CHAPTER 2

ACE のルート設定

この章では、ACE をルーテッド モードにして、ネットワーク内でルータ ホップとして認識されるようにする方法について説明します。Admin コンテキストまたはユーザ コンテキストの場合、ACE はスタティック ルートのみをサポートします。また、ACE では最大 8 つの等価コスト ルートでロード バランシングを実行できます。

この章では、ACE にデフォルト ルートまたはスタティック ルートを設定する方法について説明します。この章の主な内容は、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
- デフォルト ルートまたはスタティック ルートの設定
- デフォルト ルートまたはスタティック ルートの削除
- RHI のための VLAN のアドバタイズ
- リモート ホストまたはサーバの接続性の確認
- IP ルート情報の表示
- FIB テーブル情報の表示

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

インターフェイスに IP アドレスを割り当てると、インターフェイスは自動的にルーテッド モードになります。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。

（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。

ACE が単一のコンテキスト（Admin）で動作している場合、各インターフェイスアドレスを一意のサブネットに設定する必要があります。ACE が複数のコンテキストで動作しており、インターフェイスが共有 VLAN に属している場合、IP アドレスは一意のものにする必要があり、共有 VLAN 内の別のコンテキストで使用することはできません。共有 VLAN でない場合、IP アドレスは他のコンテキストで使用することができます。

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）を設定する必要があります。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、インターフェイス VLAN 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。ACL 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。

デフォルト ルートまたはスタティック ルートの設定

Admin コンテキストおよびユーザ コンテキストでは、ダイナミック ルーティングはサポートされません。ACE と直接接続していないネットワークに対しては、スタティック ルートを使用する必要があります。たとえば、ネットワークと ACE の間にルータがある場合、スタティック ルートを使用する必要があります。

ACE から発信されるトラフィックまたは ACE を介してルーティングされるトラフィックで、直接接続されていないネットワークを宛先とするものについては、ACE でトラフィックの送信先を判別できるようデフォルト ルートまたはスタティック ルートを設定します。ACE から発信されるトラフィックには、Syslog サーバ、Websense または N2H2 サーバ、AAA サーバへの通信が含まれます。

最も単純なオプションは、デフォルト ルートを設定して、1 台の上流のルータにすべてのトラフィックを送信する方法です。ACE がルートを持たないすべての IP パケットは、デフォルト ルートで指定されるルータの IP アドレスに送信されます。

（注） 特定の宛先アドレスが指定されたルートは、デフォルト ルートより優先されます。

デフォルト ルートまたはスタティック ルートを設定するには、コンフィギュレーション モードで **ip route** 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 route *dest_ip_prefix netmask gateway_ip_address*

キーワード、引数、およびオプションは次のとおりです。

- *dest_ip_prefix* ― ルートの IP アドレス。ドット付き 10 進表記で IP アドレスを入力します（たとえば、192.168.20.1）。
- *netmask* ― ルートのサブネット マスク。ドット付き 10 進表記でサブネット マスクを入力します（たとえば、255.255.255.0）。

- *gateway_ip_address* — ゲートウェイ ルータの IP アドレス（このルートのネクストホップ アドレス）。ゲートウェイのアドレスは、**ip address** コマンドで VLAN インターフェイスに指定したネットワークと同じネットワークに属している必要があります。アドレスの設定方法の詳細については、「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」を参照してください。

（注）　ACE に着信する管理トラフィックは、**no normalization** コマンド（非対称ルートをサポートしない）の影響を受けません。正規化の詳細については、『*Cisco Application Control Engine Module Security Configuration Guide*』を参照してください。

たとえば、宛先が 10.1.1.0/24 のすべてのトラフィックをルータ（10.1.2.45）に送信するスタティック ルートを設定するには、次のように入力します。

```
host1/Admin(config)# ip route 10.1.1.0 255.255.255.0 10.1.2.45
```

デフォルト ルートを設定するには、ルートの IP アドレスとサブネット マスクを 0.0.0.0 に設定します。たとえば、ACE がルートのないトラフィックを受信した場合に、ACE のインターフェイスから 192.168.4.8 のルータにトラフィックが送信されるようにするには、次のように入力します。

```
host1/Admin(config)# ip route 0.0.0.0 255.255.255.0 192.168.4.8
```

デフォルト ルートまたはスタティック ルートの削除

設定からデフォルト IP ルートまたはスタティック IP ルートを削除するには、**ip route** コマンドの **no** 形式を使用します。たとえば、次のように入力します。

```
host1/Admin(config)# no ip route 192.168.42.0 255.255.255.0
192.168.1.5 1
```

RHI のための VLAN のアドバタイズ

VIP インターフェイス VLAN と異なる VLAN を Route Health Injection（RHI）のためにアドバタイズするには、インターフェイス コンフィギュレーション モードで **ip route inject vlan** コマンドを使用します。デフォルトでは、ACE は RHI のために VIP インターフェイスの VLAN をアドバタイズします。

ACE と Catalyst 6500 シリーズ スーパーバイザ エンジンの間で直接共有する VLAN がない場合に、このコマンドを使用します。このようなトポロジに該当するのは、ACE とスーパーバイザ エンジンの間に Cisco Firewall Services Module（FWSM）などのデバイスが介在する構成の場合です。

（注） このコマンドは、必ず ACE の VIP インターフェイスに設定してください。

このコマンドの構文は次のとおりです。

ip route inject vlan *vlan_id*

vlan_id は、スーパーバイザ エンジンと介在しているデバイスで共有するインターフェイスです。2 ～ 4090 の整数値を入力します。

たとえば、RHI のためにルート 200 をアドバタイズするには、次のように入力します。

```
host1/Admin(config-if)# ip route inject vlan 200
```

ACE のデフォルトの動作に戻し、RHI のために VIP インターフェイス VLAN をアドバタイズするには、次のように入力します。

```
host1/Admin(config-if)# no ip route inject vlan 200
```

リモート ホストまたはサーバの接続性の確認

EXEC モードで **ping** コマンドを使用して ACE からエコー メッセージを送信することで、リモート ホストまたはサーバの接続性を確認できます。

このコマンドの構文は次のとおりです。

ping *system_address*

system_address 引数は、ping を送信するリモート ホストまたはサーバの IP アドレスです。ドット付き 10 進表記で IP アドレスを入力します（たとえば、172.27.16.10）。

次に、IP アドレスが 192.168.219.140 のサーバに ping を送信する例を示します。

```
host1/Admin# ping 192.168.173.140
PING 192.168.173.140 with timeout = 2, count = 5, size = 100
Response from 192.168.173.140 :  seq 1 time 1.213 ms
Response from 192.168.173.140 :  seq 2 time 0.175 ms
Response from 192.168.173.140 :  seq 3 time 0.210 ms
Response from 192.168.173.140 :  seq 4 time 0.162 ms
Response from 11.1.11.4 :  seq 5 time 0.214 ms
5 packet sent, 5 responses received, 0% packet loss
```

ping セッションを強制的に終了するには、**Ctrl-C** を押します。

（注） リモート ホストまたはサーバの MAC アドレスが ARP テーブルに入力されていないために、最初の ping は失敗する場合があります。

ping コマンドには、リモート ホストまたはサーバの接続性を確認するための追加オプションがあります。これらの追加パラメータを指定するには、CLI の ACE プロンプトで **ping** と入力して Enter キーを押します。

表 2-1 に、**ping** コマンドのオプションとデフォルトの要約を示します。

表 2-1　ping コマンドのオプションとデフォルト

オプション	説明	デフォルト
Target IP address	ping を送信する宛先ノードの IP アドレスまたはホスト名	該当なし
Repeat count	宛先アドレスに送信する ping パケットの数	5 パケット
Datagram size	各 ping パケットのサイズ（バイト単位）	100 バイト
Timeout in seconds	ping 要求が失敗したと判断されるまでのタイムアウト間隔。ping は中断されず、次の ping パケット（存在する場合）が送信されます。	2 秒
Extended commands	一連の追加コマンドを表示するかを指定	なし
Source address or interface	送信元インターフェイスの IP アドレス（数字）または名前	該当なし
Set DF bit in IP header	パス内での MTU 検出手段	なし
Time to Live	ping パケットが廃棄されるまでの存続期間を決める、IP ヘッダーの Time To Live（TTL; 存続可能期間）フィールドの値。TTL 値は、ホップごとに 1 減ります。	128

特定の IP アドレスへのルートをトレースするには、EXEC モードで **traceroute** 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。

traceroute [*ip_address* [**size** *packet*]]

引数とオプションは次のとおりです。

- *ip_address* **—** ルートの IP アドレス。ドット付き 10 進表記で IP アドレスを入力します（たとえば、172.27.16.10）。この引数をコマンドと一緒に指定しなくても問題はありませんが、IP アドレスを入力するよう指示されます。
- **size** *packet* **—**（任意）パケット サイズを指定します。40 ～ 452 の数値を入力します。デフォルト値は 40 です。

たとえば、IP アドレス 192.168.173.140 をトレースするには、次のように入力します。

```
host1/Admin# traceroute 192.168.173.140
traceroute to 192.168.173.140 (192.168.173.140), 30 hops max, 40 byte
packets
 1  192.86.215.2 (192.86.215.2)  0.558 ms  0.325 ms  0.297 ms
 2  * * *
 3  * * *
```

traceroute セッションを終了するには、**Ctrl-C** を押します。

ACE に設定された IP アドレスに対する traceroute の使用

ACE に設定された IP アドレスに対して traceroute を使用することはできますが、いくつかの制限があります。ACE に設定された IP インターフェイスに対して traceroute を使用する場合、以下に注意してください。

- 次の例のように、ICMP トラフィックを許可する管理ポリシーを設定しないと、ICMP traceroute は機能しません。

```
class-map type management match-any remote-access
    description remote-access-traffic-match
    match protocol icmp any
```

（注） ほとんどの traceroute ではデフォルトのプロトコルである UDP を使用します。traceroute を ICMP に変更するには、コマンドライン オプションを使用します。たとえば、Linux では -I オプションを使用します。

- UDP または TCP ベースの traceroute は機能しません。ACE への一時的なポートで UDP または TCP トラフィックを許可する方法はありません。

ACE の背後にあるホストに対して UDP、TCP、または ICMP ベースの traceroute を使用する場合は、予期したとおりに機能します。ただし、ACE は traceroute でホップとして表示されません。ACE によって、転送する IP パケットの TTL は減りません。

ACE に設定された VIP アドレスに対して traceroute を使用する場合、ACE は VIP アドレスに送信される traceroute パケットを代行受信しません。ACE は、パケットをロード バランス ポリシーと照合します。プロトコルの一致がある場合、ACE は traceroute に適宜応答する実サーバへパケットを送信します。

IP ルート情報の表示

ACE に設定された IP ルートを表示するには、EXEC モードで **show ip route** 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 ip route
```

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

表 2-2　show ip route コマンドの出力フィールドの説明

フィールド	説明
Destination	ルートの宛先アドレス
Gateway	ルートのゲートウェイ アドレス
Interface	このエントリの VLAN インターフェイス番号
Flag	ルートの種類と状態を識別するフラグ。次のいずれかのコードが出力情報の上に表示されます。 • H はホスト ルートを表します。 • I はインターフェイス ルートを表します。 • S はスタティック ルートを表します。 • N は NAT ルートを表します。 • A はルートで ARP 解決が必要であることを表します。 • E は ECMP ルートを表します。

現在のコンテキストのルート要約情報を表示するには、**show ip route summary** 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 ip route summary
```

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

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

フィールド	説明
Route Source	ルートの発信元。出力される値は次のとおりです。 • Connected　は同じネットワークに接続されたホストへのルートを表します。 • Static は設定されたルートを表します。
Count	接続されたルートまたはスタティック ルートの数
Memory (bytes)	ルート エントリによって消費されるメモリ

IP トラフィック情報を表示するには、EXEC モードで **show ip traffic** 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 traffic

たとえば、次のように入力します。

```
host1/Admin# show ip traffic
```

表 2-4 に **show ip traffic** コマンドの出力フィールドを示します。

表 2-4　show ip traffic コマンドの出力フィールドの説明

フィールド	説明
IP Statistics	
Rcvd	ACE が受信した総パケット数、ACE が受信した総バイト数、入力エラー数、ACE が受信したルートのないパケット数、ACE が受信したプロトコルの不明なパケット数
Frags	ACE が再構成したフラグメント数、ACE が再構成できなかったフラグメント数、ACE がフラグメント化したパケット数、ACE がフラグメント化できなかったパケット数
Bcast	送受信されたブロードキャスト パケット数
Mcast	送受信されたマルチキャスト パケット数

表 2-4　show ip traffic コマンドの出力フィールドの説明（続き）

フィールド	説明
Sent	送信された総パケット数、送信されたバイト数、送信されたルートのないパケット数
Drop	ルートがないために廃棄されたパケット数および廃棄されたパケット数
ICMP Statistics	
Rcvd	ACE が受信した以下の ICMP メッセージに関する統計情報のレポート • リダイレクト • ICMP 到達不能 • ICMP エコー • ICMP エコー応答 • マスク要求 • マスク応答 • 抑制 • パラメータ • タイムスタンプ
Sent	ACE が送信した以下の ICMP メッセージに関する統計情報のレポート • リダイレクト • ICMP 到達不能 • ICMP エコー • ICMP エコー応答 • マスク要求 • マスク応答 • 抑制 • タイムスタンプ • パラメータ • 超過時間

表 2-4　show ip traffic コマンドの出力フィールドの説明（続き）

フィールド	説明
TCP Statistics	
Rcvd	ACE が受信した TCP セグメントとエラーの総数
Sent	ACE が送信した TCP セグメントの総数
UDP Statistics	
Rcvd	ACE が受信した UDP セグメント、UDP エラー、ポート番号のないセグメントの総数
Sent	ACE が送信した UDP セグメントの総数
ARP Statistics	
Rcvd	ACE が受信した ARP パケット、エラー、要求、応答の数
Sent	ACE が送信した ARP パケット、エラー、要求、応答の数

show ip route 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。

FIB テーブル情報の表示

Forwarding Information Base（FIB; 転送情報ベース）テーブルには、転送プロセッサが IP 転送の判断を行うのに必要な情報が含まれています。このテーブルは、ルート テーブルと ARP テーブルを基に構築されます。コンテキストの FIB テーブルを表示するには、**show ip fib** 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 ip fib
```

表 2-5 に **show ip fib** コマンドの出力フィールドを示します。

表 2-5　show ip fib コマンドの出力フィールドの説明

フィールド	説明
Destination	ルートの宛先アドレス
Interface	このエントリの VLAN インターフェイス番号
EncapID	カプセル化 ID
Flag	ルートの種類と状態を識別するフラグ。次のいずれかのコードが出力情報の上に表示されます。 • H はホスト ルートを表します。 • I はインターフェイス ルートを表します。 • S はスタティック ルートを表します。 • N は NAT ルートを表します。 • A はルートで ARP 解決が必要であることを表します。 • E は ECMP ルートを表します。

コンテキストの FIB テーブルの要約を表示するには、**show ip fib summary** 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 ip fib summary
```

表 2-6 に **show ip fib summary** コマンドの出力フィールドを示します。

表 2-6　show ip fib summary コマンドの出力フィールドの説明

フィールド	説明
Resolved routes	mtrie に組み込まれたプレフィクスの数
Leaves, bytes	割り当てられた mtrie リーフ ノードの数と消費されたメモリ（バイト単位）
Nodes, bytes	割り当てられた mtrie 内部ノードの数と消費されたメモリ（バイト単位）
ecmps, bytes	割り当てられた ECMP ノードの数と消費されたメモリ（バイト単位）

show ip fib 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。