CHAPTER 4

# Cisco ASA 5505 適応型セキュリティ アプライアンス用スイッチ ポートおよび VLAN インターフェイスの設定

この章では、ASA 5505 適応型セキュリティ アプライアンスのスイッチ ポートと VLAN インターフェイスを設定する方法について説明します。

（注） 他のモデルのインターフェイスを設定するには、第 5 章「イーサネット設定およびサブインターフェイスの設定」および第 7 章「インターフェイス パラメータの設定」を参照してください。

この章は、次の項で構成されています。



## インターフェイスの概要

この項では、ASA 5505 適応型セキュリティ アプライアンスのポートおよびインターフェイスについて説明します。次の項目を取り上げます。

# ASA 5505 のポートおよびインターフェイスについて

ASA 5505 適応型セキュリティ アプライアンスでは、組み込みスイッチがサポートされています。次の 2 種類のポートおよびインターフェイスを設定する必要があります。

- 物理スイッチ ポート：適応型セキュリティ アプライアンスには、ハードウェアのスイッチング機能を使用して、レイヤ 2 でトラフィックを転送する 8 つのファスト イーサネット スイッチ ポートがあります。これらのポートのうちの 2 つは PoE ポートです。詳細については、「Power Over Ethernet」（P.4-4）を参照してください。これらのインターフェイスを、PC、IP 電話、DSL モデムなどのユーザ機器に直接接続できます。または、別のスイッチに接続できます。
- 論理 VLAN インターフェイス：ルーテッド モードでは、これらのインターフェイスは、設定済みのセキュリティ ポリシーを使用してファイアウォールと VPN サービスを適用することによって、レイヤ 3 の VLAN ネットワーク間でトラフィックを転送します。トランスペアレント モードでは、これらのインターフェイスは、設定済みのセキュリティ ポリシーを使用してファイアウォール サービスを適用することによって、レイヤ 2 の同じネットワーク上の VLAN 間でトラフィックを転送します。最大 VLAN インターフェイス数の詳細については、「ライセンスで使用できる最大アクティブ VLAN インターフェイス数」を参照してください。VLAN インターフェイスを使用することにより、別々の VLAN、たとえばホーム VLAN、ビジネス VLAN、インターネット VLAN などに装置を分けることができます。

スイッチ ポートを別々の VLAN に分離するには、各スイッチ ポートを VLAN インターフェイスに割り当てます。同じ VLAN 上のスイッチ ポートは、ハードウェア スイッチングを使用して相互に通信できます。ただし、VLAN 1 上のスイッチ ポートが VLAN 2 上のスイッチ ポートと通信する場合、適応型セキュリティ アプライアンスはセキュリティ ポリシーをトラフィックに適用し、2 つの VLAN 間でルーティングまたはブリッジングします。

（注）　サブインターフェイスは、ASA 5505 適応型セキュリティ アプライアンスでは使用できません。

# ライセンスで使用できる最大アクティブ VLAN インターフェイス数

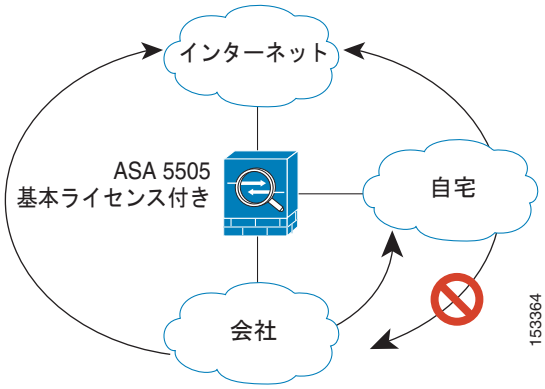
トランスペアレント ファイアウォール モードでは、基本ライセンスはアクティブ VLAN を 2 つ、Security Plus ライセンスは 3 つ設定できます。そのうちの 1 つは、フェールオーバー用です。

ルーテッド モードでは、基本ライセンスはアクティブ VLAN を 3 つまで、Security Plus ライセンスは 20 まで設定できます。

アクティブな VLAN とは、**nameif** コマンドが設定された VLAN のことです。

基本ライセンスの場合、3 つめの VLAN は他の 1 つの VLAN にのみトラフィックを開始するように設定できます。図 4-1 のネットワークの例では、ホーム VLAN はインターネットと通信できますが、ビジネス VLAN とは接続を開始できません。

**図 4-1　基本ライセンスでの ASA 5505 適応型セキュリティ アプライアンス**

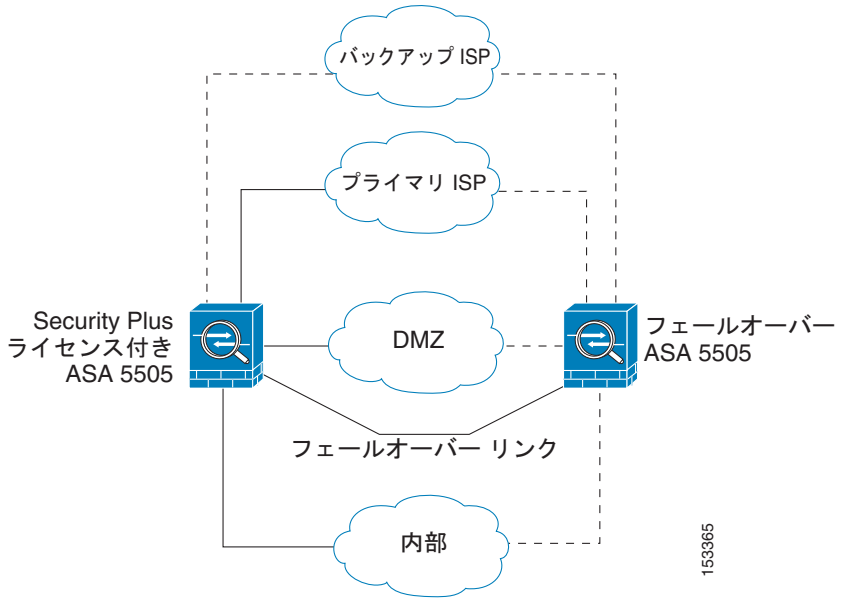



Security Plus ライセンスでは、20 の VLAN インターフェイスを設定できます。トランク ポートを設定して、1 つのポートで複数の VLAN を使用できます。

**（注）** ASA 5505 適応型セキュリティ アプライアンスは、アクティブ / スタンバイ フェールオーバーをサポートしますが、ステートフル フェールオーバーをサポートしていません。

ネットワークの例については、図 4-2 を参照してください。

**図 4-2　Security Plus ライセンスでの ASA 5505 適応型セキュリティ アプライアンス**



# デフォルト インターフェイス コンフィギュレーション

ご使用の適応型セキュリティ アプライアンスに工場出荷時のデフォルト コンフィギュレーションが含まれている場合、インターフェイスは次のように設定されています。

- 外部インターフェイス（セキュリティ レベル 0）は VLAN 2 です。

  イーサネット 0/0 が VLAN 2 に割り当てられ、イネーブルになります。

  VLAN 2 の IP アドレスは DHCP サーバから取得します。
- 内部インターフェイス（セキュリティ レベル 100）は VLAN 1 です。

  イーサネット 0/1 ～イーサネット 0/7 が VLAN 1 に割り当てられ、イネーブルになります。

  VLAN 1 の IP アドレスは 192.168.1.1 です。

**configure factory-default** コマンドを使用して、工場出荷時のデフォルト コンフィギュレーションを復元します。

この章の手順に従い、デフォルト コンフィギュレーションを変更します。たとえば、VLAN インターフェイスの追加を行います。

工場出荷時のデフォルト コンフィギュレーションになっていない場合は、すべてのスイッチ ポートが VLAN 1 ですが、その他のパラメータは未設定です。

# VLAN MAC アドレス

ルーテッド ファイアウォール モードでは、すべての VLAN インターフェイスが MAC アドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有の MAC アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。

トランスペアレント ファイアウォール モードでは、各 VLAN に固有の MAC アドレスがあります。必要に応じて、手動で MAC アドレスを割り当てて、生成された MAC アドレスを上書きできます。

# Power Over Ethernet

Ethernet 0/6 および Ethernet 0/7 は、IP 電話や無線アクセス ポイントなどのデバイス用に PoE をサポートしています。非 PoE デバイスをインストールした場合やこれらのスイッチ ポートに接続しない場合、適応型セキュリティ アプライアンスはスイッチ ポートに電源を供給しません。

**shutdown** コマンドを使用してスイッチ ポートをシャットダウンすると、デバイスへの電源がディセーブルになります。**no shutdown** を入力すると、電源が復元します。スイッチ ポートのシャットダウンの詳細については、「アクセス ポートとしてのスイッチ ポートの設定」（P.4-9）を参照してください。

接続されているデバイスのタイプ（Cisco または IEEE 802.3af）など、PoE スイッチ ポートのステータスを確認するには、**show power inline** コマンドを使用します。

# SPAN を使用したトラフィックのモニタリング

1 つまたは複数のスイッチ ポートを出入りするトラフィックをモニタするには、スイッチ ポート モニタリングとも呼ばれる SPAN をイネーブルにします。SPAN をイネーブルにしたポート（宛先ポートと呼ばれる）は、特定の送信元ポートで送受信するすべてのパケットのコピーを受信します。SPAN 機能を使用すれば、スニファを宛先ポートに添付して、すべてのトラフィックをモニタできます。SPAN を使用しないと、モニタするポートごとにスニファを添付しなければなりません。SPAN をイネーブルにすることができるのは、1 つの宛先ポートのみです。

詳細については、『*Cisco Security Appliance Command Reference*』の **switchport monitor** コマンドを参照してください。

# セキュリティ レベルの概要

各 VLAN インターフェイスには、0 ～ 100（最下位～最上位）までのセキュリティ レベルを割り当てる必要があります。たとえば、内部ビジネス ネットワークなど、最もセキュアなネットワークにはレベル 100 を割り当てる必要があります。一方、インターネットなどに接続する外部ネットワークにはレベル 0 が割り当てられる場合があります。ホーム ネットワークなどその他のネットワークはその中間に設定できます。複数のインターフェイスを同じセキュリティ レベルに割り当てることができます。

レベルによって、次の動作が制御されます。

- ネットワーク アクセス：デフォルトで、高いセキュリティ レベルのインターフェイスから低いセキュリティ レベルのインターフェイスへの通信（発信）は暗黙的に許可されます。高いセキュリティ レベルのインターフェイス上のホストは、低いセキュリティ レベルのインターフェイス上の任意のホストにアクセスできます。インターフェイスにアクセス リストを適用することによって、アクセスを制限できます。
- 同じセキュリティ レベルのインターフェイスの通信をイネーブルにすると、同じセキュリティ レベルまたはそれより低いセキュリティ レベルの他のインターフェイスにアクセスするインターフェイスは、暗黙的に許可されます。詳細については、「同一セキュリティ レベルにある VLAN インターフェイス間の通信の許可」（P.4-14）を参照してください。
- インスペクション エンジン：一部のアプリケーション インスペクション エンジンはセキュリティ レベルに依存します。同じセキュリティ レベルのインターフェイス間では、インスペクション エンジンは発信と着信のいずれのトラフィックに対しても適用されます。
  - NetBIOS インスペクション エンジン：発信接続に対してのみ適用されます。
  - SQL*Net インスペクション エンジン：SQL*Net（旧称 OraServ）ポートとの制御接続が一対のホスト間に存在する場合、着信データ接続だけが適応型セキュリティ アプライアンスを通過することを許可されます。
- フィルタリング：HTTP(S) および FTP フィルタリングは、（高いレベルから低いレベルへの）発信接続にのみ適用されます。

  同じセキュリティ レベルのインターフェイス間では、発信と着信のいずれのトラフィックもフィルタリングできます。
- NAT コントロール：NAT コントロールをイネーブルにする場合、高いセキュリティ レベルのインターフェイス（内部）上のホストから低いセキュリティ レベルのインターフェイス（外部）上のホストにアクセスするときは、内部インターフェイスのホストに NAT を設定する必要があります。

  NAT コントロールをイネーブルにしない場合、または同じセキュリティ レベルのインターフェイス間においては、任意のインターフェイス間で NAT を使用することも、使用しないこともできます。外部インターフェイスに NAT を設定する場合は、特別なキーワードが必要になることがあります。
- **established** コマンド：このコマンドを使用すると、高位レベルのホストから低位レベルのホストに接続がすでに確立されている場合に、低位のセキュリティのホストから高位のセキュリティのホストへのリターン接続が許可されます。

  同じセキュリティ レベルのインターフェイス間では、発信と着信の両方の接続に対して **established** コマンドを設定できます。

# VLAN インターフェイスの設定

トラフィックが各 VLAN を通過できるようにするには、インターフェイス名を設定する必要があります（**nameif** コマンド）。ルーテッド モードの場合は IP アドレスを設定します。また、セキュリティ レベルをデフォルトの 0 から変更する必要があります。インターフェイス名を「inside」にし、セキュリティ レベルを明示的に設定しない場合は、適応型セキュリティ アプライアンスによってセキュリティ レベルが 100 に設定されます。

設定可能な VLAN 数については、「ライセンスで使用できる最大アクティブ VLAN インターフェイス数」（P.4-2）を参照してください。

**（注）** フェールオーバーを使用している場合、フェールオーバー通信に予約されているインターフェイスには、この方法で名前を付けないでください。フェールオーバー リンクを設定するには、第 14 章「フェールオーバーの設定」を参照してください。

インターフェイスのセキュリティ レベルを変更したときに、既存の接続がタイムアウトするまで待機せずに新しいセキュリティ情報を使用する必要がある場合は、**clear local-host** コマンドを使用して接続をクリアできます。

VLAN インターフェイスを設定するには、次の手順を実行します。

**ステップ 1**　VLAN ID を指定するには、次のコマンドを入力します。

```
hostname(config)# interface vlan number
```

*number* には、1 ～ 4090 を指定します。

たとえば、次のコマンドを入力します。

```
hostname(config)# interface vlan 100
```

この VLAN インターフェイスとすべての関連コンフィギュレーションを削除するには、**no interface vlan** コマンドを入力します。このインターフェイスには、インターフェイス名コンフィギュレーションも含まれており、名前は他のコマンドでも使用されているため、それらのコマンドも削除されます。

**ステップ 2**　（任意）基本ライセンスでは、次のコマンドを使用して、このインターフェイスに対して別の VLAN への接続開始を制限することにより、このインターフェイスを 3 つ目の VLAN として使用できます。

```
hostname(config-if)# no forward interface vlan number
```

*number* には、この VLAN インターフェイスからトラフィックを開始できない VLAN ID を指定します。

基本ライセンスでは、このコマンドを使用して制限した場合だけ、3 つ目の VLAN を設定できます。

たとえば、1 つの VLAN をインターネット アクセスの外部に、もう 1 つを内部ビジネス ネットワーク内に、そして 3 つ目をホーム ネットワークにそれぞれ割り当てます。ホーム ネットワークはビジネス ネットワークにアクセスする必要がないので、ホーム VLAN で **no forward interface** コマンドを使用できます。ビジネス ネットワークはホーム ネットワークにアクセスできますが、その反対はできません。

**nameif** コマンドで 2 つの VLAN インターフェイスをすでに設定している場合、3 つ目のインターフェイスに対して **nameif** コマンドを使用する前に **no forward interface** コマンドを入力してください。ASA 5505 適応型セキュリティ アプライアンスの基本ライセンスでは、3 つの VLAN インターフェイスがフル機能を持つことは許可されていません。

**（注）** Security Plus ライセンスにアップグレードすれば、このコマンドを削除して、このインターフェイスのフル機能を取得することができます。このコマンドを設定したままにすると、アップグレード後もインターフェイスの制限はそのまま残ります。

**ステップ 3**　インターフェイスに名前を付けるには、次のコマンドを入力します。

```
hostname(config-if)# nameif name
```

*name* は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

**ステップ 4**　セキュリティ レベルを設定するには、次のコマンドを入力します。

```
hostname(config-if)# security-level number
```

*number* には、0（最下位）～ 100（最上位）の整数を指定します。

**ステップ 5**　（ルーテッド モードだけ）IP アドレスを設定するには、次のコマンドのいずれかを入力します。

**（注）** IPv6 アドレスの設定については、「インターフェイスでの IPv6 の設定」（P.12-3）を参照してください。

トランスペアレント ファイアウォール モードの管理 IP アドレスを設定する方法については、「透過ファイアウォールの管理 IP アドレスの設定」（P.8-5）を参照してください。トランスペアレント モードでは、インターフェイスごとに IP アドレスを設定せずに、適応型セキュリティ アプライアンス全体またはコンテキスト全体に設定します。

フェールオーバーの場合、IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP および PPPoE はサポートされません。

- IP アドレスを手動で設定するには、次のコマンドを入力します。

  ```
  hostname(config-if)# ip address ip_address [mask] [standby ip_address]
  ```

  フェールオーバーには、**standby** キーワードとアドレスを使用します。詳細については、第 14 章「フェールオーバーの設定」を参照してください。

- DHCP サーバから IP アドレスを取得するには、次のコマンドを入力します。

  ```
  hostname(config-if)# ip address dhcp [setroute]
  ```

  DHCP リースをリセットし、新規リースを要求するには、このコマンドを再入力します。

  **ip address dhcp** コマンドを入力する前に、**no shutdown** コマンドを使用してインターフェイスをイネーブルにしなかった場合、DHCP 要求が送信されないことがあります。

- PPPoE サーバからの IP アドレスの取得については、第 35 章「PPPoE クライアントの設定」を参照してください。

**ステップ 6**　（任意）プライベート MAC アドレスをこのインターフェイスに割り当てるには、次のコマンドを入力します。

```
hostname(config-if)# mac-address mac_address [standby mac_address]
```

ルーテッド モードではデフォルトで、すべての VLAN が同じ MAC アドレスを使用します。トランスペアレント モードでは、VLAN は固有の MAC アドレスを使用します。スイッチに必要な場合、またはアクセス コントロールの目的で、固有の VLAN を設定したり、生成された VLAN を変更したりすることができます。

**ステップ 7**　（任意）インターフェイスを管理専用モードに設定してトラフィックが通過できないようにするには、次のコマンドを入力します。

```
hostname(config-if)# management-only
```

**ステップ 8**　デフォルトで、VLAN インターフェイスはイネーブルになっています。インターフェイスをイネーブルにするには、次のコマンドを入力します（インターフェイスがまだイネーブルになっていない場合）。

```
hostname(config-if)# no shutdown
```

インターフェイスをディセーブルにするには、**shutdown** コマンドを入力します。

---

次の例では 7 つの VLAN インターフェイスを設定しています。これには、**failover lan** コマンドを使用して別々に設定されるフェールオーバー インターフェイスも含まれます。

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 201
hostname(config-if)# nameif dept1
hostname(config-if)# security-level 90
hostname(config-if)# ip address 10.2.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 202
hostname(config-if)# nameif dept2
hostname(config-if)# security-level 90
hostname(config-if)# ip address 10.2.3.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# nameif dmz
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.3.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 400
hostname(config-if)# nameif backup-isp
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# failover lan faillink vlan500
hostname(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0
```

次の例では、基本ライセンスの 3 つの VLAN インターフェイスを設定しています。3 つ目の home インターフェイスは、トラフィックを business インターフェイスに転送できません。

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address dhcp
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif business
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# no forward interface vlan 200
hostname(config-if)# nameif home
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

# アクセス ポートとしてのスイッチ ポートの設定

デフォルトでは、スイッチ ポートはすべてシャットダウンされます。1 つの VLAN にスイッチ ポートを割り当てるには、アクセス ポートとして設定します。複数の VLAN を伝送するトランク ポートを作成するには、「トランク ポートとしてのスイッチ ポートの設定」（P.4-11）を参照してください。

デフォルトでは、スイッチ ポートの速度と二重通信はオートネゴシエーションに設定されています。デフォルトのオートネゴシエーション設定には Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスに対して Auto-MDI/MDIX を無効にできません。

**注意**　ASA 5505 適応型セキュリティ アプライアンスは、ネットワーク内のループ検出用のスパニングツリー プロトコルをサポートしていません。したがって、セキュリティ アプライアンスとのすべての接続は、ネットワーク ループ内で終わらないようにする必要があります。

スイッチ ポートを設定するには、次の手順を実行します。

**ステップ 1**　設定するスイッチ ポートを指定するには、次のコマンドを入力します。

```
hostname(config)# interface ethernet0/port
```

*port* には、0 ～ 7 を指定します。たとえば、次のコマンドを入力します。

```
hostname(config)# interface ethernet0/1
```

**ステップ 2**　VLAN にスイッチ ポートを割り当てるには、次のコマンドを入力します。

```
hostname(config-if)# switchport access vlan number
```

*number* には、VLAN ID を 1 ～ 4090 で指定します。

（注）　インターネット アクセス デバイスにレイヤ 2 冗長性が含まれている場合は、複数のスイッチ ポートをプライマリ VLAN またはバックアップ VLAN に割り当てることができます。

**ステップ 3**　（任意）スイッチ ポートが他の保護されたスイッチ ポートと同じ VLAN 上で通信しないようにするには、次のコマンドを入力します。

```
hostname(config-if)# switchport protected
```

スイッチ ポート間で相互通信するのを防ぐのは、スイッチ ポート上のデバイスが主に他の VLAN からアクセスされ、VLAN 内のアクセスを許可する必要がなく、感染やセキュリティ違反が発生した際に、個々のデバイスを相互に孤立させる場合です。たとえば、3 つの Web サーバをホストする DMZ がある場合、各スイッチ ポートに **switchport protected** コマンドを適用すると、Web サーバを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバすべてと通信でき、その逆も可能ですが、Web サーバは相互に通信できません。

**ステップ 4**　（任意）速度を設定するには、次のコマンドを入力します。

```
hostname(config-if)# speed {auto | 10 | 100}
```

**auto** 設定がデフォルトです。PoE ポート Ethernet 0/6 または 0/7 で速度を **auto** 以外に設定すると、IEEE 802.3af をサポートしていない Cisco IP Phone および Cisco ワイヤレス アクセス ポイントは検出されず、電源も供給されません。

**ステップ 5**　（任意）二重通信を設定するには、次のコマンドを入力します。

```
hostname(config-if)# duplex {auto | full | half}
```

**auto** 設定がデフォルトです。PoE ポート Ethernet 0/6 または 0/7 で二重通信を **auto** 以外に設定すると、IEEE 802.3af をサポートしていない Cisco IP Phone および Cisco ワイヤレス アクセス ポイントは検出されず、電源も供給されません。

**ステップ 6**　スイッチ ポートがまだイネーブルになっていない場合、イネーブルにするには、次のコマンドを入力します。

```
hostname(config-if)# no shutdown
```

スイッチ ポートをディセーブルにするには、**shutdown** コマンドを入力します。

---

次の例では 5 つの VLAN インターフェイスを設定しています。これには、**failover lan** コマンドを使用して設定されるフェールオーバー インターフェイスも含まれます。

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# nameif dmz
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.3.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

```
hostname(config-if)# interface vlan 400
hostname(config-if)# nameif backup-isp
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# failover lan faillink vlan500
hostname(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0

hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 500
hostname(config-if)# no shutdown
```

# トランク ポートとしてのスイッチ ポートの設定

デフォルトでは、スイッチ ポートはすべてシャットダウンされます。この手順では、802.1Q タグ付けを使用して複数の VLAN を伝送するトランク ポートの作成方法について説明します。トランク モードが使用できるのは Security Plus ライセンスだけです。

インターフェイスが 1 つの VLAN にだけ割り当てられるアクセス ポートを作成するには、「アクセス ポートとしてのスイッチ ポートの設定」（P.4-9）を参照してください。

デフォルトでは、スイッチ ポートの速度と二重通信はオートネゴシエーションに設定されています。デフォルトのオートネゴシエーション設定には Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスに対して Auto-MDI/MDIX を無効にできません。

トランク ポートを設定するには、次の手順を実行します。

**ステップ 1**　設定するスイッチ ポートを指定するには、次のコマンドを入力します。

```
hostname(config)# interface ethernet0/port
```

*port* には、0 ～ 7 を指定します。たとえば、次のコマンドを入力します。

```
hostname(config)# interface ethernet0/1
```

**ステップ 2**　複数の VLAN をこのトランクに割り当てるには、次のコマンドを 1 つ以上入力します。

- ネイティブ VLAN を割り当てるには、次のコマンドを入力します。

  ```
  hostname(config-if)# switchport trunk native vlan vlan_id
  ```

*vlan_id* には、1 つの VLAN ID を 1 ～ 4090 で指定します。

ネイティブ VLAN 上のパケットは、トランク経由で送信されるときに変更されません。たとえば、ポートに VLAN 2、3、および 4 が割り当てられており、VLAN 2 がネイティブ VLAN である場合、ポートを出る VLAN 2 上のパケットは 802.1Q ヘッダーによって変更されません。このポートに入ってくるフレームは、802.1Q ヘッダーが付いていない場合は VLAN 2 に割り当てられます。

各ポートのネイティブ VLAN は 1 つのみですが、すべてのポートに同じネイティブ VLAN または異なるネイティブ VLAN を使用できます。

- VLAN を割り当てるには、次のコマンドを入力します。

```
hostname(config-if)# switchport trunk allowed vlan vlan_range
```

*vlan_range*（1 ～ 4090 の VLAN）は、次のいずれかの方法で指定できます。

単一の番号（n）

範囲（n-x）

番号および範囲は、カンマで区切ります。たとえば、次のように指定します。

5,7-10,13,45-100

カンマの代わりにスペースを入力できますが、コマンドはカンマ付きでコンフィギュレーションに保存されます。

このコマンドにネイティブ VLAN を含めることができますが、必須ではありません。ネイティブ VLAN は、このコマンドに含まれているかどうかに関係なく渡されます。

ネイティブまたは非ネイティブにかかわらず、少なくとも 1 つの VLAN が割り当てられないと、このスイッチ ポートはトラフィックを通過させることができません。

**ステップ 3**　このスイッチ ポートをトランク ポートにするには、次のコマンドを入力します。

```
hostname(config-if)# switchport mode trunk
```

このポートをアクセス モードに復元するには、**switchport mode access** コマンドを入力します。

**ステップ 4**　（任意）スイッチ ポートが他の保護されたスイッチ ポートと同じ VLAN 上で通信しないようにするには、次のコマンドを入力します。

```
hostname(config-if)# switchport protected
```

スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバをホストする DMZ がある場合、各スイッチ ポートに **switchport protected** コマンドを適用すると、Web サーバを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバすべてと通信でき、その逆も可能ですが、Web サーバは相互に通信できません。

**ステップ 5**　（任意）速度を設定するには、次のコマンドを入力します。

```
hostname(config-if)# speed {auto | 10 | 100}
```

**auto** 設定がデフォルトです。

**ステップ 6**　（任意）二重通信を設定するには、次のコマンドを入力します。

```
hostname(config-if)# duplex {auto | full | half}
```

**auto** 設定がデフォルトです。

**ステップ 7**　スイッチ ポートがまだイネーブルになっていない場合、イネーブルにするには、次のコマンドを入力します。

```
hostname(config-if)# no shutdown
```

スイッチ ポートをディセーブルにするには、**shutdown** コマンドを入力します。

---

次の例では 7 つの VLAN インターフェイスを設定しています。これには、**failover lan** コマンドを使用して設定されるフェールオーバー インターフェイスも含まれます。VLAN 200、201、および 202 は、イーサネット 0/1 でトランキングされています。

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 201
hostname(config-if)# nameif dept1
hostname(config-if)# security-level 90
hostname(config-if)# ip address 10.2.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 202
hostname(config-if)# nameif dept2
hostname(config-if)# security-level 90
hostname(config-if)# ip address 10.2.3.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# nameif dmz
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.3.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 400
hostname(config-if)# nameif backup-isp
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# failover lan faillink vlan500
hostname(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0

hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport mode trunk
hostname(config-if)# switchport trunk allowed vlan 200-202
hostname(config-if)# switchport trunk native vlan 5
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown
```

```
hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 500
hostname(config-if)# no shutdown
```

# 同一セキュリティ レベルにある VLAN インターフェイス間の通信の許可

デフォルトでは、セキュリティ レベルが同じインターフェイス同士は通信できません。同じセキュリティのインターフェイス間で通信を許可すると、アクセス リストがなくても同じセキュリティのインターフェイスすべての間で自由にトラフィックが流れるようになります。

**（注）** NAT 制御をイネーブルにする場合、同一セキュリティ レベルのインターフェイス間では NAT を設定する必要がありません。NAT および同一セキュリティ レベルのインターフェイスの詳細については、「NAT および同じセキュリティ レベルのインターフェイス」（P.17-13）を参照してください。

同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。

相互通信を可能にするために同じセキュリティ レベルのインターフェイスをイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# same-security-traffic permit inter-interface
```

この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。