CHAPTER 1

VLAN インターフェイスの設定

Cisco Application Control Engine（ACE）モジュールには、クライアントおよびサーバからのトラフィックを受信する外部物理インターフェイスは存在せず、代わりに内部 VLAN インターフェイスを使用します。まず、スーパーバイザ エンジンから ACE に VLAN を割り当ててください。ACE に VLAN を割り当てたら、ACE 上で該当する VLAN インターフェイスをルーテッドまたはブリッジドのいずれかに設定します。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 3 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、モジュールごとに最大 4093 の VLAN と最大 1024 の共有 VLAN をサポートします。

（注） さらに 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。

この章の主な内容は、次のとおりです。

- Cisco IOS ソフトウェアを使用した VLAN の設定
- ユーザ コンテキストへの VLAN の割り当て
- 共有 VLAN 用 MAC アドレスのバンクの設定
- VLAN インターフェイスに対する MAC アドレスの自動生成
- 出力 MAC ルックアップのディセーブル化
- ACE での VLAN インターフェイスの設定
- インターフェイス情報の表示
- EOBC 情報の表示
- インターフェイス統計情報のクリア

Cisco IOS ソフトウェアを使用した VLAN の設定

ACE が Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータのスーパーバイザ エンジンからトラフィックを受信できるようにするには、スーパーバイザ エンジンで VLAN グループを作成し、ACE に割り当てます。VLAN グループを ACE に割り当てたら、ACE で VLAN インターフェイスを設定します。デフォルトで、すべての VLAN は ACE の Admin コンテキストに割り当てられています。

ここで説明する内容は、次のとおりです。

- Cisco IOS ソフトウェアを使用した VLAN グループの作成
- Cisco IOS ソフトウェアによる VLAN グループの ACE への割り当て
- SVI の MSFC への追加

Cisco IOS ソフトウェアを使用した VLAN グループの作成

Cisco IOS ソフトウェアで 1 つまたは複数の VLAN グループを作成したあと、グループを ACE に割り当てます。たとえば、1 つのグループにすべての VLAN を割り当てたり、内部グループと外部グループを 1 つずつ作成したり、またはお客様ごとに 1 つずつグループを作成したりすることができます。

同一の VLAN を複数のグループに割り当てることはできませんが、最大で 16 のグループを ACE に割り当てられます。たとえば、ある VLAN を複数の ACE に割り当てようとする場合は、この VLAN を、各 ACE 専用の VLAN とは別のグループに割り当てることができます。

スーパーバイザ エンジンで Cisco IOS ソフトウェアを使用して VLAN をグループに割り当てるには、**svclc vlan-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。

svclc vlan-group *group_number vlan_range*

引数は、次のとおりです。

- *group_number* — VLAN グループの番号

- *vlan_range* — 以下のいずれかの形式で指定される、1 つまたは複数の VLAN（2 ～ 1000 および 1025 ～ 4094）
  - 1 つの数字（*n*）
  - 範囲（*n-x*）

  数字または範囲は、次のようにカンマで区切ります。

  ```
  5,7-10,13,45-100
  ```

たとえば、VLAN グループ 50 に 55 ～ 57 の範囲の VLAN、VLAN グループ 51 に 75 ～ 86 の範囲の VLAN、VLAN グループ 52 に VLAN 100 を割り当てて、3 つの VLAN グループを作成するには、次のように入力します。

```
Router(config)# svclc vlan-group 50 55-57
Router(config)# svclc vlan-group 51 70-85
Router(config)# svclc vlan-group 52 100
```

Cisco IOS ソフトウェアによる VLAN グループの ACE への割り当て

ACE は、VLAN グループが割り当てられてはじめてスーパーバイザ エンジンからトラフィックを受信できます。スーパーバイザ エンジンで Cisco IOS ソフトウェアを使用して VLAN グループを ACE に割り当てるには、コンフィギュレーション モードで **svc module** 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。

svc module *slot_number* **vlan-group** *group_number_range*

引数は、次のとおりです。

- *slot_number* — ACE が搭載されているスロット番号。EXEC モードで **show module** コマンドを使用すると、シャーシのスロット番号とモジュールを表示できます。ACE は、Card Type フィールドで Application Control Engine Module として表示されます。
- *group_number_range* — 以下のいずれかの形式で指定される、1 つまたは複数のグループ番号
  - 1 つの数字（*n*）
  - 範囲（*n-x*）

  数字または範囲は、次のようにカンマで区切ります。

  ```
  5,7-10
  ```

たとえば、VLAN グループ 50 と 52 をスロット 5 の ACE に、VLAN グループ 51 と 52 をスロット 8 の ACE に割り当てるには、次のように入力します。

```
Router(config)# svc module 5 vlan-group 50,52
Router(config)# svc module 8 vlan-group 51,52
```

ACE のグループ設定と、関連付けられている VLAN を確認するには、**show svclc vlan-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。

```
Router(config)# exit
Router# show svclc vlan-group
```

すべてのモジュールに対する VLAN グループ番号を表示するには、**show svc module** コマンドを使用します。たとえば、次のように入力します。

```
Router# show svc module
```

（注） スーパーバイザ エンジンからダウンロードされる ACE VLAN を表示するには、Admin コンテキストから EXEC モードで **show vlans** コマンドを入力します。

SVI の MSFC への追加

Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）で定義された VLAN を、Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）といいます。SVI に使用する VLAN を ACE に割り当てると、MSFC は ACE とその他のレイヤ 3 VLAN 間でルーティングを行います。デフォルトでは、SVI は MSFC と ACE の間に 1 つだけ設定できます。ただし複数のコンテキストがある場合は、各コンテキストで固有の VLAN に対して、複数の SVI を設定します。

SVI を MSFC に追加し、ACE に割り当てられた VLAN を SVI に設定する手順は次のとおりです。

ステップ 1　（任意）複数の SVI を ACE に追加する場合は、次のコマンドを入力します。

```
Router(config)# svclc multiple-vlan-interfaces
```

ステップ 2　VLAN インターフェイスを MSFC に追加します。たとえば、VLAN 55 を追加するには、次のコマンドを入力します。

```
Router(config)# interface vlan 55
```

ステップ 3　MSFC で、このインターフェイスの IP アドレスを設定します。たとえば、アドレス 10.1.1.1 255.255.255.0 を設定するには、次のコマンドを入力します。

```
Router(config-if)# ip address 10.1.1.1 255.255.255.0
```

ステップ 4　インターフェイスをイネーブルにします。たとえば、次のコマンドを入力します。

```
Router(config-if)# no shut
```

（注）　スーパーバイザ エンジンで、3 つ以上のトランク ポート、物理ポート、または物理トランクポートに関連付けられている VLAN をモニタするには、**svclc autostate** コマンドを使用して自動ステート機能をイネーブルにします。VLAN をこれらのポートに関連付けると、自動ステートにより、VLAN が up になったことが示されます。スーパーバイザ エンジンで VLAN ステートに変更が生じた場合、インターフェイスを up または down にするよう、自動ステートが ACE に通知します。

この SVI 設定を確認するには、**show 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。

```
Router# show int vlan 55
```

ユーザ コンテキストへの VLAN の割り当て

デフォルトで、ACE に割り当てられているすべての VLAN は、Admin コンテキストで使用できます。スーパーバイザ エンジンから ACE に割り当てられている VLAN を表示するには、Admin コンテキストから EXEC モードで **show vlans** コマンドを使用します。

まだ割り当てられていないコンテキストで VLAN を設定しようとすると、次のエラーメッセージが表示されます。

```
Error: invalid input parameter <<<<<<<<<<<<<
```

Admin コンテキストで、ユーザ コンテキストに VLAN を割り当てられます。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。

（注）　VLAN がスーパーバイザ エンジンから ACE に割り当てられていない場合でも、ACE により VLAN 番号をコンテキストに割り当てることができます。コンテキストでの VLAN 設定は可能ですが、スーパーバイザ エンジンから ACE への割り当てが完了するまで、この VLAN はトラフィックを受信できません。

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 VLAN に各コンテキストで異なる MAC アドレスを割り当てます。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 モジュール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 モジュールを設定して共有 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 に対して個々の MAC アドレス バンクを冗長構成で設定するには、Admin 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 インターフェイスに対する MAC アドレスの自動生成

デフォルトで、ACE は透過型ファイアウォール経由で 1 つのコンテキストから別のコンテキストへトラフィックを転送することができません。ACE は、VLAN が共有 VLAN でないかぎり、異なるコンテキストの VLAN は異なる レイヤ 2 のドメインにあるとみなします。ACE は同一の MAC アドレスを VLAN に割り当てます。

Firewall Services Module（FWSM）を利用し、ACE 上の 2 つのコンテキスト間でトラフィックをブリッジングする場合は、2 つのレイヤ 3 VLAN を同一のブリッジ ドメインに割り当てる必要があります。この設定を行うには、これらの VLAN インターフェイスにそれぞれ異なる MAC アドレスが割り当てられている必要があります。

VLAN インターフェイスに対する MAC アドレスの自動生成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 address autogenerate** 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。

mac address autogenerate

たとえば、次のように入力します。

```
host1/Admin(config-if)# mac address autogenerate
```

VLAN に対する MAC アドレスの自動生成をディセーブルにするには、**no mac address autogenerate** 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 address autogenerate
```

（注）　**mac address autogenerate** コマンドを使用すると、ACE によって、MAC アドレス バンクから MAC アドレスが共有 VLAN に割り当てられます。**no mac address autogenerate** コマンドを使用すると、インターフェイスのアドレスはそのまま維持されます。非共有 VLAN の MAC アドレスに戻すには、いったんインターフェイスを削除し、再びインターフェイスを追加する必要があります。

出力 MAC ルックアップのディセーブル化

ACE は通常、バックプレーンからパケットを受信する際と、出力インターフェイスへパケットを転送する際に MAC アドレス ルックアップを行います。Catalyst 6500 シリーズ スイッチまたは Cisco 7600 ルータに複数の ACE が搭載されている場合、トラフィック レートの高さから、予想よりもパフォーマンスが低くなる可能性があります。ACE の適正なパフォーマンスが得られない場合、コンフィギュレーション モードで **hw-module optimize-lookup** コマンドを使用して、出力 MAC アドレス ルックアップをディセーブルにできます。このコマンドの構文は次のとおりです。

hw-module optimize-lookup

（注）　Catalyst 6500 シリーズ スイッチまたは Cisco 7600 ルータで、Distributed Forwarding Card（DFC）がインテリジェント モジュールに取り付けられている場合は、このコマンドを使用しないでください。このコマンドを使用することで、これらのモジュールおよびスーパーバイザ上の Encoded Address Recognition Logic（EARL）ユニットが非同期になります。

たとえば、ACE ですべての出力 MAC アドレス ルックアップをディセーブルにするには、次のコマンドを入力します。

```
Admin/host1(config)# hw-module optimize-lookup
```

出力 MAC ルックアップを再びイネーブルにするには、次のコマンドを入力します。

```
Admin/host1(config)# no hw-module optimize-lookup
```

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、その属性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。VLAN 番号は、2 から 4094 の間で設定します。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） 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 を実行することができません。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。

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
- 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
- インターフェイスでの MTU の設定
- ピア IP アドレスの設定
- エイリアス IP アドレスの設定
- MAC スティッキ機能のイネーブル化

- インターフェイスの説明の設定
- UDP ブースター機能の設定
- インターフェイスへのポリシー マップの割り当て
- インターフェイスへのアクセス リストの適用

（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 モジュールに着信する場合、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 Application Control Engine Module Administration Guide*』を参照。
- デフォルトおよびスタティック ルート — 第 2 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 3 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 4 章「ARP の設定」を参照。
- Dynamic Host Configuration Protocol（DHCP）— 第 5 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 Application Control Engine Module 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 Application Control Engine Module 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 Application Control Engine Module 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 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）。

（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、次のように入力します。

```
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 を割り当て、ACL を動作させるには、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」を参照してください。ACL の設定の詳細については、『*Cisco Application Control Engine Module 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 Application Control Engine Module 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 **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

冗長構成の場合、スタンバイ モジュール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 モジュールで変更が発生すると、スタンバイ モジュールは自動的に同期します。ただし、アクティブ モジュールとスタンバイ 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 モジュール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 モジュールに同期させます。

スタンバイ モジュール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 モジュールのピア IP アドレスは、スタンバイ モジュール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 netmask*

ip_address netmask 引数は、ピア モジュールのアドレスとサブネット 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 モジュールの IP アドレスとネット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 モジュールの 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 モジュールおよびスタンバイ 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 モジュールで共有されるエイリアス IP アドレスを持つ 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 モジュール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 Application Control Engine Module Administration 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。ファイアウォールのロード バランシングの詳細については、『*Cisco Application Control Engine Module 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 Application Control Engine Module 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。

たとえば、「POLICY MAP 3 FOR INBOUND AND OUTBOUND TRAFFIC」という説明を設定するには、次のように入力します。

```
host1/Admin(config-if)# description POLICY MAP3 FOR INBOUND AND
OUTBOUND TRAFFIC
```

インターフェイスの説明を削除するには、**no description** 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 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 Application Control Engine Module 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 Application Control Engine Module 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。

インターフェイスにポリシー マップを割り当てるには、そのインターフェイスに対して、インターフェイス コンフィギュレーション モードで **service-policy** コマンドを使用するか、同一コンテキストのすべてのインターフェイスに対して、コンフィギュレーション モードで **service-policy** 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。

service-policy input *policy_name*

キーワードと引数は次のとおりです。

- **input —** インターフェイスのインバウンド方向にトラフィック ポリシーを割り当てるよう指定します。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* **—** インターフェイスに適用する設定済みポリシー マップ

たとえば、VLAN 3 へのインバウンド トラフィックに対して L4_SLB_POLICY というポリシー マップを割り当てるには、次のように入力します。

```
host1/Admin(config)# interface vlan 3
host1/Admin(config-if)# service-policy input L4_SLB_POLICY
```

インターフェイスからポリシー マップを削除するには、**no service-policy** 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 service-policy input L4_SLB_POLICY
```

すべてのポリシー マップまたは特定のポリシー マップに対するサービス ポリシー情報を表示するには、**show service-policy** 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 service-policy [*policy_name* [**detail**]]

コマンドにポリシー マップ名を指定しない場合、すべてのサービス ポリシーが表示されます。引数とオプションは次のとおりです。

- *policy_name* **—**（任意）表示する設定済みのポリシー マップ
- **detail —**（任意）説明情報を含めた、ポリシー マップに関する詳細情報を指定します。

表示される情報には、ポリシー マップ名、アクティブかどうか、サービス ポリシー名、クラス マップ名、およびインスペクション タイプ（該当する場合）が含まれます。

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 Application Control Engine Module 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
```

インターフェイス情報の表示

インターフェイスの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。

- VLAN および BVI 情報の表示
- VLAN および BVI の要約統計情報の表示

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 1-1 に、**show interface** コマンドの出力フィールドを示します。

表 1-1　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

表 1-1　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
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）
Assigned - Supervisor	VLAN または BVI がスーパーバイザ エンジンで割り当てられたものかどうか、およびスーパーバイザで up または down かを表示
# 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）
# 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

すべてのまたは特定の BVI または VLAN インターフェイス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 1-2 に、**show ip interface brief** コマンドの出力フィールドを示します。

表 1-2　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

EOBC 情報の表示

Ethernet out-of-band channel（EOBC）に関する情報を表示するには、EXEC モードで **show interface eobc** コマンドを使用します。このコマンドは、Admin コンテキストでのみ使用できます。たとえば、次のように入力します。

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

表 1-3 に、**show interface eobc** コマンドの出力フィールドを示します。

表 1-3　show interface eobc コマンドの出力フィールドの説明

フィールド	説明
Hardware type	ハードウェアのタイプは EOBC です
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
Description	VLAN の説明
MTU	MTU（バイト単位）
BW # bits/sec	バス幅（ビット / 秒）
IP address	内部 IP アドレス
# 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
# input errors, # ignored	着信パケットのエラー数（無視されたパケット数を含む）
# 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
# output errors, # ignore	発信パケットのエラー数（無視されたパケット数を含む）

ここで説明する内容は、次のとおりです。

- 内部インターフェイス マネージャ テーブルの表示
- スーパーバイザ エンジンからダウンロードされた ACE の VLAN の表示
- プライベート VLAN 情報の表示

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、Admin 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 Application Control Engine Module 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
```

スーパーバイザ エンジンからダウンロードされた ACE の VLAN の表示

スーパーバイザ エンジンからダウンロードされた ACE の VLAN を表示するには、Admin コンテキストから EXEC モードで **show vlans** 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# show vlans
Vlans configured on SUP for this module
    vlan192-193 vlan333
```

プライベート VLAN 情報の表示

Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータのプライベート VLAN 機能は、ACE と連携して動作します。Cisco IOS での PVLAN 設定により、ACE に PVLAN マッピング データベースが設定されます。詳細については、スイッチまたはルータのマニュアルを参照してください。

スーパーバイザ エンジンからダウンロードされた ACE のプライベート VLAN を表示するには、EXEC モードで **show pvlans** 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# show pvlans
```

表 1-4 に、**show pvlans** コマンドの出力フィールドを示します。

表 1-4　show pvlans コマンドの出力フィールドの説明

フィールド	説明
Primary	プライマリ プライベート VLAN の VLAN 番号
Secondary	セカンダリ プライベート VLAN の VLAN 番号
Type	プライベート VLAN での VLAN の 3 つの利用方法のうちの 1 つ：primary、isolated、community

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 モジュールの統計情報しかクリアしないと、スタンバイ モジュールの統計情報は古い値のまま残ります。