CHAPTER 4

トラフィックのブリッジング

この章では、VLAN 構成においてクライアントとサーバが、Cisco 4700 シリーズ Application Control Engine（ACE）アプライアンスを介してレイヤ 2（L2）またはレイヤ 3（L3）で通信する方法について説明します。クライアント側の VLAN とサーバ側の VLAN が同一のサブネットにある場合、シングル サブネット モードでトラフィックをブリッジングするよう ACE を設定できます。

クライアント側の VLAN とサーバ側の VLAN が別々のサブネットにある場合、トラフィックをルーティングするよう ACE を設定できます。詳細については、第 3 章「ACE のルート設定」を参照してください。

ブリッジ モードでは、ACE は「bump-in-the-wire」として動作し、ルーテッド ホップにはなりません。ダイナミック ルーティング プロトコルは必要ありません。

インターフェイス VLAN にブリッジ グループを設定すると、ACE では自動的にそのインターフェイスをブリッジド インターフェイスとして設定します。ACE は、ブリッジ グループごとに最大 2 つのレイヤ 2 インターフェイス VLAN をサポートします。

（注） ACE では、レイヤ 2 インターフェイスでの共有 VLAN 構成はサポートされていません。

L2 VLAN は IP アドレスとは関連付けされていないので、IP トラフィックを制御するには拡張 Access Control List（ACL; アクセス コントロール リスト）が必要です。また、非 IP トラフィックを通過させるために EtherType ACL を任意で設定できます。ACL の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*』を参照してください。

ブリッジ グループ VLAN をイネーブルにするには、当該ブリッジ グループに関連付けされた Bridge Group Virtual Interface（BVI; ブリッジ グループ仮想インターフェイス）を設定する必要があります。また、BVI に IP アドレスを設定する必要があります。このアドレスは、Address Resolution Protocol（ARP; アドレス解決プロトコル）要求や管理トラフィックなど、ACE から送信されるトラフィックの送信元 IP アドレスとして使用されます。ACE は、システムごとに 4094 の BVI をサポートします。

（注）　ACE では、システムごとに最大 8192 のインターフェイス（VLAN、共有 VLAN、および BVI インターフェイスを含む）をサポートします。

ACE では、ブリッジド インターフェイスでの MAC アドレス ラーニングはサポートされていません。その代わりに、ARP によってラーニングが実行されます。ブリッジ ルックアップは、ブリッジ グループ ID と宛先 MAC アドレスに基づいています。ブリッジド インターフェイスは、ブリッジ グループの他のインターフェイスにマルチキャストおよびブロードキャスト ブリッジド トラフィックを自動的に送信します。

ARP パケットは、確認および検査後に常に L2 インターフェイスを通過します。ACE での ARP の設定については、第 5 章「ARP の設定」を参照してください。着信インターフェイスからのマルチキャストおよびブロードキャスト パケットは、ブリッジ グループ内の他の L2 インターフェイスにフラッディングされます。

この章の主な内容は、次のとおりです。

ブリッジ モード設定のクイック スタート

表 4-1 は、ACE にブリッジ グループを設定するために必要な手順を簡潔に示したものです。各手順には、その作業を完了するために必要な CLI コマンドが示されています。

表 4-1　ブリッジ モード設定のクイック スタート

作業およびコマンド例

1. マルチ コンテキスト モードを使用している場合は、CLI プロンプトをよく見て、目的のコンテキストで動作していることを確認します。必要に応じて適切なコンテキストに変更してください。
`host1/Admin# changeto C1`
`host1/C1#`
この表の以降の例では、特に指定されていないかぎり、管理コンテキストが使用されています。コンテキスト作成に関する詳細は、『*Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*』を参照してください。

2. **config** コマンドを入力して、コンフィギュレーション モードにアクセスします。
`host1/Admin# config`
`Enter configuration commands, one per line. End with CNTL/Z`
`host1/Admin(config)#`

3. **interface vlan** コマンドを使用して、ブリッジ グループ用の VLAN を作成し、インターフェイス コンフィギュレーション モードにアクセスします。たとえば、次のように入力します。
`host1/Admin(config)# interface vlan 2`
`host1/Admin(config-if)#`

4. **bridge-group** コマンドを使用して、ブリッジ グループに VLAN を割り当てます。たとえば、次のように入力します。 `host1/Admin(config-if)# bridge-group 15`

表 4-1　ブリッジ モード設定のクイック スタート（続き）

作業およびコマンド例

5. **access-group** コマンドを使用して、VLAN に ACL を割り当ててトラフィックを許可します。トラフィックを許可するインターフェイスに ACL を設定する必要があります。設定しない場合、ACE によってそのインターフェイスですべてのトラフィックが拒否されます。IP トラフィック用の拡張 ACL または非 IP トラフィック用の EtherType ACL の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*』を参照してください。
 	
次に、IP トラフィックを許可する ACL の例を示します。
`access-list ACL1 line 5 extended permit ip any any`
 	
トラフィック用の ACL を設定したのち、VLAN に割り当てます。たとえば、インターフェイスのインバウンド トラフィックに ACL1 を割り当てるには、次のように入力します。
`host1/Admin(config-if)# access-group input ACL1`

6. **no shutdown** コマンドを使用して、VLAN をイネーブルにします。たとえば、次のように入力します。
`host1/Admin(config-if)# no shutdown`
`host1/Admin(config-if)# exit`

7. ブリッジ グループに 2 つめの VLAN を設定します。ステップ 3 ～ 6 を再度実行します。

8. コンフィギュレーション モードで **interface bvi** コマンドを使用して、ブリッジ グループ用の BVI を作成し、インターフェイス コンフィギュレーション モードにアクセスします。たとえば、ブリッジ グループ 15 用の BVI を作成するには、次のように入力します。
`host1/Admin(config)# interface bvi 15`
`host1/Admin(config-if)#`

表 4-1　ブリッジ モード設定のクイック スタート（続き）

作業およびコマンド例
9. **ip address** コマンドを使用して、BVI に IP アドレスを割り当てます。BVI の IP アドレスとマスクを設定するには、次の例のように入力します。 `host1/Admin(config-if)# ip address 10.0.0.81 255.0.0.0`
10. **no shutdown** コマンドを使用して、BVI をイネーブルにします。BVI をイネーブルにするには、次の例のように入力します。 `host1/Admin(config-if)# no shutdown`

ブリッジ グループ VLAN の設定

ブリッジ モードでは、2 つのインターフェイス VLAN をグループ化して、インターフェイス VLAN 間でパケットをブリッジングできます。すべてのインターフェイスが 1 つのブロードキャスト ドメインに属し、一方の VLAN からのパケットは他方の VLAN にスイッチングされます。ACE のブリッジ モードでは、ブリッジ グループごとにサポートされる L2 VLAN は 2 つだけです。このモードでは、L2 VLAN インターフェイスに IP アドレスは設定されていません。

ブリッジ グループを作成する前に、VLAN をコンテキストに割り当て、インターフェイス コンフィギュレーション モードにアクセスしてからアトリビュートを設定します。コンフィギュレーション モードで **interface vlan** コマンドを使用します。このコマンドの構文は次のとおりです。

interface vlan *number*

number 引数は、コンテキストに割り当てる VLAN 番号です。たとえば、次のように入力します。

```
host1/Admin(config)# interface vlan 2
```

VLAN を削除するには、**no interface vlan** コマンドを使用します。たとえば、次のように入力します。

```
host1/Admin(config)# no interface vlan 2
```

VLAN の設定後、次の項目の説明に従ってアトリビュートを設定します。

- VLAN へのブリッジ グループの設定（p.4-7）
- ブリッジ グループ VLAN への ACL の割り当て（p.4-7）
- インターフェイスのイネーブル化（p.4-9）

VLAN へのブリッジ グループの設定

VLAN にブリッジ グループを設定すると、ACE では自動的にその VLAN をブリッジド VLAN として設定します。ブリッジ グループに VLAN を割り当てるには、インターフェイス コンフィギュレーション モードで **bridge-group** コマンドを使用します。このコマンドの構文は次のとおりです。

bridge-group *number*

number 引数は 1 ～ 4094 の数字です。たとえば、VLAN にブリッジ グループ 15 を割り当てるには、次のように入力します。

```
host1/Admin(config-if)# bridge-group 15
```

VLAN からブリッジ グループを削除するには、**no bridge group** コマンドを使用しますたとえば、次のように入力します。

```
host1/Admin(config-if)# no bridge-group
```

ブリッジ グループ VLAN への ACL の割り当て

ブリッジ グループ VLAN では、IP トラフィック用の拡張 ACL または非 IP トラフィック用の EtherType ACL がサポートされます。次に、IP トラフィックを許可する拡張 ACL の例を示します。

```
host1/Admin(config)# access-list ACL1 line 5 extended permit ip any
any
```

非 IP トラフィックには、EtherType ACL を設定します。EtherType ACL はイーサネット V2 フレームをサポートします。Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）、Internet Protocol（IP; インターネット プロトコル）version 6（IPv6）、および Bridge Protocol Data Unit（BDPU; ブリッジ プロトコル データ ユニット）の非 IP EtherType のうち、1 つまたはすべてを通過させるよう ACE を設定できます。

BPDU を許可または拒否できます。デフォルトでは、すべての BPDU は拒否されます。ACE のポートはトランク ポートなので、ACE はトランク ポート（シスコ独自）BPDU を受信します。トランク BPDU のペイロードには VLAN 情報が含まれています。そのため、BPDU を許可した場合、ACE はペイロードを発信 VLAN で変更します。

（注） ACE にフェールオーバーを設定した場合、ブリッジング ループを防止するために、EtherType ACL を使用して両方のインターフェイスで BPDU を許可する必要があります。

次に、BPDU を許可する EtherType ACL の例を示します。

```
host1/Admin(config)#  access-list NONIP ethertype permit bdpu
```

拡張 ACL または EtherType ACL の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*』を参照してください。

トラフィックを許可する ACL を設定したのち、ブリッジ グループ VLAN に割り当てます。VLAN のインバウンドまたはアウトバウンド方向に対して ACL を割り当てるには、インターフェイス コンフィギュレーション モードで **access-group** コマンドを使用します。このコマンドの構文は次のとおりです。

access-group {**input** | **output**} *acl_name*

オプションと引数は次のとおりです。

- **input** — ACL をインターフェイスのインバウンド方向に適用するよう指定します。
- **output** — ACL をインターフェイスのアウトバウンド方向に適用するよう指定します。このオプションは EtherType ACL ではサポートされていません。
- *acl_name* — インターフェイスに適用する既存の ACL の ID を指定します。

たとえば、インターフェイスのインバウンド トラフィックに ACL1 を割り当てるには、次のように入力します。

```
host1/Admin(config-if)# access-group input ACL1
```

インターフェイスのアウトバウンド トラフィックに ACL1 を割り当てるには、次のように入力します。

```
host1/Admin(config-if)# access-group output ACL1
```

インターフェイスから ACL を削除するには、**no access-group** コマンドを使用します。たとえば、次のように入力します。

```
host1/Admin(config-if)# no access-group output ACL1
```

インターフェイスのイネーブル化

インターフェイスを作成しても、イネーブルにするまではシャットダウン状態のままです。インターフェイスを使用できるようイネーブルにするには、**no shutdown** コマンドを使用します。たとえば、次のように入力します。

```
host1/Admin (config-if)# no shutdown
```

VLAN をディセーブルにするには、**shutdown** コマンドを使用します。たとえば、次のように入力します。

```
host1/Admin(config-if)# shutdown
```

ブリッジ グループ VLAN をイネーブルにしたのち、BVI を設定して動作させます。

BVI の設定

ACE からトラフィック（ARP 要求など）を発信したり、管理トラフィックを処理したりするには、ブリッジ グループに対して、同じサブネット上の IP アドレスが設定されたインターフェイスが必要です。このインターフェイスが BVI です。

BVI は対応するブリッジ グループと共に、ルータのルーテッド インターフェイスに関連付けされますが、ブリッジングをサポートしないルーテッド インターフェイスとして動作します。BVI には関連付けされたブリッジ グループの番号が割り当てられます。各ブリッジ グループでサポートされる BVI は 1 つだけです。BVI の MAC アドレスは、関連付けされたブリッジ グループ インターフェイスのアドレスと同じです。トラフィックを転送するには、BVI および関連付けされたブリッジ グループ インターフェイスをイネーブルにする必要があります。

BVI を使用して管理トラフィックを終端させるには、管理トラフィックの送信元となるレイヤ 2 インターフェイスに管理ポリシーを適用します。このポリシーを適用するには、ブリッジ グループ インターフェイス VLAN にサービス ポリシーを設定し、BVI に管理 IP アドレスを設定します。

ここで説明する内容は、次のとおりです。

ブリッジ グループの仮想ルーテッド インターフェイスの作成

コンフィギュレーション モードで **interface bvi** コマンドを使用すると、ブリッジ グループの仮想ルーテッド インターフェイスを作成できます。このコマンドの構文は次のとおりです。

interface bvi *group_number*

group_number 引数は、レイヤ 2 VLAN インターフェイスに設定されたブリッジ グループ番号です。

たとえば、ブリッジ グループ 15 用の BVI を作成するには、次のように入力します。

```
host1/Admin(config)# interface bvi 15
host1/Admin(config-if)#
```

ブリッジ グループ 15 用の BVI を削除するには、次のように入力します。

```
host1/Admin(config)# no interface bvi 15
```

BVI の IP アドレスの設定

BVI のインターフェイス コンフィギュレーション モードで **ip address** コマンドを使用すると、BVI に IP アドレスを割り当てることができます。このコマンドの構文は次のとおりです。

ip address *ip_address mask*

ip_address mask 引数は、インターフェイスのアドレスとサブネット マスクです。ドット付き 10 進表記で IP アドレスとサブネット マスクを入力します。

BVI の IP アドレスとマスクを設定するには、次の例のように入力します。

```
host1/Admin(config-if)# ip address 10.0.0.10 255.255.255.0
```

BVI の IP アドレスを削除するには、次のように入力します。

```
host1/Admin(config-if)# no ip address
```

エイリアス IP アドレスの設定

アクティブ appliance およびスタンバイ モジュールで冗長構成を設定する場合、アクティブおよびスタンバイ appliance で共有される IP アドレスを持つ VLAN インターフェイスを設定できます。BVI の共有アドレスを設定するには、インターフェイス コンフィギュレーション モードで **alias** コマンドを使用します。このコマンドの構文は次のとおりです。

alias *ip_address mask*

ip_address mask 引数は、インターフェイスのアドレスとサブネット マスクです。ドット付き 10 進表記で IP アドレスとサブネット マスクを入力します。

BVI の IP アドレスとマスクを設定するには、次の例のように入力します。

```
host1/Admin(config-if)# alias 10.0.0.15 255.255.255.0
```

BVI のエイリアス IP アドレスを削除するには、次のように入力します。

```
host1/Admin(config-if)# no alias 10.0.0.15 255.255.255.0
```

ピア IP アドレスの設定

冗長構成の場合、スタンバイ appliance のコンフィギュレーション モードはデフォルトでディセーブルであり、アクティブ appliance で変更が発生すると、スタンバイ appliance は自動的に同期します。ただし、アクティブ appliance とスタンバイ モジュールの IP アドレスは一意である必要があります。各インターフェイスのアドレスが一意になるよう、アクティブ appliance のインターフェイスの IP アドレスをピア IP アドレスとしてスタンバイ appliance に自動的に同期させます。

スタンバイ appliance のインターフェイスに IP アドレスを設定するには、インターフェイス コンフィギュレーション モードで **peer ip address** コマンドを使用します。アクティブ appliance のピア IP アドレスは、スタンバイ appliance でインターフェイス IP アドレスとして同期化されます。このコマンドの構文は次のとおりです。

peer ip address *ip_address mask*

ip_address mask 引数は、ピア appliance のアドレスとサブネット マスクです。

ピア appliance の IP アドレスとマスクを設定するには、次の例のように入力します。

```
host1/Admin(config-if)# peer ip address 10.0.0.18 255.255.255.0
```

ピア appliance の IP アドレスを削除するには、次のように入力します。

```
host1/Admin(config-if)# no peer ip address
```

BVI の説明の設定

BVI に関する説明を設定するには、インターフェイス コンフィギュレーション モードで **description** コマンドを使用します。このコマンドの構文は次のとおりです。

description *text*

text 引数は、最大 240 文字の英数字（スペースを含む）からなる文字列です。

BVI に関する説明を設定するには、次の例のように入力します。

```
host1/Admin(config-if)# description BVI for Bridge Group 15
```

説明を削除するには、次のように入力します。

```
host1/Admin(config-if)# no description
```

BVI のイネーブル化

BVI をイネーブルにするには、インターフェイス コンフィギュレーション モードで **no shutdown** コマンドを使用します。このコマンドの構文は次のとおりです。

no shutdown

BVI をイネーブルにするには、次の例のように入力します。

```
host1/Admin(config-if)# no shutdown
```

BVI をディーセブルにするには、次のように入力します。

```
host1/Admin(config-if)# shutdown
```

ブリッジ グループまたは BVI 情報の表示

EXEC モードで **show interface vlan** コマンドを使用すると、ブリッジ グループ VLAN に関する情報を表示できます。たとえば、次のように入力します。

```
host1/Admin# show interface vlan 15
```

EXEC モードで **show interface bvi** コマンドを使用すると、BVI に関する情報を表示できます。たとえば、次のように入力します。

```
host1/Admin# show interface bvi 15
```

show interface コマンドの各フィールドの詳細については、第 2 章「VLAN インターフェイスの設定」の 表 2-2 を参照してください。