CHAPTER 10

イーサネット スイッチの設定

この章では、Cisco 819 サービス統合型ルータ（ISR）上に組み込まれているワイヤレス アクセス ポイントに対してサービスを提供する、4 ポート ファスト イーサネット（FE）スイッチと、ギガビット イーサネット（GE）スイッチの設定作業の概要について説明します。

FE スイッチは、10/100Base T レイヤ 2 ファスト イーサネット スイッチです。スイッチ上の異なる VLAN の間のトラフィックは、スイッチ仮想インターフェイス（SVI）を使用し、ルータ プラットフォームを通じてルーティングされます。

GE スイッチは、ルータと組み込みワイヤレス アクセス ポイントの間の内部インターフェイスを備えた 1000Base T レイヤ 2 ギガビット イーサネット スイッチです。

どのスイッチ ポートも、他のシスコ イーサネット スイッチに接続するためのトランキング ポートとして設定できます。

この章の内容は、次のとおりです。

スイッチ ポートの番号付けと命名

FE スイッチ上のポートには、番号 FE0 ～ FE3 が付与されています。GE スイッチ上のポートには、Wlan-GigabitEthernet0 という名前と番号が付けられています。

FE スイッチの制限事項

FE スイッチには次の制限事項があります。

- FE スイッチのポートを、ルータのファスト イーサネット オンボード ポートに接続してはなりません。
- Cisco 819 ISR では、インライン パワーはサポートされていません。
- VTP プルーニングはサポートされません。
- FE スイッチは、最大 200 個の安全な MAC アドレスをサポートできます。

イーサネット スイッチについて

イーサネット スイッチを設定するには、次の概念について理解しておく必要があります。

VLAN および VLAN トランク プロトコル

VLAN および VLAN トランク プロトコル（VTP）の概念については、「*VLANs*」を参照してください。

レイヤ 2 イーサネット スイッチング

レイヤ 2 イーサネット スイッチングの概念については、「*Layer 2 Ethernet Switching*」を参照してください。

802.1X 認証

802.1x 認証の概念については、「*802.1x Authentication*」を参照してください。

スパニングツリー プロトコル

スパニングツリー プロトコルの概念については、「*Using the Spanning Tree Protocol with the Cisco EtherSwitch Network Module*」を参照してください。

Cisco Discovery Protocol

Cisco Discovery Protocol（CDP）は、シスコ製のすべてのルータ、ブリッジ、アクセス サーバ、スイッチで、レイヤ 2（データリンク層）上で動作します。CDP を使用することにより、ネットワーク管理アプリケーションで、既知装置のネイバーであるシスコ製の装置、特に下位レイヤのトランスペアレント プロトコルを実行しているネイバーを検索することができます。ネットワーク管理アプリケーションは CDP によって、近接装置の装置タイプおよび SNMP エージェント アドレスを学習できます。この機能によって、アプリケーションからネイバー デバイスに SNMP クエリーを送信できます。

CDP は、サブネットワーク アクセス プロトコル（SNAP）をサポートしているすべての LAN および WAN メディア上で動作します。CDP を設定した各デバイスは、マルチキャスト アドレスに対して定期的にメッセージを送信します。各デバイスは、SNMP メッセージを受信できるアドレスを少なくとも 1 つアドバタイズします。アドバタイズには、存続可能時間（ホールドタイム情報）も含まれています。これは、受信側の装置が CDP 情報を破棄せずに保持する時間の長さを示します。

スイッチド ポート アナライザ

スイッチド ポート アナライザの概念については、「*Switched Port Analyzer*」を参照してください。

IGMP スヌーピング

IGMP スヌーピングの概念については、「*IGMP Snooping*」を参照してください。

IGMP バージョン 3

Cisco 819 ISR は、IGMP スヌーピングのバージョン 3 をサポートしています。

IGMPv3 は、発信元フィルタリングをサポートしています。これを使用すると、マルチキャスト レシーバ ホストは、マルチキャスト トラフィックの受信元のグループと、どの発信元からのトラフィックを待っているかをルータに知らせることができます。Cisco ISR 上で IGMP スヌーピングとともに IGMPv3 機能を有効にすることで、Basic IGMPv3 Snooping Support（BISS）が提供されます。BISS では、IGMPv3 ホストの存在の下で、マルチキャスト トラフィックの制約されたフラッディングが可能になります。このサポートは、トラフィックを、IGMPv2 スヌーピングが IGMPv2 ホストで行うのとほぼ同じポート セットに制約します。制約されたフラッディングでは、宛先マルチキャスト アドレスだけが考慮されます。

ストーム制御

ストーム制御の概念については、「*Storm Control*」を参照してください。

フォールバック ブリッジング

フォールバック ブリッジングの概念については、「*Fallback Bridging*」を参照してください。

SNMP MIB の概要

簡易ネットワーク管理プロトコル（SNMP）の開発と使用は、管理情報ベース（MIB）周辺で一元化されます。SNMP MIB は抽象的なデータベースで、管理アプリケーションが特定の形式で読み取りおよび変更できる、情報の概念的な仕様です。これは、情報が同じ形式で管理対象システムに保持されているという意味は含まれません。SNMP エージェントでは、管理対象システムの内部データ構造と形式、および MIB 用に定義された外部データ構造と形式の間で変換が行われます。

SNMP MIB は、概念的には、概念上のテーブルを使用するツリー構造です。シスコのレイヤ 2 スイッチング インターフェイス MIB については、次の項で詳しく説明します。このツリー構造に対して、MIB という用語は 2 つの意味で使用されます。1 つ目の意味では、実際に MIB ブランチであり、通常、伝送メディアまたはルーティング プロトコルなどのテクノロジーの 1 つの側面に関する情報を含みます。この意味で使用される MIB は、正確には MIB モジュールと呼ばれ、通常は 1 つのドキュメントで

定義されます。もう 1 つの意味では、MIB はこのようなブランチの集合です。このような集合体は、たとえば、該当のエージェントによって実装されたすべての MIB モジュール、または、SNMP で定義された MIB モジュールの全体の集まりで構成されます。

MIB は、オブジェクトと呼ばれる、データの個々の項目に分岐されるツリーです。オブジェクトは、たとえば、カウンターまたはプロトコルのステータスです。MIB オブジェクトも、変数と呼ばれることがあります。

Cisco 819 4 G LTE ルータでサポートされる MIB の一覧については、『*Configuring Cisco 4G LTE Wireless WAN EHWIC*』の「SNMP MIBs」の項を参照してください。

MIB は、IOS Release 15.2(4)M1 で Cisco 819HGW および Cisco 819HWD SKU をサポートするように変更されました。表 10-1 に、Cisco 819 ISR の MIB を示します。

表 10-1　Cisco 819 ISR の MIB

MIB	MIB のリンク
CISCO-PRODUCTS-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://tools.cisco.com/ITDIT/MIBS/servlet/index
CISCO-ENTITY-VENDORTYPE-OID-MIB	
OLD-CISCO-CHASSIS-MIB	
CISCO-WAN-3G-MIB	

レイヤ 2 イーサネット スイッチングの BRIDGE-MIB

レイヤ 2 イーサネット スイッチング インターフェイス BRIDGE-MIB は Cisco 819 プラットフォームでサポートされます。BRIDGE-MIB により、ユーザはイーサネット スイッチ モジュールのメディア アクセス コントロール（MAC）アドレスとスパニングツリー情報を把握することができます。ユーザは、SNMP プロトコルを使用して MIB エージェントを照会し、MAC アドレスなどのイーサネット スイッチ モジュールの詳細や、各インターフェイスおよびスパニング プロトコル情報に関する詳細を取得できます。

ブリッジ MIB は L2 レイヤ BRIDGE-MIB 情報を取得するために次のアプローチを使用します。

- コミュニティ ストリングに基づくアプローチ
- コンテキストに基づくアプローチ

コミュニティ ストリングに基づくアプローチでは、VLAN ごとに、1 個のコミュニティ ストリングが作成されます。クエリに基づいて、各 VLAN MIB が表示されます。

BRIDGE-MIB の詳細情報を取得するには、コンフィギュレーション モードで **snmp-server community public RW** コマンドを使用します。

```
Router(config)#snmp-server community public RW
```

SNMP BRIDGE-MIB の詳細をクエリするには、次の構文を使用します。

```
snmpwalk -v2c <ip address of the ISR, …>  public .1.3.6.1.2.1.17
snmpwalk -v2c <ip address of the ISR, …>  public@2 .1.3.6.1.2.1.17
snmpwalk -v2c <ip address of the ISR, …>  public@3 .1.3.6.1.2.1.17
```

（注）　VLAN「x」を作成すると、論理エンティティ public@x が追加されます。パブリック コミュニティについてクエリを実行すると、L3 MIB が表示されます。public@x についてクエリを実行すると、VLAN「x」の L2 MIB が表示されます。

コンテキストに基づくアプローチでは、L2 インターフェイスの値を表示するために、SNMP コンテキスト マッピング コマンド使用されます。各 VLAN はコンテキストにマッピングされます。ユーザがコンテキストを使用してクエリを実行すると、MIB は、コンテキストにマッピングされた特定の VLAN のデータを表示します。このアプローチでは、各 VLAN はコンテキストに手動でマッピングされます。

BRIDGE-MIB の詳細情報を取得するには、コンフィギュレーション モードで次のコマンドを使用します。

```
Router(config)#Routersnmp-server group public v2c context bridge-group
Router(config)#snmp-server community public RW
Router(config)#snmp-server community private RW
Router(config)#snmp-server context bridge-group
Router(config)#snmp mib community-map public context bridge-group
```

SNMP BRIDGE-MIB の詳細をクエリするには、次の構文を使用します。

```
snmpwalk -v2c <ip address of the ISR, …>  public@1 .1.3.6.1.2.1.17 ?L2-MIB
snmpwalk -v2c <ip address of the ISR, …>  private .1.3.6.1.2.1.17?L3-MIB
```

（注）　パブリック コミュニティについてクエリを実行すると、L2 MIB が表示されます。L3 MIB のプライベート グループを使用します。

BRIDGE-MIB の詳細を設定および取得する方法の詳細については、「*The BRIDGE-MIB*」を参照してください。

MAC アドレス通知

MAC アドレス通知は、スイッチに MAC アドレス アクティビティを保存することでネットワーク上のユーザを追跡できます。スイッチが MAC アドレスを学習または削除すると常に、SNMP 通知を生成して NMS に送信させることができます。ネットワークから多数のユーザの出入りがある場合は、トラップ インターバル タイムを設定して通知トラップを組み込み、ネットワーク トラフィックを削減できます。MAC 通知履歴テーブルは、トラップがイネーブルに設定されたハードウェアのポートごとの MAC アドレス アクティビティを保存します。MAC アドレス通知は、動的でセキュアな MAC アドレスについて生成されます。自己アドレス、マルチキャスト アドレス、またはその他のスタティック アドレスについては、イベントは生成されません。

MAC アドレス通知の設定については、「*Configuring MAC Address Notification Traps*」を参照してください。

イーサネット スイッチの設定方法

イーサネット スイッチの設定作業については、以降のセクションを参照してください。

VLAN の設定

ここでは、VLAN の設定方法について説明します。Cisco 819 ISR は 2 個の VLAN をサポートし、Cisco 819 ISR は 8 個の VLAN をサポートします。

FE ポート上の VLAN

VLAN を設定するには、コンフィギュレーション モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**interface fe** *port*	設定対象のファスト イーサネット ポートを選択します。
ステップ 2	**shutdown**	（任意）設定が完了するまでトラフィック フローを防止するために、インターフェイスをシャットダウンします。

	コマンド	目的
ステップ 3	**switchport**	ファスト イーサネット ポートでレイヤ 2 スイッチングを設定します。 **（注）** ファスト イーサネット ポートをレイヤ 2 ポートとして設定するには、**switchport** コマンドをキーワードなしで実行してから、他のキーワード付きの switchport コマンドを実行する必要があります。このコマンドは、シスコ デフォルト VLAN を作成します。 この設定は、デフォルトのトランキング管理モードを **switchport mode dynamic desirable** に設定し、トランク カプセル化を **negotiate** に設定します。 デフォルトでは、作成されるすべての VLAN がデフォルト トランクに追加されます。
ステップ 4	**switchport access vlan** *vlan_id*	追加の VLAN のインスタンスを作成します。*vlan_id* に指定できる値の範囲は 2 ～ 4094 ですが、値 1002 と 1005 は予約されています。
ステップ 5	**no shutdown**	インターフェイスをアクティブにします
ステップ 6	**end**	コンフィギュレーション モードを終了します。

追加情報については、「*Layer 2 LAN Ports*」を参照してください。

GE ポート上の VLAN

GE ポートはルータの組み込みアクセス ポイントだけにサービスを提供する内部インターフェイスであるため、X に 1 以外を指定した **switchport access vlan X** コマンドだけでは設定できません。ただし、トランク モードで設定することはできます。そのためには、コンフィギュレーション モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**interface** *Wlan-GigabitEthernet0*	設定対象のギガビット イーサネット ポートを選択します。
ステップ 2	**switchport mode trunk**	ポートをトランク モードにします。
ステップ 3	**switchport access vlan** *vlan_id*	（任意）ポートがトランク モードになったら、1 以外の VLAN 番号を割り当てることができます。

レイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスの設定方法については、「*Configuring Layer 2 Interfaces*」を参照してください。

ここでは、次のトピックについて説明します。

- Configuring a range of interfaces
- Defining a range macro
- Configuring Layer 2 optional interface features

802.1x 認証の設定

802.1x ポートベース認証の設定方法については、「*Configuring IEEE 802.1x Port-Based Authentication*」を参照してください。

ここでは、次のトピックについて説明します。

- Understanding the default 802.1x configuration
- Enabling 802.1x Authentication
- Configuring the switch-to-RADIUS-server comunication
- Enabling periodic reauthentication
- Changing the quiet period
- Changing the switch-to-client retransmission time
- Setting the switch-to-client frame-retransmission number
- Enabling multiple hosts
- Resetting the 802.1x configuration to default values
- Displaying 802.1x statistics and status

スパニングツリー プロトコルの設定

スパニングツリー プロトコルの設定方法については、「*Configuring Spanning Tree*」を参照してください。

ここでは、次のトピックについて説明します。

- Enabling spanning tree
- Configuring spanning tree port priority
- Configuring spanning tree port cost
- Configuring the bridge priority of a VLAN
- Configuring the Hello Time
- Configuring the forward-delay time for a VLAN
- Configuring the maximum aging time for a VLAN
- Disabling spanning tree

MAC テーブルの操作の設定

MAC テーブルの操作の設定方法については、「*Configuring MAC Table Manipulation*」を参照してください。

ポート セキュリティ

既知の MAC アドレス トラフィックのイネーブル化に関するトピックでは、ポート セキュリティを扱います。ポート セキュリティには、スタティックなポート セキュリティとダイナミックなポート セキュリティがあります。

スタティックなポート セキュリティでは、指定したスイッチ ポートを通じてアクセスすることを許可する装置を、ユーザが指定できます。指定は、許可する装置の MAC アドレスを MAC アドレス テーブルに格納することで、手動で行います。スタティックなポート セキュリティは、MAC アドレス フィルタリングとも呼ばれます。

ダイナミックなポート セキュリティもこれに似ています。ただし、装置の MAC アドレスを指定する代わりに、ポート上で許可する装置の最大数を指定します。指定した最大数が手動で指定した MAC アドレスの数よりも大きい場合、スイッチは、指定された最大値になるまで、MAC アドレスを自動的に学習します。指定した最大数がスタティックに指定されている MAC アドレスの数よりも小さい場合は、エラー メッセージが生成されます。

スタティックまたはダイナミックなポート セキュリティを指定するには、次のコマンドを使用します。

コマンド	目的
`Router(config)# mac-address-table secure [<mac-address> | maximum maximum addresses] fastethernet interface-id [vlan <vlan id>]`	*<mac-address>* を指定すると、スタティックなポート セキュリティがイネーブルになります。キーワード **maximum** を使用すると、ダイナミックなポート セキュリティがイネーブルになります。

Cisco Discovery Protocol の設定

Cisco Discovery Protocol（CDP）を設定する方法については、「*Configuring Cisco Discovery Protocol*」を参照してください。

ここでは、次のトピックについて説明します。

- Enabling CDP
- Enabling CDP on an interface
- Monitoring and maintaining CDP

スイッチド ポート アナライザ（SPAN）の設定

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、「*Configuring the Switched Port Analyzer (SPAN)*」を参照してください。

ここでは、次のトピックについて説明します。

- Configuring the SPAN sources
- Configuring SPAN destinations
- Verifying the SPAN session
- Removing sources or destinations from a SPAN session

IP マルチキャスト レイヤ 3 スイッチングの設定

IP マルチキャスト レイヤ 3 スイッチングの設定方法については、「*Configuring IP Multicast Layer 3 Switching*」を参照してください。

ここでは、次のトピックについて説明します。

- Enabling IP multicast routing globally
- Enabling IP protocol-independent multicast (PIM) on Layer 3 interfaces
- Verifying IP multicast Layer 3 hardware switching summary
- Verifying the IP multicast routing table

IGMP スヌーピングの設定

IGMP スヌーピングの設定方法については、「*Configuring IGMP Snooping*」を参照してください。

ここでは、次のトピックについて説明します。

- Enabling or disabling IGMP snooping
- Enabling IGMP immediate-leave processing
- Statically configuring an interface to join a group
- Configuring a multicast router port

IGMP バージョン 3

Cisco IOS Release 12.4(15)T で IGMPv3 機能をサポートするため、キーワード **groups** および **count** が **show ip igmp snooping** コマンドに追加されました。また、**show ip igmp snooping** コマンドの出力に、IGMP スヌーピング グループに関するグローバル情報が含まれるように変更されました。**show ip igmp snooping** コマンドを **groups** キーワードとともに使用すると、すべての VLAN に対して IGMP スヌーピングによって学習されたマルチキャスト テーブルが表示されます。また、**show ip igmp snooping** コマンドを、**groups** キーワード、**vlan-id** キーワード、*vlan-id* 引数とともに使用すると、特定の VLAN に対して IGMP スヌーピングによって学習されたマルチキャスト テーブルが表示されます。**show ip igmp snooping** コマンドを **groups** キーワードおよび **count** キーワードとともに使用すると、IGMP スヌーピングによって学習されたマルチキャスト グループの数が表示されます。

ポート単位のストーム制御の設定

ポート単位のストーム制御の設定方法については、「*Configuring Per-Port Storm-Control*」を参照してください。

ここでは、次のトピックについて説明します。

- Enabling per-port storm-control
- Disabling per-port storm-control

フォールバック ブリッジングの設定

フォールバック ブリッジングの設定方法については、「*Configuring Fallback Bridging*」を参照してください。

ここでは、次のトピックについて説明します。

- Understanding the default fallback bridging configuration
- Creating a bridge group
- Preventing the forwarding of dynamically learned stations
- Configuring the bridge table aging time
- Filtering frames by a specific MAC address
- Adjusting spanning-tree parameters
- Monitoring and maintaining the network

スイッチの管理

スイッチの管理については、「*Managing the EtherSwitch HWIC*」を参照してください。

ここでは、次のトピックについて説明します。

- Adding Trap Managers
- Configuring IP Information
- Enabling Switch Port Analyzer
- Managing the ARP Table
- Managing the MAC Address Tables
- Removing Dynamic Addresses
- Adding Secure Addresses
- Configuring Static Addresses
- Clearing all MAC Address Tables