Catalyst 4000 Supervisor III および IV でのレガシープロトコルのサポート

内容

概要

この文書では、新しい Supervisor III または IV を搭載した Catalyst 4000 または 4500 が、IPX、AppleTalk、Data-Link Switching（DLSw）などの既存プロトコルのサポートにどのように優れているかを説明します。このスーパーバイザは、ハードウェア スイッチ IP バージョン 4（IPv4）パケットのために設計されています。

前提条件

要件

このドキュメントの読者は、IPX、AppleTalk、および DLSw の設定に関する知識が必要です。これらのプロトコルの情報については、以下のサポートページを参照してください。

- 「IPX 技術に関するサポートページ」
- 「AppleTalk 技術に関するサポートページ」
- 「DLSw 技術に関するサポートページ」

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Supervisor IV を搭載した Catalyst 4507R
- Cisco IOS® ソフトウェア リリース 12.1(13)EW

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

IPX のルーティング

Cisco IOS ソフトウェア リリース 12.1(12c)EW 以降では、ルーティング IPX がサポートされています。初期リリースのパフォーマンスは、20 ~ 30 kpps の範囲でした。Cisco IOS ソフトウェア リリース 12.1(13)EW では、パフォーマンスが 80 ~ 90 kpps にまで増加しています。ソフトウェア修正プログラム（Cisco bug ID CSCea85204（登録ユーザ専用））を利用できる、Cisco IOS ソフトウェア リリース 12.1(19)EW 以降のご使用をお勧めします。 この転送レートは、スイッチを通過するすべてのフローで共通です。この転送によるソフトウェア処理が原因で、CPU の負荷が増大します。そのため、達成される転送レートは、スイッチ CPU によって異なります。たとえば、Border Gateway Protocol（BGP）ポリシー、Enhanced Interior Gateway Routing Protocol（EIGRP）や Open Shortest Path First（OSPF）のルート、スイッチ仮想インターフェイス（SVI）などをスイッチがいくつ持っているかによって左右されます。

注：IPXパケットがソフトウェアルーティングであっても、IPv4パケットは引き続きハードウェアでルーティングされます。

サポートされている機能

- IPX 用の MAC アクセス コントロール リスト（ACL）。IPX パケットを制御するために使用され、Cisco IOS ソフトウェア リリース 12.1(12c)EW 以降でサポートされています。
- IPX Routing Information Protocol（RIP）（サービス アドバタイジング プロトコル（SAP））
- IPX Enhanced Interior Gateway Routing Protocol（EIGRP）
- ヘッダ圧縮

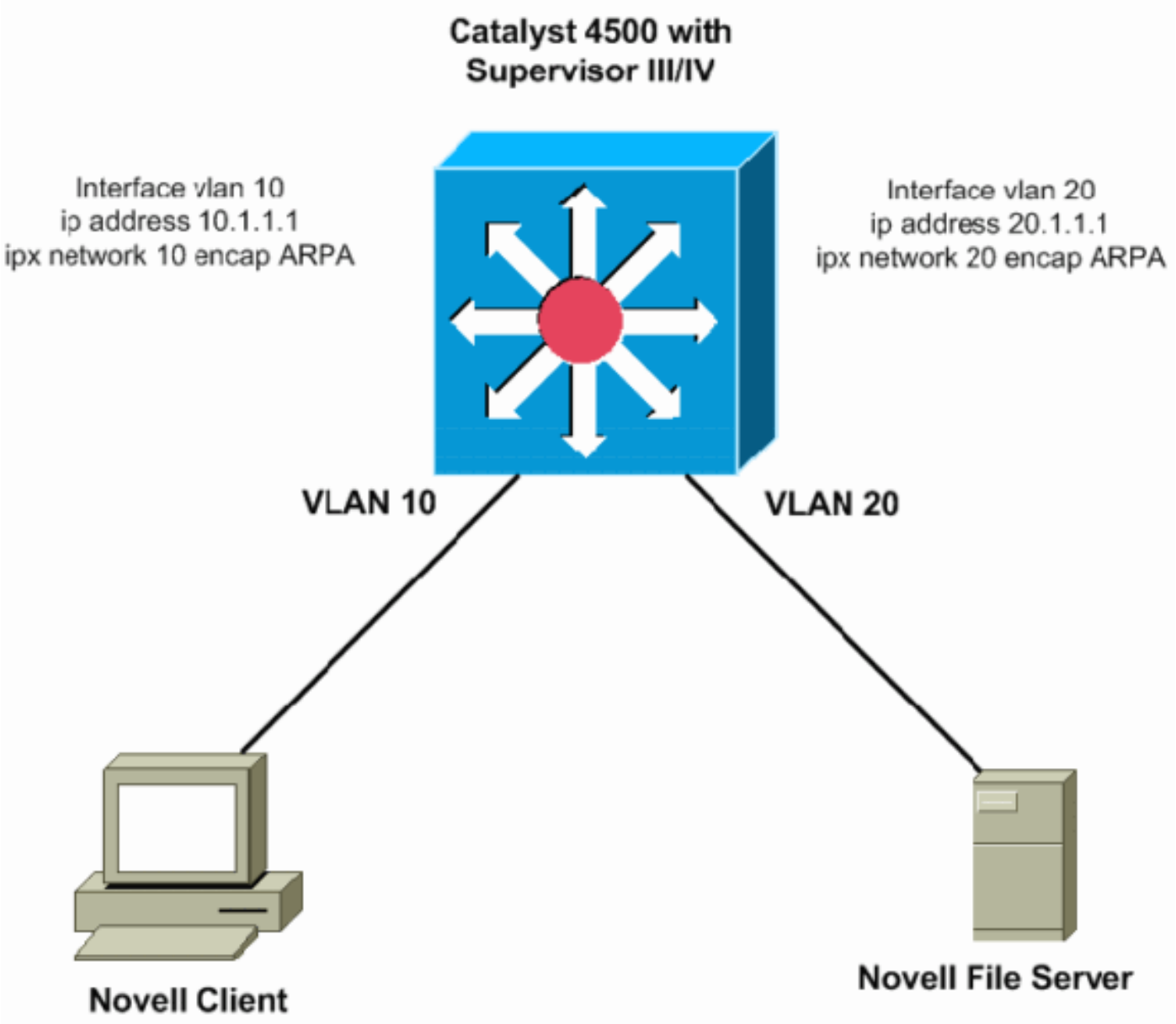
注：EIGRPはSAPの差分アップデートを行うために、IPX EIGRPはルータ間のパフォーマンスを向上させるために推奨されるルーティングプロトコルです。IPX EIGRP は、 サーバレスのセグメント上でもイネーブルにすることができます。IPX EIGRP の詳細は、「IPX-EIGRP の概要」を参照してください。

制限

- パケットの IPX ルーティングはハードウェアでサポートされません。これはソフトウェア処理でサポートされます。
- Novell IPX 標準 (800-899)、IPX 拡張 (900-999)、Get Nearest Server（GNS）、SAP フィル

タ (1000-1099) の各アクセスリストは現在サポートされていません。
- IPX ソフトウェア ルーティングでサポートされないものは以下のとおりです。Next Hop Resolution Protocol（NHRP）Netware Link Service Protocol（NLSP; Netware リンク サービス プロトコル）ジャンボ フレーム

次の図は、IPX をルーティングする Supervisor III または IV を搭載した Catalyst 4000 または 4500 の標準的なシナリオを表しています。このシナリオでは、クライアントはVLAN 10にあり、サーバはVLAN 20にあります。IPXは、次の図に示すように、VLAN 10および20インターフェイスで設定されています。



AppleTalk のルーティング

Cisco IOS ソフトウェア リリース 12.1(12c)EW 以降では、ルーティング AppleTalk がサポートされています。初期リリースのパフォーマンスは、20 ~ 30 kpps の範囲でした。Cisco IOS ソフトウェア リリース 12.1(13)EW では、パフォーマンスが 80 ~ 90 kpps にまで増加しています。ソフトウェア修正プログラム（Cisco bug ID CSCea85204（登録ユーザ専用））を利用できる、Cisco IOS ソフトウェア リリース 12.1(19)EW 以降のご使用をお勧めします。この転送レートは、スイッチを通過するすべてのフローで共通です。この転送によるソフトウェア処理が原因で、CPU の負荷が増大します。そのため、達成される転送レートはスイッチ CPU に依存しています。たとえば、BGP ポリシー、EIGRP や OSPF ルート、SVI などをスイッチがいくつ持っている

かによって左右されます。

注：AppleTalkパケットはソフトウェアルーティングですが、IPv4パケットは引き続きハードウェアでルーティングされます。

サポートされている機能

- AppleTalk 用の MAC ACL。IPX パケットを制御するために使用され、Cisco IOS ソフトウェア リリース 12.1(12c)EW 以降でサポートされています。
- Datagram Delivery Protocol（DDP; データグラム送達プロトコル）ルーティング
- Routing Table Maintenance Protocol（RTMP; ルーティング テーブル メンテナンス プロトコル）
- Name Binding Protocol（NBP; ネーム バインディング プロトコル）
- AppleTalk Echo Protocol（AEP;AppleTalk エコー プロトコル）
- AppleTalk EIGRP

注：AppleTalk EIGRP は、EIGRP が差分更新を行うため、ルータ間で優れた性能を発揮するのに適切なルーティング プロトコルです。AppleTalk EIGRP についての情報は、『AppleTalk の設定』の「AppleTalk Enhanced IGRP の設定」の項を参照してください。

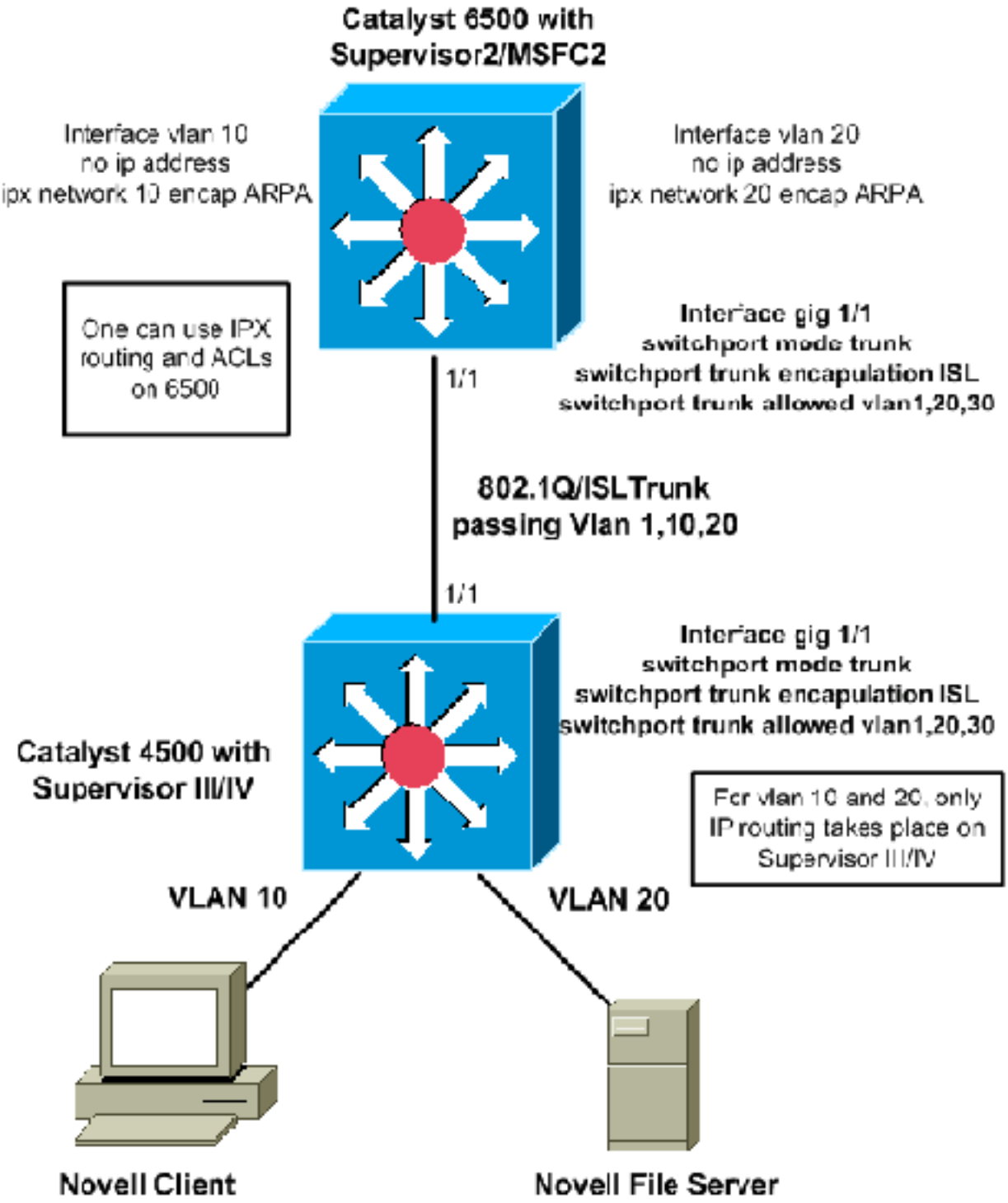
制限

- パケットの AppleTalk ルーティングはハードウェアでサポートされません。これはソフトウェア処理でサポートされます。
- 現在、AppleTalk ACL はサポートされていません。
- AppleTalk ソフトウェア ルーティングでサポートされないものは以下のとおりです。AppleTalk Update-Based Routing Protocol (AURP; AppleTalk アップデートベース ルーティング プロトコル)PPP の AppleTalk コントロール プロトコルジャンボ フレーム

外部ルータでのルーティング

ネットワークで、上記で述べたより高速の既存プロトコルのルーティング パーフォーマンスが必要であれば、外部ルータ（レイヤ 3（L3）デバイス）が適しています。 このような L3 デバイスには、Catalyst 6000 マルチレイヤ スイッチ フィーチャ カード（MSFC）、Catalyst 5000 RSM、L3 スイッチ（2948G-L3 など）の他、任意のルータがあります。これらのデバイスは IPX のルーティングをハードウェア アシスタンスで行い、その性能はスーパーバイザ III や IV よりもはるかに優れています。スーパーバイザ III および IV は IP をハードウェア スイッチング パスでルーティングできますが、外部デバイスはレガシープロトコルをルーティングします。

以下の図は、MSFC のコア/ディストリビューション Catalyst 6500 で IPX がルーティングされたシナリオを表しています。IP は、スーパーバイザ III または IV を搭載した Catalyst 4500 の VLAN 10 と VLAN 20 との間でルーティングされます。2 つのスイッチがトランク接続され、必要な VLAN に許可を与えています。このタイプの設計の利点は、標準 IPX ACL が使用できることと、2 つの VLAN 間のパケット転送がハードウェアでサポートされるため、性能が向上することです。ピア間での通信に Catalyst 6500 や外部ルータで IPX ルーティング プロトコルを使用して、データベース交換をルーティングすることが可能です。



さらなるパフォーマンス向上

この項では、外部ルータでの IPX または AppleTalk スイッチングに関して、パーフォーマンス向上が可能なその他の要素を説明します。

- 外部ルータと Catalyst スイッチ間のリンクは、port-channel リンク化して、より高い帯域幅を達成し、リンクに冗長性を持たせることができます。
- すべての帯域幅を非 IP トラフィックに使用するよう、IP トラフィックをリンク外にフィルタにかけることができます。次に、Quality of Service（QoS）を通して、IP トラフィックをフィルタにかける設定例を示します。

1. スーパーバイザで QoS をイネーブルにするには、QoS グローバル コンフィギュレーション

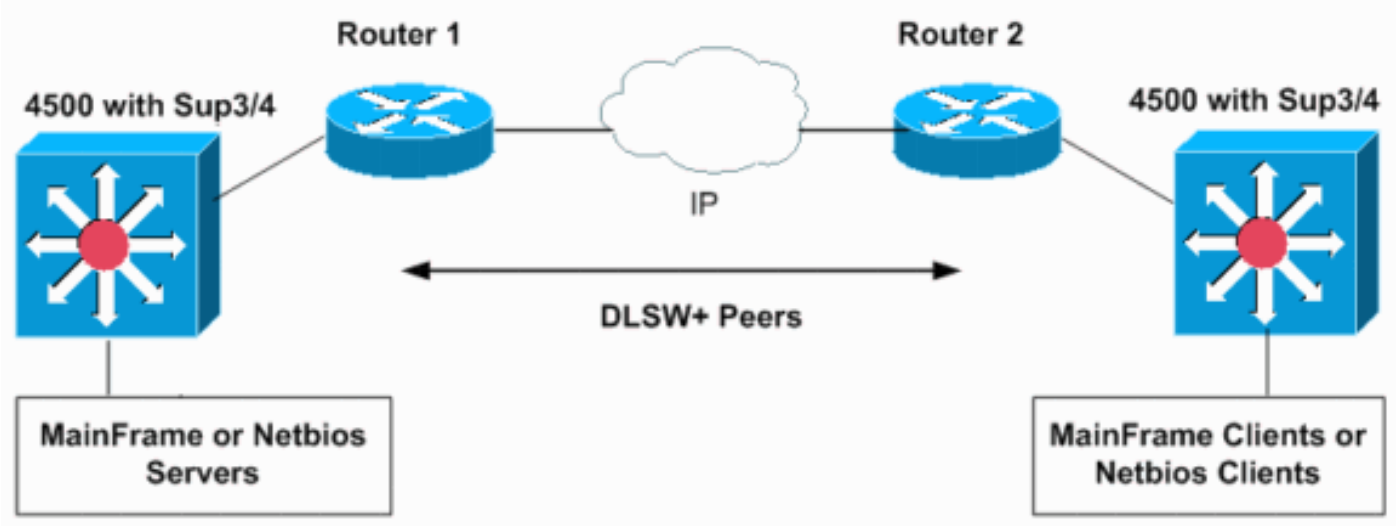
コマンド qos を発行します。

2. すべての IP トラフィックに合致するように ACL を定義します。
```
access-list 101 permit ip any any
```
3. 手順 2 で定義した ACL に合致するクラスマップを定義します。
```
class-map match-any ip-drops
  match access-group 101
```
4. ポリシーを定義します。手順 3 で定義されたクラスのすべてのトラフィックをドロップするポリサーを定義します。32 kbps の最小粒度を使用してすべてのトラフィックをポリシングします。スーパーバイザはこのポリサーで、32 kbps を超えるすべての IP トラフィックをドロップします（Cisco IOS IP ping は通ることができない場合があります）。
```
policy-map drop-ip
  class ip-drops
    police 32000 bps 1000 byte conform-action drop exceed-action drop
```
5. 外部ルータに接続するインターフェースにサービス ポリシー アウトバウンドを適用します。
```
interface GigabitEthernet 1/1
    service-policy output drop-ip
```

ポリシング アクションを確認するために、show policy-map interface interface-idコマンドを発行します。

DLSw

DLSw はスーパーバイザ III と IV ではサポートされていません。SNA や IP プロトコルを使用したネットワークの場合、Catalyst 4000 スーパーバイザ III と IV での IP トラフィックのルーティング、および、外部ルータ上の Cisco IOS ソフトウェアでの DLSw スイッチングによる SNA トラフィックのブリッジが可能です。



次の設定は、異なる 2 つの SNA ドメインで、それぞれ Catalyst 6500 MSFC2 を使用した VLAN 10 と 20 での SNA トラフィックをブリッジする方法を示しています。スーパーバイザ III と IV の 802.1Q トランクを使用して、SNA または NetBIOS トラフィックをシスコ ルータや Catalyst 6500 スイッチに配信する（ブリッジする）ことが可能です。

hostname MSFCRouter-1 interface loopback1 ip address 1.1.1.1 !	hostname MSFCRouter-2 interface loopback1 ip address 2.2.2.2 !

int vlan10 ip add 10.10.10.254 255.255.255.0 bridge-group 1 ! bridge 1 protocol ieee dlsw local-peer peerid 1.1.1.1 dlsw remote-peer 0 tcp 2.2.2.2 dlsw bridge-group 1	int vlan20 ip add 10.10.20.254 255.255.255.0 bridge-group 2 ! bridge 2 protocol ieee dlsw local-peer peerid 2.2.2.2 dlsw remote-peer 0 tcp 1.1.1.1 dlsw bridge-group 2

これは、異なるドメインでの Catalyst 6500 スイッチのネットワーク設定を示しています。VLAN 10 と 20 が同一のスイッチまたは MSFC にある場合、DLSw は必要ありません。1 つの MSFC 上で、シンプルな IEEE ブリッジグループが機能します。

MAC 拡張 ACL と VLAN マップを使用した非 IP パケットのフィルタリング

スーパーバイザ III および IV は、IPX、AppleTalk、または他のレガシー プロトコル ACL をサポートしていません。それらのフィルタリングには、MAC 拡張 ACL と VLAN アクセス マップを組み合わせて行うことができます。VLAN マップは VLAN 内のすべてのトラフィックのアクセスをコントロールできます。VLAN に出入りしたり、VLAN 内でブリッジされるパケットをルーティングするスイッチに、VALN マップを適用できます。ルータ ACL とは異なり、VLAN マップは方向（入力、出力）では定義されません。

このシナリオ例では、次の 2 点を設定上の目標としています。

- ホスト 000.0c00.0111 からホスト 000.0c00.0211 へのすべての IPX トラフィックを阻止し、VLAN 20 内での他のすべての IPX、非 IP プロトコルのトラフィックを許可します。
- VLAN 10 へのすべての AppleTalk トラフィックを拒否します。

注：IP パケットはMAC ACL ではフィルタリングできません。

注：名前付きMAC拡張ACLはL3インターフェイスに適用できません。

1. 拡張 MAC ACL の定義で VLAN マップへの注意を引くトラフィックを定義します。

```
Switch(config)# mac access-list extended denyIPXACL

Switch(config-ext-macl)# permit host 000.0c00.0111 host 000.0c00.0211  protocol-family ?
  appletalk
  arp-non-ipv4
  decnet
  ipx
  ipv6
  rarp-ipv4
  rarp-non-ipv4
  vines
  xns

Switch(config-ext-macl)# $00.0c00.0111 host 000.0c00.0211 protocol-family ipx

Switch(config-ext-macl)# exit

Switch(config)# mac access-list extended denyatalk

Switch(config-ext-macl)# permit any any protocol-family appletalk
```

```
Switch(config)#
```

2. show access-list *access-list-name* コマンドを発行し、設定された拡張 MAC ACL を確認します。上記例の ACL は `denyIPXACL  denyatalk` です。

```
Switch# show access-lists denyIPXACL

Extended MAC access list denyIPXACL
    permit   host 0000.0c00.0111 host 0000.0c00.0211 protocol-family ipx

Switch# show access-lists denyatalk

Extended MAC access list denyatalk
    permit any any protocol-family appletalk
```

3. VLAN アクセス マップを使用してアクションを定義します。

```
Switch(config)# vlan access-map denyIPX

Switch(config-access-map)# match mac address denyIPXACL

Switch(config-access-map)# action drop

Switch(config-access-map)# exit

Switch(config)# vlan access-map denyapple

Switch(config-access-map)# match mac address denyatalk

Switch(config-access-map)# action drop

Switch(config-access-map)# exit
```

4. show vlan access-map *name コマンドを発行して、定義された VLAN アクセス マップを確認します。*

```
Switch# show vlan access-map denyIPX

Vlan access-map "denyIPX"  10
  Match clauses:
    mac address: denyIPXACL
  Action:
    drop

Switch# show vlan access-map denyapple

Vlan access-map "denyapple"  10
  Match clauses:
    mac address: denyatalk
  Action:
    drop
```

5. vlan filter *name vlan-list vlan-list* コマンドを発行して、VLAN マップを VLAN にマップします。この例では、VLAN 20 内の指定したホスト間で IPX をフィルタリングし、VLAN 10 で AppleTalk を拒否します。

```
Switch(config)# vlan filter denyIPX vlan-list 20

Switch(config)# vlan filter denyapple vlan-list 10
```

6. show vlan filter vlan *vlan-id* コマンドを発行して、VLAN フィルタが適切であることを確認します。

```
Switch# show vlan filter vlan 20

Vlan 20 has filter denyIPX.
```

```
Switch# show vlan filter vlan 10

Vlan 10 has filter denyapple.
```

その他のサポートされない機能

スーパーバイザ III および IV は次の機能をサポートしていません。

- フォールバック ブリッジングや VLAN 間ブリッジングなど、ルーティングできないプロトコルのブリッジ
- DECnet ルーティング

この機能を実行するための外部ルータの使用例は、前項を参照してください。

IPX または AppleTalk ルーティングをイネーブルにした後の CPU の高負荷

IPX や AppleTalk ルーティングをイネーブルにすると、スイッチによりソフトウェアでルーティングされる IPX や AppleTalk のトラフィック量によって CPU 使用率が増大します。**show processor cpu コマンドを発行すると、CPU を使う** `Cat4k Mgmt LoPri` これは、パケットがプロセス スイッチされたことを示します。

```
Switch# show processes cpu

CPU utilization for five seconds: 99%/0%; one minute: 86%; five minutes: 54%
 PID  Runtime(ms)  Invoked  uSecs    5Sec   1Min   5Min TTY Process
   1           8      607     13   0.00%  0.00%  0.00%   0 Load Meter
   2         496     4549    109   0.00%  0.01%  0.00%   0 Spanning Tree
   3           0        1      0   0.00%  0.00%  0.00%   0 Deferred Events
   4        4756      480   9908   0.00%  0.08%  0.11%   0 Check heaps
   5           0        1      0   0.00%  0.00%  0.00%   0 Chunk Manager
   6           0        1      0   0.00%  0.00%  0.00%   0 Pool Manager
   7           0        2      0   0.00%  0.00%  0.00%   0 Timers
   8           4        2   2000   0.00%  0.00%  0.00%   0 Serial Backgroun
   9           4       64     62   0.00%  0.00%  0.00%   0 ARP Input
  10          24        3   8000   0.00%  0.00%  0.00%   0 Entity MIB API
  11           0        1      0   0.00%  0.00%  0.00%   0 SERIAL A'detect
  12           0        1      0   0.00%  0.00%  0.00%   0 Critical Bkgnd
  13       25436      864  29439   0.00%  0.00%  0.00%   0 Net Background
  14           0       58      0   0.00%  0.00%  0.00%   0 Logger
  15          52     2607     19   0.00%  0.00%  0.00%   0 TTY Background
  16         440     2666    165   0.00%  0.00%  0.00%   0 Per-Second Jobs
  17      112328   410885    273   1.66%  2.37%  2.74%   0 Cat4k Mgmt HiPri
  18     1197172    21536  55589  98.56% 84.14% 49.15%   0 Cat4k Mgmt LoPri
  19           0        1      0   0.00%  0.00%  0.00%   0 Routekernel Proc
```

注：IPXまたはAppleTalkルーティングが有効になっていなく、CPU使用率が高い`Cat4k Mgmt LoPri`は、どのパケットがCPUに送信されて処理されるかをトラブルシューティングする必要があります。詳細については、シスコ テクニカル サポートにお問い合わせください。

関連情報

- ACL によるネットワーク セキュリティの設定
- Catalyst 4500 サポート ページ

- LAN 製品に関するサポート ページ
- LAN スイッチングに関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems