イーサネット スイッチ ポートの設定

この章は、次の項で構成されています。

VLAN の設定

VLANは、ユーザの物理的な位置に関係なく、機能、プロジェクトチーム、またはアプリケーションなどで論理的に分割されたスイッチドネットワークです。VLAN は、物理 LAN と同じ属性をすべて備えていますが、同じ LAN セグメントに物理的に配置されていないエンド ステーションもグループ化できます。どのスイッチ ポートも VLAN に割り当てることができます。ユニキャスト、ブロードキャスト、およびマルチキャスト パケットは、VLAN 内のエンド ステーションだけに転送およびフラッディングが行われます。各 VLAN は論理ネットワークと見なされ、VLANに属さないステーション宛てのパケットはルータで転送する必要があります。

IR1101 では、すべてのファスト イーサネット ポートが vlan1 で設定されているため、作成する必要はありません。ギガビット イーサネット ポート（gi0/0/0）のデフォルトはレイヤ 3 です。必要に応じて、ギガビットイーサネットポート（gi0/0/0）をレイヤ2として設定し、vlan1に追加できます。次に例を示します。

```
#config terminal
interface gi0/0/0
switchport
exit
```

以下は vlan 設定の例です。

```
IR1101#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
```

```
1    default                          active    Fa0/0/1, Fa0/0/2, Fa0/0/3, Fa0/0/4
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

IR1101#
```

特定のポートを vlan に割り当てるには、次の手順を実行します。

```
interface fastethernet0/0/4
switchport access vlan 4

interface vlan 4
ip v4 address ...
ipv6 address autoconf

show vlan
```

IOS-XE バージョン 16.10.1 以降は、パケットのトレースとトラブルシューティングに役立つ組み込みシステム管理機能を提供する組み込みパケット キャプチャ（EPC）をサポートしてます。この機能を使用すると、ネットワーク管理者は、シスコデバイスを出入りするか通過するデータ パケットをキャプチャできます。ネットワーク管理者は、キャプチャ バッファ サイズとタイプ（循環または線形）、キャプチャする各パケットの最大バイト数、およびトラフィック フローの方向（入力と出力のどちらか、または両方）を定義する場合があります。パケット キャプチャ レートは、詳細な管理制御を使用してスロットリングできます。たとえば、アクセス コントロール リストを使用してキャプチャ対象パケットをフィルタリングするオプションや、最大パケット キャプチャ レートまたはサンプリング間隔の指定などの詳細な定義を行うオプションが利用できます。詳細については、次の場所にあるガイドを参照してください。
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/epc/configuration/xe-16-10/epc-xe-16-10-book/nm-packet-capture-xe.html

VLAN トランキング プロトコル（VTP）

VTP は、レイヤ 2 のメッセージ プロトコルであり、ネットワーク全体にわたって VLAN の追加、削除、名前の変更を管理することにより、VLAN 設定の整合性を維持します。VTP により、VLAN 名の重複、誤った VLAN タイプの指定、セキュリティ違反など、さまざまな問題を引き起こしかねない設定の誤りや矛盾が最小限に抑えられます。

VLAN を作成する前に、ネットワークで VTP を使用するかどうかを決定する必要があります。VTP を使用すると、1 台または複数のスイッチ上で集中的に設定変更を行い、その変更を自動的にネットワーク上の他のスイッチに伝達できます。VTP を使用しない場合、VLAN に関する情報を他のスイッチに送信できません。VTP は、1 台のスイッチで行われた更新が VTP を介

してドメイン内の他のスイッチに送信される環境で動作するように設計されています。VLAN データベースに対する複数の更新が同一ドメイン内のスイッチ上で同時に発生する環境の場合、VTP は適していません。VLAN データベースの不整合が生じます。

VTP の設定の詳細については、以下を参照してください。http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/geshwic_cfg.html#wp1046901

802.1X 認証の設定

IEEE 802.1x ポート ベース認証は、一般的にアクセス可能なポートから認証されていないクライアントが LAN に接続しないように規制する、クライアント/サーバ ベースのアクセス コントロールおよび認証プロトコルを規定しています。認証サーバがスイッチ ポートに接続する各クライアントを認証したうえで、スイッチまたは LAN サービスにアクセスできるようにします。クライアントが認証されるまで、IEEE 802.1x アクセス コントロールでは、クライアントの接続先であるポートを介して、Extensible Authentication Protocol over LAN（EAPOL）、Cisco Discovery Protocol（CDP）、およびスパニングツリー プロトコル（STP）トラフィックだけが許可されます。認証後、通常のトラフィックをポート経由で送受信できます。

IEEE 802.1x 認証では、ネットワーク内のデバイスにそれぞれ固有の役割があります。

- サプリカント：LAN およびスイッチ サービスへのアクセスを要求し、ルータからの要求に応答するデバイス（ワークステーション）。ワークステーションでは、Microsoft Windows XP オペレーティング システムで提供されるクライアントなど、IEEE 802.1x 準拠のクライアント ソフトウェアが稼働している必要があります（サプリカントはクライアントと呼ばれることもあります）。
- 認証サーバ：サプリカントの実際の認証を実行する装置。認証サーバはサプリカントの識別情報を確認し、そのサプリカントに LAN およびスイッチ サービスへのアクセスを許可すべきかどうかをルータに通知します。ネットワーク アクセス デバイスは、サプリカントと認証サーバ間で認証メッセージを透過的に渡し、サプリカントと認証サーバ間で認証プロセスが実行されます。サプリカントと認証サーバ（RADIUS サーバ）間で使用される EAP 方式が決定されます。EAP 拡張機能を搭載した RADIUS セキュリティ システムは、Cisco Secure Access Control Server バージョン 3.0 以降で使用できます。RADIUS はクライアントおよびサーバ モデルで動作し、RADIUS サーバと 1 つまたは複数の RADIUS クライアントとの間でセキュア認証情報を交換します。
- オーセンティケータ：サプリカントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御するルータ。ルータは、サプリカントと認証サーバ間で仲介装置として動作し、サプリカントからの ID 情報を要求し、その情報を認証サーバで確認し、応答をサプリカントにリレーします。ルータには、EAP フレームのカプセル化/カプセル化解除、および認証サーバとの対話を処理する、RADIUS クライアントが含まれています。

802.1x ポートベース認証の設定方法に関する詳細については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/15-mt/sec-user-8021x-15-mt-book/config-ieee-802x-pba.html

例：スイッチポートでの IEEE 802.1x および AAA のイネーブル化

次に、IR1101 ルータを 802.1x オーセンティケータとして設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# dot1x system-auth-control
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# interface FastEthernet 0/0/1
Router(config-if)# switchport mode access
Router(config-if)# access-session port-control auto
Router(config-if)# dot1x pae authenticator
Router(config-if)# access-session closed
Router(config-if)# access-session host-mode single-host
Router(config-if)# end
```

スパニングツリー プロトコルの設定

スパニングツリープロトコル（STP）は、ネットワーク内のループを回避しながらパスを冗長化するためのレイヤ2リンク管理プロトコルです。レイヤ2イーサネット ネットワークの正常な動作を実現するには、どの2つのステーション間でもアクティブ パスを1つにする必要があります。エンド ステーション間に複数のアクティブ パスがあると、ネットワークにループが生じます。このループがネットワークに発生すると、エンドステーションにメッセージが重複して到着する可能性があります。また、スイッチも複数のレイヤ2インターフェイスのエンドステーション MAC アドレスを学習する可能性が出てきます。このような状況によって、ネットワークが不安定になります。スパニングツリーの動作は透過的であり、エンドステーション側で、単一 LAN セグメントに接続されているのか、複数セグメントからなるスイッチド LAN に接続されているのかを検出することはできません。

STP は、スパニングツリー アルゴリズムを使用し、スパニングツリーのルートとして冗長接続ネットワーク内のスイッチを1つ選択します。スパニングツリーアルゴリズムは、アクティブトポロジでのポートの役割に基づいて各ポートに役割を割り当てることにより、スイッチド レイヤ 2 ネットワーク上で最良のループフリー パスを算出します。

- ルート：スパニングツリー トポロジに対して選定される転送ポート
- 指定：各スイッチド LAN セグメントに対して選定される転送ポート
- 代替：スパニングツリーのルート ブリッジへの代替パスとなるブロック ポート
- バックアップ：ループバック コンフィギュレーションのブロック ポート

すべてのポートに役割が指定されているスイッチ、またはバックアップの役割が指定されているスイッチはルート スイッチです。少なくとも1つのポートに役割が指定されているスイッチは、指定スイッチを意味します。スパニング ツリーは、冗長データ パスを強制的にスタンバイ（ブロック）ステートにします。スパニングツリーのネットワーク セグメントでエラーが発生したときに冗長パスが存在する場合は、スパニングツリーアルゴリズムがスパニングツリートポロジを再計算し、スタンバイ パスをアクティブにします。スイッチは、定期的にブリッジ プロトコル データ ユニット（BPDU）と呼ばれるスパニングツリー フレームを送受信します。スイッチはこのフレームを転送しませんが、このフレームを使用してループフリー パスを構築

します。BPDU には、送信側スイッチおよびそのポートについて、スイッチおよび MAC アドレス、スイッチ プライオリティ、ポート プライオリティ、パス コストなどの情報が含まれます。スパニングツリーはこの情報を使用して、スイッチド ネットワーク用のルート スイッチおよびルート ポートを選定し、さらに、各スイッチド セグメントのルート ポートおよび指定ポートを選定します。

スイッチの 2 つのポートがループの一部になっている場合、スパニングツリー ポート プライオリティとパス コストの設定値によって、どちらのポートをフォワーディング ステートにするか、どちらをブロッキング ステートにするかが制御されます。スパニングツリー ポート プライオリティ値は、ネットワーク トポロジにおけるポートの位置とともに、トラフィック転送におけるポートの位置がどれだけ適切であるかを表します。パス コストの値は、メディアの速度を表します。

STP の設定に関する詳細については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/NIM/software/configuration/guide/4_8PortGENIM.html#pgfId-1079138

例：スパニングツリー プロトコルの設定

次に、ギガビット イーサネット インターフェイスのスパニングツリー ポート プライオリティの設定の例を示します。ループが発生した場合、スパニングツリーはポート プライオリティを使用して、フォワーディング ステートにするインターフェイスを選択します。

```
Router# configure terminal
Router(config)# interface FastEthernet 0/0/1
Router(config-if)# spanning-tree vlan 1 port-priority 64
Router(config-if)# end
```

ギガビット イーサネット インターフェイスのスパニングツリー ポート コストを変更する方法の例を示します。ループが発生した場合、スパニングツリーはコストを使用して、フォワーディング ステートにするインターフェイスを選択します。

```
Router#configure terminal
Router(config)# interface FastEthernet 0/0/1
Router(config-if)# spanning-tree cost 18
Router(config-if)# end
```

VLAN 10 のブリッジ プライオリティを 33792 に設定する例を示します。

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 priority 33792
Router(config)# end
```

VLAN 10 の hello タイムを 4 秒に設定する例を示します。hello タイムはルート スイッチがコンフィギュレーション メッセージを生成する間隔です。

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 hello-time 7
Router(config)# end
```

転送遅延時間を設定する例を示します。転送遅延時間は、スパニングツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、インターフェイスが待機する秒数です。

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 forward-time 21
Router(config)# end
```

スパニング ツリーの最大エージング インターバルの設定の例を示します。最大エージング タイムは、再構成を試行するまでにスイッチがスパニングツリー コンフィギュレーション メッセージを受信せずに待機する秒数です。

```
Router# configure terminal
Router(config)# spanning-tree vlan 20 max-age 36
Router(config)# end
```

スイッチを VLAN 10 のルート ブリッジとして設定し、ネットワークの直径を 4 に設定する例を示します。

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 root primary diameter 4
Router(config)# exit
```

MAC アドレス テーブル操作の設定

MAC アドレス テーブルには、スイッチがポート間のトラフィック転送に使用するアドレス情報が含まれています。このアドレス テーブルに登録されたすべての MAC アドレスは、1 つまたは複数のポートに対応しています。アドレス テーブルに含まれるアドレス タイプには、次のものがあります。

- ダイナミック アドレス：スイッチが学習し、使用されなくなった時点でドロップされる送信元 MAC アドレス。エージング タイム設定を使用して、テーブル内で使用されていないアドレスをスイッチが保持する期間を定義します。
- スタティック アドレス：手動で入力され、期限切れにならず、スイッチのリセット時にも消去されないユニキャスト アドレス。

アドレス テーブルは、宛先 MAC アドレス、対応する VLAN（仮想 LAN）ID、アドレスに対応付けられたポート、およびタイプ（スタティックまたはダイナミック）のリストです。

セキュア MAC アドレスのイネーブル化、スタティック エントリの作成、セキュア MAC アドレス最大数の設定、エージング タイムの設定の例については、「例：MAC アドレス テーブル操作」を参照してください。

MAC アドレス テーブルの操作の設定に関する詳細については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/geshwic_cfg.html#wp1048223

例：MAC アドレス テーブル操作

次に、MAC アドレス テーブルにスタティック エントリを作成する例を示します。

```
Router# configure terminal
Router(config)# mac address-table static 0002.0003.0004 interface FastEthernet 0/0/1
vlan 3
Router(config)# end
```

次に、エージング タイマーを設定する例を示します。

```
Router# configure terminal
Router(config)# mac address-table aging-time 300
Router(config)# end
```

スイッチ ポート アナライザの設定

Cisco IR1101 がサポートしているのは、ローカル SPAN のみ、かつ最大 1 つの SPAN セッションです。ポートを通過するネットワーク トラフィックを解析するには、SPAN を使用して、そのスイッチ上の別のポート、またはネットワーク アナライザやその他のモニタ デバイスもしくはセキュリティ デバイスに接続されている別のスイッチ上のポートに、トラフィックのコピーを送信します。SPAN は送信元ポート上で受信、送信、または送受信されたトラフィックを宛先ポートにコピー（ミラーリング）して、解析します。SPAN は発信元ポート上のネットワーク トラフィックのスイッチングには影響しません。宛先ポートは SPAN 専用にする必要があります。SPAN または RSPAN セッションに必要なトラフィック以外、宛先ポートがトラフィックを受信したり転送したりすることはありません。

SPAN を使用してモニタできるのは、送信元ポートを出入りするトラフィックまたは送信元に出入りするトラフィックだけです。送信元にルーティングされたトラフィックはモニタできません。たとえば、着信トラフィックをモニタしている場合、別の送信元からルーティングされているトラフィックはモニタできません。ただし、送信元で受信し、別の送信元にルーティングされるトラフィックは、モニタできます。

スイッチド ポート アナライザ（SPAN）セッションの設定方法については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/15-0_2_se/configuration/guide/scg3750/swspan.html

例：SPAN の設定

ギガビット イーサネット送信元インターフェイスからの双方向トラフィックをモニタするように SPAN セッションを設定する方法の例を示します。

```
Router# configure terminal
Router(config)# monitor session 1 source FastEthernet 0/0/1
Router(config)# end
```

ギガビット イーサネット インターフェイスを SPAN セッションの宛先として設定する方法の例を示します。

```
Router# configure terminal
Router(config)# monitor session 1 destination FastEthernet 0/0/1
Router(config)# end
```

SPAN セッション 1 の SPAN 送信元としてのギガビット イーサネットを削除する方法の例を示します。

```
Router# configure terminal
Router(config)# no monitor session 1 source FastEthernet 0/0/1
Router(config)# end
```

IGMP スヌーピングの設定

IGMP スヌーピングは、レイヤ2インターフェイスを動的に設定し、マルチキャスト トラフィックが IP マルチキャスト デバイスと対応付けられたインターフェイスにだけ転送されるようにすることによって、マルチキャスト トラフィックのフラッディングを制限します。名称が示すとおり、IGMP スヌーピングの場合は、LAN スイッチでホストとルータ間の IGMP 伝送をスヌーピングし、マルチキャスト グループとメンバ ポートを追跡する必要があります。特定のマルチキャスト グループについて、ホストから IGMP レポートを受信したスイッチは、ホストのポート番号を転送テーブル エントリに追加します。ホストから IGMP Leave Group メッセージを受信した場合は、テーブル エントリからホスト ポートを削除します。マルチキャスト クライアントから IGMP メンバーシップ レポートを受信しなかった場合にも、スイッチはエントリを定期的に削除します。

マルチキャスト ルータは、すべての VLAN に定期的にジェネラル クエリーを送出します。このマルチキャスト トラフィックに関心のあるホストはすべて Join 要求を送信し、転送テーブルのエントリに追加されます。

IR1101 で IGMP スヌーピングを設定するには、ip igmp snooping enable コマンドを使用します。

デフォルトでは、IGMP スヌーピングは IR1101 で有効です。

MLD スヌーピングは IR1101 でもサポートされています。詳細については、次のドキュメントセットを参照してください。 https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/16-1/configuration_guide/b_161_consolidated_3850_cg/b_161_consolidated_3850_cg_chapter_01100.html