク上の端末の稼動状態や障害状態を一元管理します。SNMPエージェント機能は、SNMPマネージャの要求に対してMIB（Management Information Base：管理情報ベース）という管理情報を返します。
SNMP機能は、この2 つの機能を使用して、SNMPマネージャとSNMPエージェントとの間でMIBに定義されたパラメタを送受信してネットワークを管理します。
本装置では、SNMPv1、SNMPv2cおよびSNMPv3をサポートします。また、標準MIBおよび富士通拡張MIBをサポートしています。

SNMP 機能による管理



ヒント

◆ MIBとは

MIBには、装置のベンダに関係ない標準MIB と装置ベンダ固有の拡張MIBがあります。RFC1213などで定義される標準MIBは、管理ノードのそれぞれの管理対象（オブジェクト）にアクセスするための仮想の情報領域です。RFCでは、SNMPエージェントが取り付けるべき管理情報を定義しています。管理情報には、SNMPノードとしてのシステム情報（システム名や管理者名など）やTCP/IP に関連する統計情報があります。しかし、RFCで定義されている項目では伝送路やHUBなどを十分に管理できません。そのため、各種プロトコルの情報や各社の装置ごとのベンダ固有に合わせてMIB を拡張します。これを拡張MIBと言います。MIBはASN.1（Abstract Syntax Notation 1）という形式で定義します。SNMPマネージャが拡張MIBを管理するためには、SNMPエージェント側でその拡張MIBを公開して、SNMPマネージャがその拡張MIBの情報を収集するように定義する必要があります。

2.27.1 RMON機能

RMON（Remote Network Monitoring）とは、ネットワーク監視のための標準規格であり、遠隔地にあるLANのトラフィックやエラーなどの通信状況を監視する機能です。RMON機能はSNMP機能を拡張したものであり、SNMPエージェント側でLANの統計情報を蓄積しておき、SNMPマネージャ（またはRMONマネージャ）からの要求に応じて蓄積したデータをSNMPの応答として返します。

本装置では以下のRMONグループをサポートします。

• statistics グループ

監視対象ETHERポート上のパケット数やエラー数などの基本的な統計情報を収集します。

• historyグループ

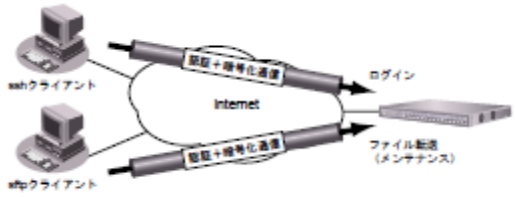
statistics グループで収集する情報とほぼ同じ統計情報を履歴情報として保持します。

履歴情報は一定期間の統計情報として装置内で保持されますので、SNMPマネージャ（またはRMONマネージャ）は一連の統計情報をまとめて取得することができます。

2.28SSH サーバ機能

SSHサーバ機能とは、TELNET サーバ機能と同じリモートログイン機能（ssh サーバ）とFTP サーバ機能と同じリモートファイル転送機能（sftp サーバ）をサポートしています。
TELNET サーバ機能およびFTPサーバ機能では、平文テキストデータのまま通信するため、通信内容を傍受されたり、改ざんされる危険性があります。SSHサーバ機能では、ホスト認証および暗号化通信により、安全で信頼できるログイン機能およびファイル転送機能を利用することができます。

参照 本装置のSSHサーバ機能は、BSDライセンスに基づいて公開されているフリーソフトウェアのOpenSSHを利用しています。詳しくは、以下のURLを参照してください。
英語版 ：http://www.openssh.com/
日本語版 ：http://www.openssh.com/ja/



※一時点ではどちらか一方の接続のみ

本装置の電源投入時およびリセット時に本装置のSSHホスト認証鍵が生成されます。生成時間は、数十秒から数分です。SSHホスト認証鍵生成開始時と完了時にシスログが出力され、生成完了した時点から本装置にSSH接続することができます。
SSHクライアントソフトウェアにあらかじめ接続相手のSSHホスト認証鍵を設定しておく必要がある場合は、本装置でshow ssh server key dsa コマンドまたはshow ssh server key rsa コマンドを実行して表示されるSSHホスト認証鍵を設定します。
本装置にSSH接続した際に、本装置のSSHホスト認証鍵がSSHクライアント側に送信されて、設定または保存されている鍵と異なる場合は、SSH接続が拒否されます。したがって、装置交換などにより、SSHホスト認証鍵が変更された場合は、SSHクライアントソフトウェアに設定または保存されているSSHホスト認証鍵を再設定するか削除してからSSH接続します。
そのあと、パスワード入力プロンプトが表示されますが、SSHホスト認証などの処理により、表示されるまで多少時間がかかります。
また、serverinfo ssh/serverinfo sftp コマンドをoff に設定することにより、SSHサーバ機能を完全に停止させることができます。
ssh クライアントとsftp クライアントはSSHポートに接続するため、serverinfo コマンドのssh またはsftp のどちらかがon の場合、本装置のSSHポートは接続できる状態のままであるため、off に設定した方はパスワード 入力まで行われたあとに接続拒否されます。

こんな事に気をつけて

SSHサーバ機能が完全に停止している状態で本装置を起動し、serverinfo コマンドでSSH機能のどちらかを有効にして設定を反映した場合、SSHホスト認証鍵の生成に時間がかかります。このとき、セッション監視タイムアウトが発生するなど、ほかの処理に影響する可能性があります。

以下に、sftp接続とftp接続の相違点を示します。

項目	Sftp接続	ftp接続
ユーザID指定	接続前に指定 （一部のsftpクライアントは接続開始時に指定する）	接続後に指定 （一部のftpクライアントは接続前に指定する）
バイナリモード指定	なし	あり
パッシブモード指定	なし	あり

本装置でサポートするSSHサーバ機能

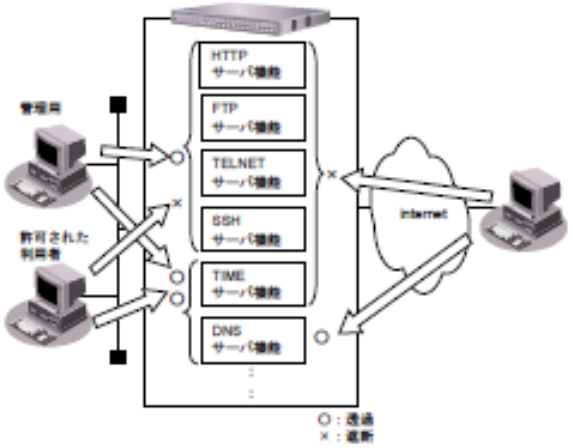
項目	サポート内容
SSHサーババージョン	OpenSSH 3.9p1
SSHプロトコルバージョン	SSHプロトコルバージョン2 だけをサポート
SSHポート番号/プロトコル	22 ／TCP
IPプロトコルバージョン	IPv4、IPv6
ホスト認証プロトコル	RSA
ホスト認証アルゴリズムの種類	ssh-rsa, ssh-dss
暗号方式の種類	aes128-cbc、3des-cbc、blowfish-cbc、cast128-cbc、arcfour、aes192-cbc、aes256- cbc、rijndael-cbc@lysator.liu.se、aes128-ctr、aes192-ctr、aes256-ctr
メッセージ認証コードの種類	hmac-md5、hmac-sha1、hmac-ripemd160、hmac-ripemd160@openssh.com、hmacsha1- 96、hmac-md5-96
同時接続数	5

2.28.1 SSHクライアントソフトウェア

本装置にSSH接続するには、SSHクライアントソフトウェアが別途必要です。
本装置のSSHサーバ機能では、SSHプロトコルバージョン2 だけをサポートしているため、SSHプロトコルバージョン2 に対応したSSHクライアントソフトウェア（ssh クライアントソフトウェアおよびsftp クライアントソフトウェア）を使用してください。

2.29アプリケーションフィルタ機能

アプリケーションフィルタ機能では、本装置で動作する各サーバ機能に対してアクセスを制限することができます。これにより、本装置のメンテナンスまたは本装置のサーバ機能を使用する端末を限定し、セキュリティを向上することができます。



2.30TACACS+機能

TACACS+機能は、AAA（Authentication, Authorization, Accounting）情報の管理を外部サーバ（TACACS+サーバ）を利用して行う機能です。複数の装置で同じAAA情報が必要な場合や、大量のユーザ情報を管理する場合など、認証（Authentication）、認可（Authorization）およびアカウンティング（Accounting）情報を集約して管理することができます。
本装置では、TACACS+クライアント機能のユーザ認証機能とコマンド認可機能をサポートしています。
ユーザ認証機能とは、アクセスユーザが本装置にログイン時に認証処理を行います。
コマンド認可機能とは、アクセスユーザが本装置の提供するコマンド実行時に認可処理を行います。

TACACS+クライアント機能は、複数台のTACACS+サーバを使用したバックアップ構成または負荷分散構成が可能です。

それぞれの状態の意味は以下のとおりです。
・alive状態
サーバが使用可能である状態です。
優先度が高い(定義上の数値が小さい)サーバから優先して使用されます。
同じ優先度のサーバが複数存在する場合は、ランダムにサーバが選択されます。
・dead状態
サーバとのTCP接続失敗やサーバあてのリクエストがタイムアウトしたことにより、そのサーバの使用を一時的に停止している状態です。ほかにalive状態のサーバが存在する場合、定義した優先度の値は使用されません。
復旧待機時間で指定した時間が経過すると、自動的にalive状態に復旧します。
認証または認可を行う場合、すべてのサーバがdead状態になると、ランダムに１つのサーバで試行し、応答の得られたサーバはalive状態に復旧します。

こんな事に気をつけて

・TACACS+クライアント機能のアカウンティング機能はサポートしていません。
・RADIUS クライアント機能との併用はできません。AAA グループに RADIUS クライアント機能(aaa radius)と TACACS+クライアント機能(aaa tacacsp)の両方を定義した場合、TACACS+クライアント機能は無効となります。AAA グループに TACACS+クライアント機能とユーザ情報(aaa user)の両方を定義した場合は、TACACS+クライアント機能で認証が行われます。TACACS+クライアント機能で認証が失敗しても、ユーザ情報での認証は行われません。
・TACACS+サーバ用共有鍵の定義を省略した場合、認証や認可データは暗号化されません。認証や認可データを暗号化する場合は、共有鍵を定義してください。
・TACACS+コマンド認可機能は、TACACS+ユーザ認証機能を使用してログインした場合のみ有効となります。
・TACACS+ユーザ認証時の権限クラスは、管理者パスワード(password admin set)設定の有無に依存します。
・TACACS+コマンド認可機能は、Web 設定および FTP/SFTP では動作しません。

・TACACS+コマンド認可機能で、実際に実行するコマンドとは別のコマンドに対する認可の設定が必要なものは、以下になります。

実行するコマンド	認可設定が必要なコマンド
diff	show running-config(running-config に対して diff を実行する場合)
show tech-support	show(show コマンド全体)
save	show(show コマンド全体)
load	構成定義コマンド全体

以下に管理者パスワードの有無による認証時の権限クラスを示します。
＜管理者パスワードなしの場合＞
一般ユーザクラスでの認証のみ行います。
＜管理者パスワードありの場合＞
管理者クラスでの認証を行い、認証が失敗した場合に一般ユーザクラスでの認証を行います。

2.31 LDAP 機能

LDAP機能は、AAA（Authentication, Authorization, Accounting）情報の管理を外部サーバ（LDAPサーバ）を利用して行う機能です。複数の装置で同じAAA情報が必要な場合や、大量のユーザ情報を管理する場合など、認証（Authentication）情報を集約して管理することができます。
本装置では、LDAPクライアント機能のユーザ認証機能をサポートしています。
ユーザ認証機能とは、アクセスユーザが本装置にログイン時に認証処理を行います。

LDAPクライアント機能は、複数台のLDAPサーバを使用したバックアップ構成または負荷分散構成が可能です。

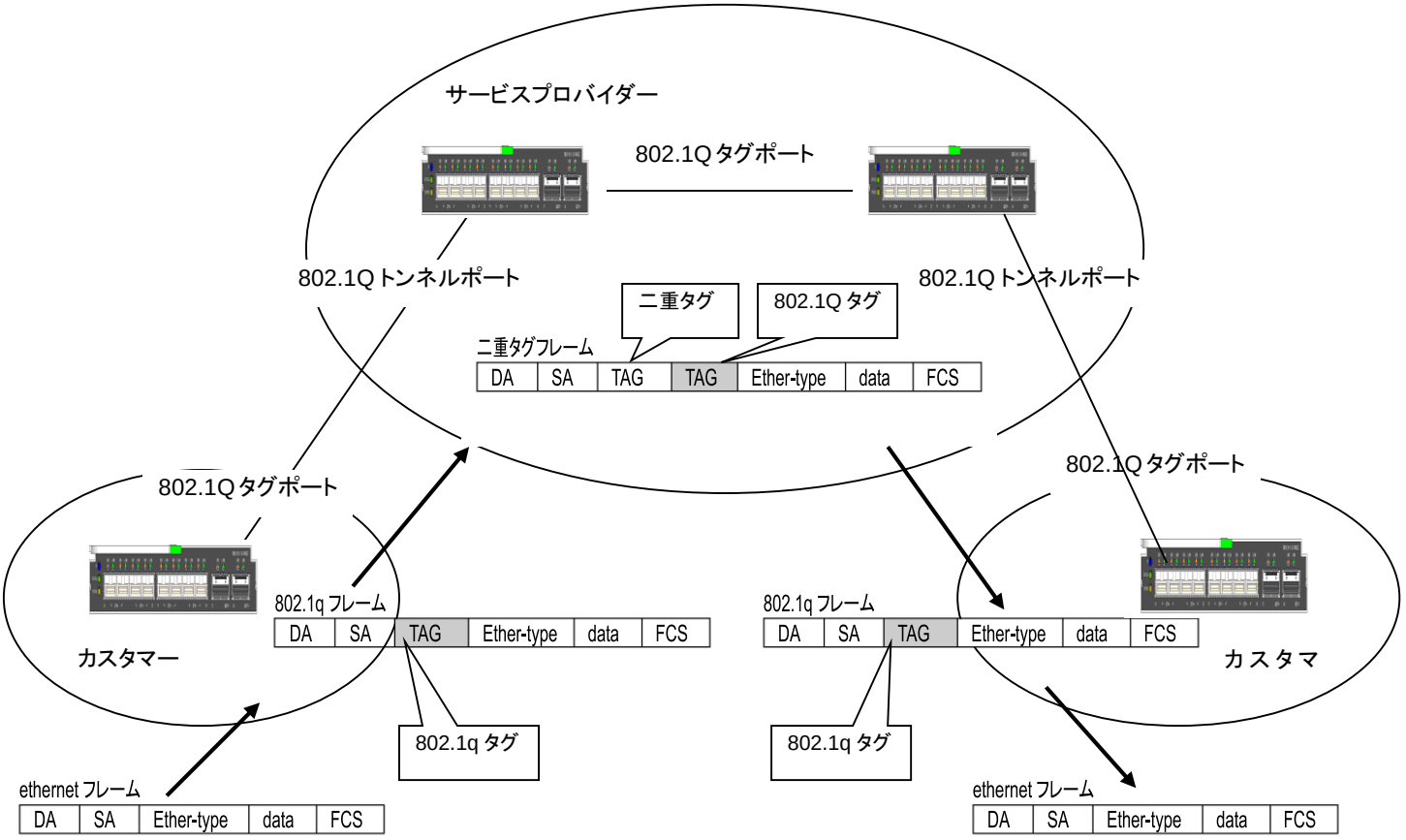
それぞれの状態の意味は以下のとおりです。
・alive状態
サーバが使用可能である状態です。
優先度が高い(定義上の数値が小さい)サーバから優先して使用されます。
同じ優先度のサーバが複数存在する場合は、ランダムにサーバが選択されます。
・dead状態
サーバとのTCP接続失敗やサーバあてのリクエストがタイムアウトしたことにより、そのサーバの使用を一時的に停止している状態です。ほかにalive状態のサーバが存在する場合、定義した優先度の値は使用されません。
復旧待機時間で指定した時間が経過すると、自動的にalive状態に復旧します。
認証を行う場合、すべてのサーバがdead状態になると、ランダムに１つのサーバで試行し、応答の得られたサーバはalive状態に復旧します。

こんな事に気をつけて

・RADIUS クライアント機能および TACACS+クライアント機能との併用はできません。AAA グループに RADIUS クライアント機能(aaa radius) または TACACS+クライアント機能(aaa tacacsp)と LDAP クライアント機能を定義した場合、LDAP クライアント機能は無効となります。AAA グループに LDAP クライアント機能とユーザ情報(aaa user)の両方を定義した場合は、LDAP クライアント機能で認証が行われます。LDAP クライアント機能で認証が失敗しても、ユーザ情報での認証は行われません。

2.32IEEE802.1Q トンネリング機能

IEEE802.1Qトンネリング機能とは、サービスプロバイダー用に設計された機能です。
IEEE802.1Qトンネリングにより、カスタマーのVLANトラフィックを他のVLANトラフィックに影響を与えずに、サービスプロバイダーのネットワークを経由して伝送することができます。
下図において、カスタマーの802.1Qタグポートからサービスプロバイダーのトンネルポートに発信されるパケットは、802.1Qタグがついています。次に、サービスエッジのトンネルポートで受信してサービスプロバイダーの802.1Qタグポートから発信される場合、別の802.1Qタグが再び付加されます（二重タグ）。サービスプロバイダー内で転送される場合、２度目に付加されるタグを付けたり外すことでスイッチングを行うので、元の802.1Qタグは保護されます。そして、エッジスイッチのトンネルポートからカスタマー側のスイッチに送信される時は、タグは付加されません。



導入のメリット

サービスプロバイダーが、複数のカスタマーに対してWAN(Ethernet)を提供する場合、カスタマーで使用するVLAN IDに重複が発生する可能性だけでなく、すぐにIEEE802.1Q仕様のVLAN制限（４０９６個）を超えてしまいます。IEEE802.1Qトンネリングにより、カスタマーから送信されるタグ付きトラフィックに対して、キャリア側のスイッチで再びタグを付加することにより、カスタマーVLANトラフィックを単一のVLANトラフィックにして送信できる事からVLAN ID重複やVLAN制限の問題を解決します。

こんなことに気をつけて

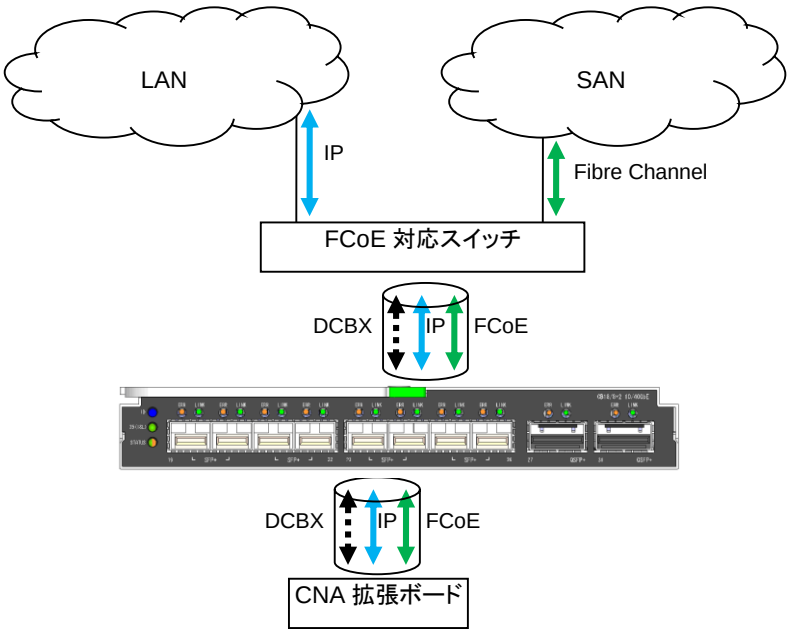
・STP(スパニングツリー)機能、およびLLDP(Link Layer Discovery Protocol)機能を定義した場合、そのポートは利用できなくなります。

・IEEE802.1Qトンネルポートの所属するVLAN IDに、IEEE802.1Qトンネルポートでないポートをuntag設定したポートは、二重タグを適用しないためパケットが誤ったあて先に送信されることがあります。

・IEEE802.1Qトンネルポートでは、"acl vlan"定義は該当ポートに設定したタグなしのポートVLANに対して動作します。

・プロトコルVLAN機能併用時、IEEE802.1Qトンネルポートでプロトコルvlanとして認識されるフレームを受信 した場合、そのフレームはプロトコルVLANが適用対象となり、IEEE802.1Qトンネリング機能は無効となります。

2.33CEE 機能



CEE (Converged Enhanced Ethernet) 機能とは、従来の LAN, IPC, SAN など、タイプの異なる通信を一つのネットワークに統合するために必要な拡張を Ethernet に追加したものです。SAN (Storage Area Network) のプロトコルである Fibre Channel を Ethernet で送受信するための FCoE (Fibre Channel over Ethernet) 等で利用されます。本装置では、CEE 機能として以下の要素技術をサポートしています。

ETS (Enhanced Transmission Selection)
複数のトラフィッククラス (Traffic Class. または優先度 Priority) のフローをトラフィッククラスグループ (Traffic Class Group TCG. またはPriority Group PG) としてまとめ、その流量を制御することで各トラフィッククラスグループの最小帯域を確保する機能です。IEEE802.1Qaz として検討されています。各トラフィッククラスグループには、LAN, IPC, SAN など、タイプの異なる通信を割り当てることが想定されています。

DCBX (Data Center Bridging eXchange)
CEE 装置のピア間で交換される情報を定義し、ETS (IEEE802.1Qaz) の一部として検討されています。各ピアの ETS や PFC 設定情報をお互いに通知し、可能であれば設定を整合させる処理を行います。LLDP の拡張として実現されています。

PFC (Priority-based Flow Control)
2.2 節で説明したフロー制御機能はリンクレベルの制御でしたが、これを優先度 (Priority) ごとのフロー制御ができるように拡張するもので、IEEE802.1Qbb として検討されています。たとえば FCoE のようにフレームロスに弱いプロトコルを通す Priority や PG は PFC を有効にし、ロスを許容しても高いスループットが求められるフローは PFC を無効にするような運用が想定されています。

こんなことに気をつけて

・CEE 機能はポートまたはリンクアグリゲーション毎に有効 / 無効を設定できますが、CEE 機能の有効 / 無効や設定が異なるポート間でフレーム転送を行った場合は帯域制御や PFC 制御を保証できません。すべてのポートで設定を同一にするか、egress permission コマンドや VLAN の設定を利用して、CEE 機能の有効 / 無効や設定が異なるポート間でのフレーム転送が行われないようにしてください。

・CEE 機能は、出力レート制限機能、IEEE802.1Qトンネリング機能とは併用できません。CEE機能が有効なポートにこれらの機能が定義された場合、そのポートは利用できなくなります。

・CEE 機能が有効なポートでは、ETHERポートに対するACL によるキュー指定またはキュー変更機能の設定は無効となります。

・CEE 機能が有効なポートでは、WRR、WDRR を用いた優先制御機能、VLANに対するACL によるキュー指定またはキュー変更機能の設定、2.2 節で説明したリンクレベルのフロー制御機能、qos cosmap コマンドによるプライオリティ毎の格納キュー設定は無視されます。

・トラフィッククラスグループ 15 を使用する場合、トラフィッククラスグループ 15 は最優先で転送され、その他のトラフィッククラスグループは残りの帯域をそれぞれ指定された帯域幅の割合で分けあいながら転送されます。

・PFC は DCBX によるピア間でのネゴシエーションが完了して初めて有効になります。

・PFC が有効なトラフィッククラスグループのフレームに関しては、buffermode コマンドの設定にかかわらず、出力キューの長さが制限されません。このため PFC が有効なトラフィッククラスグループのフレームが多数滞留する状況では他のトラフィッククラスグループまたは他ポート宛のフレームが廃棄されやすくなる可能性があります。

・CEE 機能は 2300Bytes 以下のサイズのフレームに対して有効です。それ以上のサイズのフレームについてはフロー制御が有効に機能しないことや帯域制御が期待通りにならないことがあります。

・トラフィッククラスグループの帯域は百分率で指定しますが、実際に制御可能な最小帯域と最大帯域の比には制限があります。PFC が無効なトラフィッククラスグループのみが 2 つ定義されている場合、最小帯域と最大帯域の比は最大 1:14 になります。PFC が無効なトラフィッククラスグループのみが 3 つ定義されている場合、最小帯域と最大帯域の比は最大 1:7 になります。また、PFC が有効なトラフィッククラスグループが定義されている場合、最小帯域と最大帯域の比は最大 1:4 程度になります。例えば、10Gbps のポートに対して PFC が有効なトラフィッククラスグループと PFC が無効なトラフィッククラスグループを 1 つずつ定義して使用する場合、帯域をそれぞれ 10 および 90 と設定しても実際には 2Gbps と 8Gbps 程度になるように制御されます。

2.34エッジ仮想スイッチ機能

エッジ仮想スイッチ(Edge Virtual Bridging)機能とは、サーバ仮想化環境においてサーバに接続する隣接スイッチに必要な機能です。サーバ仮想化環境ではサーバ仮想化ソフト上で動作する仮想スイッチが存在し、仮想マシン間の通信をスイッチングします。このため、隣接スイッチでは仮想スイッチの形態に応じた処理が必要となります。本装置ではエッジ仮想スイッチ機能として以下の要素技術をサポートしています。

・Virtual Ethernet Bridge (VEB)
同一物理マシン上の仮想マシン間の通信を仮想化ソフト上で動作する仮想スイッチで行います。

・Virtual Ethernet Port Aggregator (VEPA)
仮想スイッチの処理を外部の物理スイッチにオフロードする技術です。物理スイッチは個々の仮想マシンをMACアドレスで識別し、同一物理サーバ上の仮想マシン宛のフレームはリフレクティブリレーにより送信を行います。

こんなことに気をつけて

・STP(スパニングツリー)機能を定義した場合、そのポートは利用できなくなります。
・リンクアグリゲーションで機能を定義する場合はそのリンクアグリゲーションを構成する全てのポートで同様に定義してください。