CHAPTER 2

VLAN インターフェイスの設定

この章では、Cisco 4700 シリーズ Application Control Engine（ACE）アプライアンスに 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。インターフェイスに IP アドレスを設定すると、ACE では自動的にそのインターフェイスをルーテッド モードに設定します。

同様に、VLAN インターフェイスにブリッジ 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。次に、Bridge Group Virtual Interface（BVI; ブリッジ グループ仮想インターフェイス）をブリッジ グループに関連付けます。ブリッジ グループと BVI の詳細については、第 4 章「トラフィックのブリッジング」を参照してください。

ACE は、共有 VLAN もサポートします。共有 VLAN は、同一 VLAN および同一サブネット上にある、コンテキストが異なる複数のインターフェイスです。VLAN を共有できるのはルーテッド インターフェイスのみです。共有 VLAN が設定されていても、コンテキスト間でのルーティングは行われません。

ACE では、システムごとに最大 4093 の VLAN と最大 1024 の共有 VLAN をサポートします。

（注） ACE 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。

この章の主な内容は、次のとおりです。

VLAN インターフェイス設定のクイック スタート

表 2-1 は、ACE に VLAN インターフェイス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 コマンドまたは手順への参照が示されています。各機能の詳細な説明および各 CLI コマンドに関するすべてのオプションについては、表 2-1 以降のセクションを参照してください。

表 2-1　VLAN インターフェイス設定のクイック スタート

作業およびコマンド例

1. 複数のコンテキスト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、説明のため C1 ユーザ 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. グローバル コンフィギュレーション モードを開始します。
`host1/Admin# config`
`host1/Admin(config)#`

3. 開始していない場合は、ACE でイーサネット ポートを設定し、VLAN トランキングを指定します。詳細については、第 1 章「イーサネット インターフェイスの設定」を参照してください。
4. VLAN インターフェイスを設定し、そのアトリビュートを設定するためのモードにアクセスします。たとえば、VLAN 200 を作成するには、次のコマンドを入力します。 `host1/Admin(config)# interface vlan 200`
5. トラフィックのルーティングのため、VLAN インターフェイスに IP アドレスを割り当てます。たとえば、VLAN インターフェイス 200 の IP アドレスを 192.168.1.1 255.255.255.0 に設定するには、次のコマンドを入力します。 `host1/Admin(config-if)# ip address 192.168.1.1 255.255.255.0`
6. VLAN インターフェイスをイネーブルにします。 `host1/Admin(config-if)# no shutdown`

表 2-1　VLAN インターフェイス設定のクイック スタート（続き）

作業およびコマンド例
7. （任意）VLAN インターフェイスの MTU を指定します。 `host1/Admin(config-if)# mtu 1000`
8. スタンバイ ACE アプライアンスのインターフェイスに IP アドレスを設定します。 `host1/Admin(config-if)# peer ip address 11.0.0.81 255.0.0.0`
9. （任意）VLAN インターフェイスの送信元 MAC アドレスに基づいて、Reverse-Path Forwarding（RPF）をイネーブルにします。 `host1/Admin(config-if)# mac-sticky enable`
10. （任意）インターフェイスの機能をわかりやすくするため、インターフェイスに関する説明を追加します。 `host1/Admin(config-if)# description FOR INBOUND AND OUTBOUND TRAFFIC`

11. ポリシー マップをインターフェイスに割り当てます。たとえば、VLAN 3 へのインバウンド トラフィックに対して SLB_OPTIMIZE_POLICY というポリシー マップを割り当てるには、次のコマンドを入力します。
`host1/Admin(config)# interface vlan 200`
`host1/Admin(config-if)# service-policy input SLB_OPTIMIZE_POLICY`

12. ACL　をインターフェイスのインバウンドまたはアウトバウンド方向に適用し、ACL をアクティブにします。たとえば、次のコマンドを入力します。
`host1/Admin(config-if)# access-group input INBOUND`
`host1/Admin(config-if)# exit`

13. VLAN インターフェイスを特定のコンテキストに割り当てます。たとえば、VLAN 200 をコンテキスト C1 に割り当てるには、次のコマンドを入力します。
`host1/Admin(config)# context C1`
`host1/C1(config-context)# allocate-interface vlan 200`

14. （任意）ACE に対して特定の MAC アドレス バンクを設定します。たとえば、MAC アドレス バンク 2 を設定するには、次のコマンドを入力します。 `host1/Admin(config)# shared-vlan-hostid 2`
15. （任意）必要に応じて設定変更をフラッシュ メモリに保存します。 `host1/Admin# copy running-config startup-config`

ACE での VLAN インターフェイスの設定

VLAN インターフェイスを設定し、そのアトリビュートを設定するためのモードにアクセスするには、コンテキストから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、インターフェイスに割り当てる VLAN 番号です。有効な値は 2 ～ 4094 です。デフォルトでは、すべてのデバイスはデフォルト VLAN である VLAN 1 に割り当てられます。

（注） セキュリティ上の理由から、ACE では、ACE の一方の側の VLAN 上のインターフェイスから、モジュールの他方の側の別の VLAN 上のインターフェイスへ、モジュールを介した ping を実行することはできません。たとえばあるホストから、そのホストと同一の VLAN を使用する IP サブネット上の ACE アドレスに対して ping を実行することは可能ですが、ACE の別の VLAN 上に設定された IP アドレスに対して ping を実行することはできません。

たとえば、VLAN 200 を作成するには、次のように入力します。

```
host1/Admin(config)# interface vlan 200
```

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 200
```

（注） ACE は、サーバへ要求を転送する前に、クライアントへのルート バックを必要とします。ルート バックが存在しない場合、ACE はフローを確立できず、クライアントの要求はドロップされます。クライアント トラフィックが ACE に着信する場合、ACE の VLAN 上でクライアント ネットワークへのルーティング設定を適切に行ってください。

ここで説明する内容は、次のとおりです。

- インターフェイスへのトラフィック ルーティング用の IP アドレスの割り当て（p.2-7）
- インターフェイス上のトラフィックのディセーブル化およびイネーブル化（p.2-9）
- インターフェイスでの MTU の設定（p.2-10）
- ピア IP アドレスの設定（p.2-11）
- エイリアス IP アドレスの設定（p.2-12）
- MAC スティッキ機能のイネーブル化（p.2-13）
- インターフェイスの説明の設定（p.2-14）
- UDP ブースター機能の設定（p.2-14）
- インターフェイスへのポリシー マップの割り当て（p.2-15）
- インターフェイスへのアクセス リストの適用（p.2-17）

（注） ACE は、サーバへ要求を転送する前に、クライアントへのルート バックを必要とします。ルート バックが存在しない場合、ACE はフローを確立できず、クライアントの要求はドロップされます。クライアント トラフィックが ACE アプライアンスに着信する場合、ACE の VLAN 上でクライアント ネットワークへのルーティング設定を適切に行ってください。

VLAN インターフェイスで実行できる設定やコマンドのうち、この章では触れていないものがあります。次を参照してください。

- リモート ネットワーク管理 — 『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照
- トランク リンクへの個々の VLAN の割り当て — 第 1 章「イーサネット インターフェイスの設定」の「VLAN トランクへのイーサネット ポートまたはポート チャネル インターフェイスの割り当て」（p.1-31）を参照
- トランクの IEEE 802.1Q ネイティブ VLAN — 第 1 章「イーサネット インターフェイスの設定」の「トランクの 802.1Q ネイティブ VLAN の指定」（p.1-33）を参照

- 特定の VLAN に対するアクセス ポート — 第 1 章「イーサネット インターフェイスの設定」の「VLAN アクセス ポートの設定」（p.1-27）を参照
- デフォルトおよびスタティック ルート — 第 3 章「ACE のルート設定」を参照
- **interface bvi** コマンドを含むブリッジ パラメータ — 第 4 章「トラフィックのブリッジング」を参照
- Address Resolution Protocol（ARP; アドレス解決プロトコル）— 第 5 章「ARP の設定」を参照
- DHCP — 第 6 章「DHCP リレーの設定」を参照
- VLAN に対するポリシー マップ、クラス マップ、SNMP 管理、およびフォールト トレラント VLAN — 『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照
- ステルス ファイアウォール ロード バランシングを含むロード バランシング トラフィック — 『*Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*』を参照
- ACL、Network Address Translation（NAT; ネットワーク アドレス変換）、IP フラグメント再構成、IP 標準化 — 『*Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*』を参照

インターフェイスへのトラフィック ルーティング用の IP アドレスの割り当て

VLAN インターフェイスに IP アドレスを割り当てると、ACE では自動的にそのインターフェイスをルーテッド モードに設定します。VLAN インターフェイスに IP アドレスを割り当てるには、インターフェイス コンフィギュレーション モードで **ip address** 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。

ip address *ip_address mask*

ip_address mask 引数では、VLAN インターフェイスに割り当てる IP アドレスとマスクを指定します。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（たとえば、192.168.1.1 255.255.255.0）。

（注） ACE のどのインターフェイスでもセカンダリ IP アドレスはサポートされません。

単一のコンテキスト内では、各インターフェイス アドレスは一意のサブネット上に割り当てられ、重複することはできません。ただし、IP サブネットが別のコンテキストのインターフェイスと重複することは可能です。

共有 VLAN で複数のコンテキストがある場合は、IP アドレスは一意でなければなりません。非共有 VLAN 上では、同一の IP アドレスを割り当てられます。

たとえば、IP アドレスとマスク、192.168.1.1 255.255.255.0 を VLAN インターフェイス 200 に割り当てるには、次のコマンドを入力します。

```
host1/Admin(config)# interface vlan 200
host1/Admin(config-if)# ip address 192.168.1.1 255.255.255.0
```

このコマンドの入力時に誤った設定を行った場合、正しい情報でコマンドを再度入力してください。

（注） ルーテッド モードとブリッジド モードでは、トラフィックを通過させるために Access Control List（ACL; アクセス コントロール リスト）が必要です。インターフェイスのインバウンドまたはアウトバウンド方向に対して ACL を適用し、ACL をアクティブにするには、VLAN のインターフェイス 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。詳細は、「インターフェイスへのアクセス リストの適用」（p.2-17）を参照してください。ACL の設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*』を参照してください。

インターフェイスでリモート ネットワーク管理アクセスを設定する際は、インターフェイスで ACL を設定する必要はありません。ただしこの場合、クラス マップとポリシー マップの設定が必要です。ACE へのリモート アクセス設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照してください。

VLAN の IP アドレスを削除するには、**no ip address** 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 ip address
```

インターフェイス上のトラフィックのディセーブル化およびイネーブル化

インターフェイスを設定する際、インターフェイスはイネーブルにするまでシャットダウン状態のままです。コンテキスト内でインターフェイスをディセーブルまたは再びイネーブルにする場合、そのコンテキストのインターフェイスのみが設定の対象になります。

インターフェイス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。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、インターフェイス コンフィギュレーション モードで **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。

shutdown

たとえば、VLAN 3 をディセーブルにするには、次のように入力します。

```
host1/Admin(config)# interface vlan 3
host1/Admin(config-if)# shutdown
```

インターフェイスでの MTU の設定

デフォルトの最大伝送ユニット（maximum transmission unit; MTU）は、イーサネット インターフェイスで 1500 バイト ブロックに設定されています。これはほとんどのアプリケーションで十分な値ですが、ネットワークの状態によっては、これより低い値を設定することも可能です。MTU 値よりも大きなデータは、送信前にフラグメント化されます。

注意　レイヤ 7 のポリシー マップを設定し、クライアントの Maximum Segment Size（MSS; 最大セグメント サイズ）よりも小さい値を ACE のサーバ側 VLAN の MTU に設定する場合、**set tcp mss max** コマンドを使用して ACE に設定した MSS の最大値が ACE のサーバ側 VLAN の MTU よりも 40 バイト（TCP ヘッダー＋オプションのサイズ）以上小さい値であることを確認してください。40 バイト以上小さい値でない場合、サーバからの着信パケットが ACE で破棄されることがあります。

インターフェイスに MTU を指定するには、インターフェイス コンフィギュレーション モードで **mtu** コマンドを使用します。このコマンドにより、接続上で送信するデータ サイズを設定できます。このコマンドの構文は次のとおりです。

mtu *bytes*

bytes 引数は、MTU のバイト数です。64 から 9216 のバイト数を入力します。デフォルトは 1500 です。

たとえば、インターフェイスに 1000 バイトの MTU データ サイズを設定するには、次のように入力します。

```
host1/Admin(config-if)# mtu 1000
```

MTU ブロック サイズを 1500 バイトに戻すには、**no mtu** 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 mtu
```

ピア IP アドレスの設定

冗長性を設定する場合、スタンバイ ACE アプライアンスのコンフィギュレーション モードはデフォルトではディセーブルであり、アクティブ アプライアンスで変更が発生すると、スタンバイ ACE アプライアンスで自動的に同期化されます。ただし、アクティブおよびスタンバイ ACE アプライアンスのインターフェイス IP アドレスは一意である必要があります。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 ACE アプライアンスのインターフェイスの IP アドレスはピア IP アドレスとして、スタンバイ ACE アプライアンスで同期化されます。

スタンバイ ACE アプライアンス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 ACE アプライアンスのピア IP アドレスは、スタンバイ ACE アプライアンス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 ACE アプライアン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（たとえば、192.168.1.1 255.255.255.0）。

（注） ピア IP アドレスは、共有 VLAN の複数のコンテキストで一意である必要があります。

ピア ACE アプライアンスの 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 11.0.0.81 255.0.0.0
```

ピア ACE アプライアンスの 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
```

エイリアス IP アドレスの設定

アクティブおよびスタンバイ アプライアンス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 アプライアンスで移動するエイリアス IP アドレスを持った VLAN インターフェイスを設定できます。エイリアス IP アドレスは、冗長構成にある 2 つの ACE アプライアンスの共有ゲートウェイとして機能します。

（注） エイリアス IP アドレスが機能するには、ACE を冗長構成（フォールト トレランス）にする必要があります。冗長構成の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照してください。

また、ACE は VLAN に割り当てられたエイリアス IP アドレスを使用して、残りのネットワークから非表示にするネットワーク デバイスに対応します。一般的に、ファイアウォールが見えないようなステルス ファイアウォールで VLAN にエイリアス IP アドレスを割り当てます。ACE は、ファイアウォールを通じてフローを送信するロード バランシング プロセスの宛先として、別の ACE で設定されたエイリアス IP アドレスを使用します。ACE 上のファイアウォールとファイアウォール負荷分散（FWLB）の設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*』を参照してください。

エイリアス 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 **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 netmask*

ip_address netmask 引数では、VLAN インターフェイスに割り当てる IP アドレスとネットマスクを指定します。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（たとえば、192.168.1.1 255.255.255.0）。

エイリアス IP アドレスを設定するには、次の例のように入力します。

```
host1/Admin(config-if)# alias 192.168.12.15 255.255.255.0
```

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 192.168.12.15 255.255.255.0
```

MAC スティッキ機能のイネーブル化

MAC スティッキ機能により、ACE では、元のクライアントからの接続設定を受信したアップストリーム デバイスに対して、リターン トラフィックを確実に送信できます。この機能をイネーブルにすると、ACE は新規接続における最初のパケットの送信元 MAC アドレスを使用して、リターン トラフィックを送信するデバイスを決定します。これにより、ACE では、ロード バランシング接続を利用したリターン トラフィックを、接続を開始した同一デバイスに送信できます。デフォルトでは、ACE は、ルート ルックアップを実行してクライアントへ到達するためのネクスト ホップを選択します。

この機能は、ACE が、ファイアウォールや透過型キャッシュなどのレイヤ 2 およびレイヤ 3 の隣接ステートフル デバイスからトラフィックを受信するときに有効です。この機能を使用すると、ACE が送信元 NAT を必要とせずに、接続元となる正しいステートフル デバイスにリターン トラフィックを送信できるからです。ファイアウォール負荷分散の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*』を参照してください。

VLAN インターフェイスで MAC スティッキ機能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 **mac-sticky enable** コマンドを使用します。デフォルトで、MAC スティッキ機能は ACE で無効になっています。このコマンドの構文は次のとおりです。

mac-sticky enable

（注）　**ip verify reverse-path** コマンドを使用する場合、このコマンドは使用できません。**ip verify reverse-path** コマンドの詳細については、『*Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*』を参照してください。

MAC スティッキ機能をイネーブルにするには、次のように入力します。

```
host1/Admin(config-if)# mac-sticky enable
```

MAC スティッキ機能をディセーブルにするには、**no mac-sticky enable** 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 mac-sticky enable
```

インターフェイスの説明の設定

インターフェイスに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、インターフェイスの説明です。最大 240 の英数字（スペースを含む）からなる引用符なしの文字列を入力します。

インターフェイス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 FOR INBOUND AND OUTBOUND TRAFFIC
```

インターフェイスの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
```

UDP ブースター機能の設定

ネットワーク アプリケーションで非常に高い UDP 接続レートが必要な場合は、UDP ブースター機能を設定します。この機能と設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*』を参照してください。この機能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 **udp** 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。

udp {**ip-source-hash** | **ip-destination-hash**}

キーワードは次のとおりです。

- **ip-source-hash —** 接続のマッチングを行う前に、送信元ハッシュ VLAN インターフェイスに一致する UDP パケットの送信元 IP アドレスをハッシュするように、ACE を設定します。クライアント側のインターフェイスでこのキーワードを設定します。
- **ip-destination-hash —** 接続のマッチングを行う前に、宛先ハッシュ VLAN インターフェイスに一致する UDP パケットの宛先 IP アドレスをハッシュするように、ACE を設定します。サーバ側のインターフェイスでこのキーワードを設定します。

たとえば、クライアント側のインターフェイスで、UDP パケットの送信元 IP アドレスに対する UDP ハッシュ転送をイネーブルにするには、次のように入力します。

```
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# udp ip-source-hash
```

この機能をディセーブルにするには、次のように入力します。

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

インターフェイスへのポリシー マップの割り当て

VLAN インターフェイスにポリシー マップを割り当てると、このマップを使用して、ACE でインターフェイス上のすべてのネットワーク トラフィックを評価できます。ポリシー マップの設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照してください。

1 つの VLAN インターフェイスに対して、または同一コンテキスト内のすべての VLAN インターフェイスに対してグローバルに、1 つまたは複数のポリシー マップを適用できます。インターフェイスで有効化されたポリシー マップによって、指定済みのグローバルなポリシー マップの重複する分類やアクションはすべて上書きされます。

1 つのインターフェイスに複数のポリシー マップを割り当てることができます。ただし ACE では、各インターフェイスで 1 度に 1 つのポリシー マップしかアクティブにできません。ACE にポリシー マップを設定する場合、設定順序が重要です。

service-policy コマンドは、インターフェイス コンフィギュレーション モードとコンフィギュレーション モード両方で使用できます。インターフェイス コンフィギュレーション モードでポリシー マップを指定すると、ポリシー マップを特定の VLAN インターフェイスに適用します。コンフィギュレーション モードでポリシー マップを指定すると、ポリシーをコンテキストに関連付けられたすべての VLAN インターフェイスに適用します。

このコマンドの構文は次のとおりです。

service-policy input *policy_name*

キーワード、引数、およびオプションは次のとおりです。

- **input** — VLAN インターフェイスのインバウンド方向に適用するトラフィック ポリシーを指定します。トラフィック ポリシーにより、該当インターフェイスで受信されたすべてのトラフィックが評価されます。
- *policy_name* — **policy-map** コマンドを使用して作成した設定済みポリシーマップ。名前には最大 64 文字の英数字を入力できます。

たとえば、VLAN インターフェイスを指定し、複数のサービス ポリシーを VLAN に適用するには、次のように入力します。

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip address 172.16.1.100 255.255.255.0
host1/Admin(config-if)# service-policy input L4_SLB_POLICY
host1/Admin(config-if)# service-policy input SLB_OPTIMIZE_POLICY
host1/Admin(config-if)# service-policy input HTTP_INSPECT_L4POLICY
```

たとえば、複数のサービス ポリシーをコンテキストに関連付けられた VLAN すべてにグローバルに適用するには、次のように入力します。

```
host1/Admin(config)# service-policy input L4_SLB_POLICY
host1/Admin(config)# service-policy input SLB_OPTIMIZE_POLICY
host1/Admin(config)# service-policy input HTTP_INSPECT_L4POLICY
```

VLAN インターフェイスからトラフィック ポリシーを削除するには、次のように入力します。

```
host1/Admin(config-if)# no service-policy input L4_SLB_POLICY
```

コンテキストに関連付けられたすべての VLAN からトラフィック ポリシーをグローバルに削除するには、次のように入力します。

```
host1/Admin(config)# no service-policy input L4_SLB_POLICY
```

次のいずれかの方法でトラフィック ポリシーを削除できます。

- サービス ポリシーを適用した最後の VLAN インターフェイスから個別に削除
- 同じコンテキスト内のすべての VLAN インターフェイスからグローバルに削除

ACE は関連するサービス ポリシーの統計情報を自動的にリセットします。ACE は、次にトラフィック ポリシーを特定の VLAN インターフェイスに適用する、または同じコンテキスト内のすべての VLAN インターフェイスにグローバルに適用するときに、サービス ポリシー統計情報の新しい開始点を提供するため、このアクションを実行します。

サービス ポリシーを作成するときの注意点は次のとおりです。

- コンテキストにグローバルに適用されたポリシー　マップは、そのコンテキストに存在するすべてのインターフェイスに内部的に適用されます。
- VLAN インターフェイスで有効化されたポリシーによって、指定済みのグローバルなポリシーの重複する分類やアクションはすべて上書きされます。
- ACE では、特定のインターフェイスで有効化できるのは、特定機能タイプの 1 つのポリシーだけです。

インターフェイスへのアクセス リストの適用

トラフィックがインターフェイスを通過することを許可するには、VLAN インターフェイスに ACL を適用する必要があります。タイプ（拡張、ICMP、または EtherType）ごとに 1 つの ACL をインターフェイスのインバウンドおよびアウトバウンド方向に適用できます。ACL および ACL を適用する方向の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*』を参照してください。

コネクションレス型のプロトコルの場合、両方向でトラフィックを通過させるには、ACL を送信元および宛先のインターフェイスに適用する必要があります。たとえば、透過モードの場合に ACL で Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）を許可するには、ACL を両方のインターフェイスに適用する必要があります。

ACL をインターフェイスのインバウンドまたはアウトバウンド方向に適用し、ACL をアクティブにするには、インターフェイス コンフィギュレーション モードで **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。
- *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、次のように入力します。

```
host1/Admin(config)# interface vlan100
host1/Admin(config-if)# access-group input INBOUND
```

インターフェイスから ACL 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 input INBOUND
```

ユーザ コンテキストへの VLAN の割り当て

デフォルトでは、設定されたすべての VLAN は管理コンテキストで使用できます。管理コンテキストで、ユーザ コンテキストに VLAN を割り当てることができます。管理コンテキストで **allocate-interface vlan** コマンドを使用して 1 つまたは複数の VLAN インターフェイスを関連するユーザ コンテキストに割り当てる前に、すべてのユーザ コンテキストにこれらの VLAN インターフェイスを設定できます。

VLAN は、複数のコンテキストで共有できます。ただし、ACE がサポートできる共有 VLAN の数は、システムごとに 最大 1024 です。

（注） VLAN が複数のコンテキストで共有される場合、コンテキスト全体で使用される IP アドレスは一意でなければならず、インターフェイスは同一のサブネットに属している必要があります。複数のコンテキスト上のトラフィックを分類するため、複数のコンテキストに割り当てられた 1 つの VLAN は、複数の MAC アドレスを持ちます。共有 VLAN を設定した場合、コンテキスト間でのルーティングは行われません。

コンテキストに VLAN インターフェイスを割り当てるには、コンテキスト モードにアクセスし、コンフィギュレーション モードで **allocate-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。

allocate-interface vlan *vlan_number*

vlan_number 引数は、ACE に割り当てられた VLAN の番号または範囲です。

たとえば、VLAN 10 をコンテキスト A に割り当てるには、次のように入力します。

```
host1/Admin(config)# context A
host1/Admin(config-context)# allocate-interface vlan 10
```

VLAN 100 から 200 までの範囲をコンテキストに割り当てるには、次のように入力します。

```
host1/Admin(config-context)# allocate-interface vlan 100-200
```

ユーザ コンテキストから VLAN を削除するには、コンテキスト コンフィギュレーション モードで **no allocate-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)# context A
host1/Admin(config-context)# no allocate-interface vlan 10
```

（注） ユーザ コンテキストで VLAN が使用中の場合は、コンテキストから VLAN を割り当て解除できません。

コンテキストから VLAN の範囲を削除するには、次のように入力します。

```
host1/Admin(config-context)# no allocate-interface vlan 100-200
```

共有 VLAN 用 MAC アドレスのバンクの設定

複数のコンテキストが 1 つの VLAN を共有する場合、ACE はコンテキストごとに異なる MAC アドレスを VLAN に割り当てます。共有 VLAN 用に確保された MAC アドレスの範囲は、0x001243dc6b00 から 0x001243dcaaff です。すべての ACE アプライアンスはこれらのアドレスを、16,000 の MAC アドレスを含むグローバル プールから取得します。このプールは 16 のバンクに分けられ、各バンクには 1024 のアドレスが含まれています。各サブネットには 16 の ACE が割り当て可能です。

各 ACE は 1024 の共有 VLAN をサポートし、プールから取得した 1 つの MAC アドレス バンクのみを使用します。共有 MAC アドレスは、共有 VLAN インターフェイスと関連付けられます。

デフォルトで、ACE が使用する MAC アドレス バンクは、起動時にランダムに選択されます。ただし、同一のレイヤ 2 ネットワーク上で 2 つの ACE アプライアンスを設定して共有 VLAN を使用する場合、ACE は同一のアドレス バンクを選択する可能性があり、結果として同一の MAC アドレスが使用されることになります。この重複を避けるため、ACE が使用するバンクを必ず設定してください。

ローカルの ACE、またはピアの ACE に対して特定の MAC アドレス バンクを冗長構成で設定するには、管理コンテキストからコンフィギュレーション モードでそれぞれ **shared-vlan-hostid** または **peer shared-vlan-hostid** 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。

shared-vlan-hostid *number*

peer shared-vlan-hostid *number*

number 引数は、ACE が使用する MAC アドレス バンクを表します。1 から 16 の数を入力します。複数の ACE に対しては、必ず異なるバンク番号を設定してください。

たとえば、ローカルの ACE に MAC アドレス バンク 2 を、ピアの ACE にバンク 3 を設定するには、次のように入力します。

```
host1/Admin(config)# shared-vlan-hostid 2
host1/Admin(config)# peer shared-vlan-hostid 3
```

設定済みの MAC アドレス バンクを削除して、ACE がランダムにバンクを選択できるようにするには、**no shared-vlan-hostid** 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 shared-vlan-hostid
```

ピア ACE から設定済みの MAC アドレス バンクを削除して、ランダムにバンクを選択できるようにするには、**no peer shared-vlan-hostid** 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 peer shared-vlan-hostid
```

VLAN または BVI インターフェイス情報の表示

VLAN または BVI インターフェイスに関する情報を表示するには、**show interface** コマンドを使用します。ここで説明する内容は、次のとおりです。

イーサネット データ ポート、イーサネット管理ポート、またはポート チャネル仮想インターフェイスに関する情報を表示するには、**show interface** コマンドを使用します。詳細については、第 1 章「イーサネット インターフェイスの設定」を参照してください。

VLAN および BVI 情報の表示

すべてのまたは特定の VLAN または BVI インターフェイスに関する詳細、統計情報、または IP 情報を表示するには、EXEC モードで **show interface** 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。

show interface [**bvi** *number* | **vlan** *number*]

bvi | **vlan** *number* オプションを指定すると、特定の VLAN またはブリッジ グループの仮想インターフェイス番号に関する情報が表示されます。

オプションを指定せずに **show interface** コマンドを入力すると、ACE によってすべての VLAN および BVI インターフェイスの情報が表示されます。たとえば、次のように入力します。

```
host1/Admin# show interface
```

表 2-2 に、**show interface** コマンドの出力フィールドを示します。

表 2-2　show interface コマンドの出力フィールドの説明

フィールド	説明
VLAN_name/ *BVI_number* is	特定の VLAN または BVI のステータス：up または down
Hardware type is	インターフェイスのハードウェア タイプ：VLAN または BVI
MAC address	IP アドレスにマッピングされたシステムの MAC アドレス。BVI MAC アドレスは、関連付けられたブリッジ グループの VLAN アドレスと同一であることに注意
Mode	VLAN または BVI に関するモード。ブリッジ グループの VLAN の場合は transparent、ルーテッド VLAN または BVI の場合は routed、その他の場合は「unknown」と表示
FT status	インターフェイスの冗長構成に関するステータス
Description	VLAN または BVI の説明
MTU	設定された MTU（バイト単位）
Last cleared	VLAN または BVI が最後にクリアされた時間
Alias IP address	設定されたエイリアス IP アドレス
Peer IP address	設定されたピア IP アドレス
Virtual MAC address	インターフェイスが冗長構成でアクティブの場合に、エイリアス IP アドレスおよび VIP アドレスにより使用される MAC アドレス（インターフェイスがこのステートの場合に限り表示）
# unicast packets input, # bytes	着信ユニキャスト パケットの総数およびバイト数
# multicast, # broadcast	着信マルチキャスト パケットおよびブロードキャスト パケットの総数
# input errors, # unknown, # ignored, # unicast RFP drops	着信パケットのエラー総数（不明または無視されたパケット、あるいは RFP によりドロップされたパケットを含む）

表 2-2　show interface コマンドの出力フィールドの説明（続き）

フィールド	説明
# unicast packets output, # bytes	発信ユニキャスト パケットの総数およびバイト数
# multicast, # broadcast	発信マルチキャスト パケットおよびブロードキャスト パケットの総数
# output errors, # unknown	発信パケットのエラー数（不明パケットを含む）

VLAN および BVI の要約統計情報の表示

すべてのまたは指定された BVI または VLAN に関する設定およびステータスの要約情報を表示するには、EXEC モードで **show ip interface brief** 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。

show ip interface brief [**bvi** *number* | **vlan** *number*]

bvi | **vlan** *number* オプションを指定すると、特定の VLAN またはブリッジ グループの仮想インターフェイス番号に関する情報が表示されます。

オプションを指定せずに **show ip interface brief** コマンドを入力すると、ACE によってすべての VLAN および BVI インターフェイスの情報が表示されます。たとえば、次のように入力します。

```
host1/Admin# show ip interface brief
```

表 2-3 に、**show ip interface brief** コマンドの出力フィールドを示します。

表 2-3　show ip interface brief コマンドの出力フィールドの説明

フィールド	説明
Interface	VLAN 番号またはブリッジ グループの仮想インターフェイス番号
IP Address	VLAN インターフェイスの IP アドレスとマスク
Status	特定の VLAN または BVI のステータス：up または down
Protocol	ライン プロトコルのステータス：up または down

内部インターフェイス マネージャ テーブルの表示

内部インターフェイス マネージャ テーブルとイベントを表示するには、EXEC モードで **show interface internal** 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。

show interface internal {**event-history** {**dbg** | **mts**} | **iftable** [*interface_name*] | **vlantable** [*vlan_number*]

キーワードと引数は次のとおりです。

- **event-history** {**dbg** | **mts**} **—** デバッグ履歴（dbg）またはメッセージ履歴（mts）を表示します。このキーワードは、管理コンテキストでのみ使用できます。
- **iftable** [*interface_name*] **—** マスター インターフェイス テーブルを表示します。インターフェイス名を指定すると、ACE によって該当インターフェイスのテーブル情報が表示されます。
- **vlantable** [*vlan_number*] **—** VLAN テーブルを表示します。インターフェイス番号を指定すると、ACE によって該当インターフェイスのテーブル情報が表示されます。

（注）　**show interface internal** コマンドは、デバッグに使用します。このコマンドの出力は、訓練を受けたシスコの保守担当者が ACE のデバッグとトラブルシューティングを行う際に活用するためのものです。このコマンド構文の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Command Reference*』を参照してください。

たとえば、最新のイベントから始まるインターフェイス内部デバッグ イベント履歴を表示するには、次のように入力します。

```
host1/Admin# show interface internal event-history dbg
```

最新のイベントから始まるインターフェイス内部メッセージ イベント履歴を表示するには、次のように入力します。

```
host1/Admin# show interface internal event-history mts
```

マスター インターフェイス テーブルを表示するには、次のように入力します。

```
host1/Admin# show interface internal iftable
```

マスター VLAN テーブルを表示するには、次のように入力します。

```
host1/Admin# show interface internal vlantable
```

VLAN または BVI インターフェイス統計情報のクリア

show interface コマンドで表示される統計情報をクリアするには、EXEC モードで **clear interface** 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。

clear interface [**vlan** *number* | **bvi** *number*]

オプションや引数を指定しない場合、すべての VLAN および BVI の統計情報がゼロに設定されます。オプションと引数は次のとおりです。

- **vlan** *number* **—** 特定の VLAN の統計情報をクリアします。
- **bvi** *number* **—** 特定の BVI の統計情報をクリアします。BVI インターフェイスの統計情報は収集されません。パケット数は、下位のブリッジド（レイヤ 2）インターフェイスについてカウントされます。

たとえば、VLAN 10 の統計情報をクリアするには、次のように入力します。

```
host1/Admin# clear interface vlan 10
```

（注） 冗長構成の場合、アクティブ ACE およびスタンバイ ACE の両方で、統計情報（ヒット カウント）を明示的にクリアする必要があります。アクティブ ACE アプライアンスの統計情報しかクリアしないと、スタンバイ ACE アプライアンスの統計情報は古い値のまま残ります。