CHAPTER 4

ARP の設定

この章では、ACE 上で Address Resolution Protocol（ARP; アドレス解決プロトコル）を使用して IP-to-MAC 情報のマッピングを管理および学習し、パケットの転送および送信を行う方法について説明します。ACE は、ARP パケットを受信するか、または ACE 上に IP アドレス（実サーバ、ゲートウェイ、またはインターフェイス VLAN 用の IP アドレスなど）が設定された場合、ARP キャッシュ エントリを作成します。

IP-to-MAC 変換および ARP インスペクション用のスタティック ARP エントリを設定して ARP スプーフィングを防止することもできます。ARP インスペクションを使用すると、正しい MAC アドレスおよび関連付けられた IP アドレスがスタティック ARP テーブル内にある場合、攻撃者は自身の MAC アドレスを使用して ARP 応答を送信することができなくなります。

この章では、ARP パラメータの設定方法および ARP インスペクションのイネーブル化について説明します。主な内容は、次のとおりです。

- スタティック ARP エントリの追加
- ARP インスペクションのイネーブル化
- ARP 再試行回数の設定
- ARP 再試行間隔の設定
- ARP 要求間隔の設定
- MAC アドレス学習のイネーブル化
- 送信元 MAC 検証のイネーブル化
- ARP 学習間隔の設定

- ARP エントリの複製のディセーブル化
- ARP 同期メッセージの時間間隔の指定
- gratuitous ARP パケットのレート リミットの設定
- ARP 情報の表示
- ARP テーブルからの ARP 学習済みエントリのクリア
- ARP 統計情報のクリア

スタティック ARP エントリの追加

ARP テーブル内にスタティック ARP エントリを追加するには、コンフィギュレーション モードまたはインターフェイス コンフィギュレーション モードで **arp** コマンドを使用します。コンテキスト レベルでスタティック ARP エントリを作成できます。ブリッジド インターフェイスでは、インターフェイス コンフィギュレーション モードでスタティック ARP エントリを設定する必要があります。

（注） ARP インスペクションをイネーブルにすると、ACE は ARP パケットと ARP テーブル内のスタティック ARP エントリを比較して取るべき対応を決定します。詳細については、「ARP インスペクションのイネーブル化」を参照してください。

このコマンドの構文は次のとおりです。

arp *ip_address mac_address*

引数は、次のとおりです。

- *ip_address* — ARP テーブル エントリの 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、172.16.56.76）。
- *mac_address* — ARP テーブル エントリのハードウェア MAC アドレス。ドット付き 16 進表記で MAC アドレスを入力します（たとえば、00.60.97.d5.26.ab）。

たとえば、00.02.9a.3b.94.d9 という MAC アドレスを持つルータ（10.1.1.1）からの ARP 応答を許可するには、次のコマンドを入力します。

```
host1/Admin(config)# arp 10.1.1.1 00.02.9a.3b.94.d9
```

スタティック ARP エントリを削除するには、**no arp** 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 arp 10.1.1.1 00.02.9a.3b.94.d9
```

ARP インスペクションのイネーブル化

ARP インスペクションを使用すると、悪意のあるユーザがその他のホストまたはルータになりすます ARP スプーフィングを防止できます。ARP スプーフィングは「man-in-the-middle」攻撃を引き起こします。たとえば、ホストがゲートウェイ ルータに ARP 要求を送信します。ゲートウェイ ルータは、ゲートウェイ ルータ MAC アドレスを使用して応答します。

しかし、攻撃者は、ルータ MAC アドレスではなく、攻撃者自身の MAC アドレスを使用して、ホストに別の ARP 応答を送信します。これにより、攻撃者はホストのトラフィックすべてを、ルータに転送される前に代行受信できます。ARP インスペクションを使用すると、正しい MAC アドレスおよび関連付けられた IP アドレスがスタティック ARP テーブル内にある場合、攻撃者が自身の MAC アドレスを使用して ARP 応答を送信することができなくなります。

ARP インスペクションは入力ブリッジド インターフェイス上でのみ動作します。デフォルトでは、ARP インスペクションはすべてのインターフェイス上でディセーブルです。このため、すべての ARP パケットは ACE を通過します。ARP インスペクションをイネーブルにすると、ACE は ARP テーブルへのインデックスとして着信 ARP パケットの IP アドレスおよびインターフェイス ID（ifID）を使用します。ACE は ARP パケットの MAC アドレスと ARP テーブル内のインデックス付きスタティック ARP エントリの MAC アドレスを比較して、次のように対応します。

- IP アドレス、送信元 ifID、および MAC アドレスがスタティック ARP エントリと一致する場合、インスペクションは成功となり、ACE はパケットの通過を許可します。
- 着信 ARP パケットの IP アドレスおよびインターフェイスがスタティック ARP エントリと一致するが、パケットの MAC アドレスがそのスタティック ARP エントリで設定した MAC アドレスと一致しない場合、ARP インスペクションは失敗となり、ACE はパケットをドロップし、**flood** または **no-flood** オプションの設定の有無にかかわらず Inspect Failed カウンタを増分します。

- ARP パケットが ARP テーブル内にあるスタティック エントリのいずれとも一致しない場合やテーブル内にスタティック エントリが存在しない場合は、パケットをすべてのインターフェイスから転送する（**flood**）か、またはパケットをドロップする（**no-flood**）ように ACE を設定できます。この場合、送信元 IP アドレスと MAC アドレスの新しいマッピングが ACE に適用されます。**flood** オプションを入力した場合、ACE は新しい ARP エントリを作成し、それを LEARNED としてマーキングします。**no-flood** オプションを指定すると、ACE は ARP パケットをドロップします。

ARP インスペクションをイネーブルにするには、コンフィギュレーション モードで **arp inspection enable** 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。

arp inspection enable [**flood** | **no-flood**]

オプションは、次のとおりです。

- **flood —** 一致しない ARP パケットの ARP 転送をイネーブルにします。ACE は、ブリッジ グループ内のすべてのインターフェイスにすべての ARP パケットを転送します。これがデフォルトの設定です。スタティック ARP エントリが存在しない場合にこのオプションが指定されていると、すべてのパケットがブリッジングされます。このオプションでは、ACE は **show arp statistics** コマンドの Inspect Failed カウンタを増分しません。
- **no-flood —** インターフェイスでの ARP 転送をディセーブルにし、一致しない ARP パケットをドロップします。スタティック ARP エントリが存在しない場合にこのオプションが指定されていると、すべてのパケットがブリッジングされません。このオプションでは、ACE は **show arp statistics** コマンドの Inspect Failed カウンタを増分します。

たとえば、ARP インスペクションをイネーブルにし、一致しない ARP パケットをすべてドロップするには、次のように入力します。

```
host1/Admin(config)# arp inspection enable no-flood
```

ARP をディセーブルにするには、**no arp inspection 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)# no arp inspection enable
```

ARP 再試行回数の設定

デフォルトでは、ACE が学習および設定済みホストにダウンというフラグを付けるまでに ARP を試行する回数は 3 回です。ARP 再試行回数を設定するには、コンフィギュレーション モードで **arp retries** コマンドを使用します。このコマンドはコンテキストごとに設定します。このコマンドの構文は次のとおりです。

arp retries *number*

number 引数は、ARP 再試行回数です。2 ～ 15 の値を入力します。デフォルト値は 3 です。

たとえば、再試行回数を 6 回に設定するには、次のように入力します。

```
host1/Admin(config)# arp retries 6
```

ARP 再試行回数をデフォルトの 3 回にリセットするには、**no arp retries** 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 arp retries
```

ARP 再試行間隔の設定

デフォルトでは、ACE が学習および設定済みホストに ARP 再試行を送信する間隔は 10 秒です。間隔を設定するには、コンフィギュレーション モードで **arp rate** コマンドを使用します。このコマンドはコンテキストごとに設定します。このコマンドの構文は次のとおりです。

arp rate *seconds*

seconds 引数は、ホストに対する ARP 再試行の間隔（秒）です。1 ～ 60 の値を入力します。デフォルト値は 10 です。

たとえば、再試行間隔を 15 秒に設定するには、次のように入力します。

```
host1/Admin(config)# arp rate 15
```

ARP 再試行間隔をデフォルトの 10 秒にリセットするには、**no arp rate** 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 arp rate
```

ARP 要求間隔の設定

デフォルトでは、設定済みホスト アドレスの既存の ARP エントリをリフレッシュする間隔は 300 秒です。間隔を設定するには、コンフィギュレーション モードで **arp interval** コマンドを使用します。このコマンドはコンテキストごとに設定します。このコマンドの構文は次のとおりです。

arp interval *seconds*

seconds 引数は、ホストに送信された各 ARP 要求の間隔（秒）です。15 ～ 31536000 の値を入力します。デフォルト値は 300 です。

たとえば、要求間隔を 15 秒に設定するには、次のように入力します。

```
host1/Admin(config)# arp interval 15
```

ARP 要求間隔をデフォルトの 300 秒にリセットするには、**no arp interval** 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 arp interval
```

MAC アドレス学習のイネーブル化

デフォルトでは、ACE はブリッジングされたすべてのトラフィックについて MAC アドレスを学習します。ルーティングされたトラフィックについては、ACE は ARP 応答パケットから、または ACE 宛てのパケット（VIP や VLAN インターフェイスへの ping など）からのみ MAC アドレスを学習します。コマンドがディセーブルにされたあとで ACE がトラフィックから MAC アドレスを学習するように設定するには、コンフィギュレーション モードで **arp learned-mode enable** コマンドを使用します。このコマンドはコンテキストごとに設定します。このコマンドはデフォルトでイネーブルです。

このコマンドの構文は次のとおりです。

arp learned-mode enable

コマンドがディセーブルにされたあとで ACE がトラフィックから MAC アドレスを学習するように設定するには、次の例のように入力します。

```
host1/Admin(config)# arp learned-mode enable
```

ACE が ARP 情報を学習せずにパケットを転送するように設定するには、**no arp learned-mode 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)# no arp learned-mode enable
```

送信元 MAC 検証のイネーブル化

送信元 MAC の検証を使用すると、特定のインターフェイスで ACE が受信したすべての ARP パケットの ARP ペイロード内にある送信者の MAC アドレスに対して、イーサネット ヘッダー内の送信元 MAC アドレスをチェックするように ACE を設定できます。ACE は、異なる MAC アドレスを使用するパケットの ARP テーブルまたは MAC テーブルについては、学習およびアップデートを行いません。デフォルトでは、送信元 MAC の検証はディセーブルです。

（注）　ARP インスペクションが失敗した場合、ACE は送信元 MAC の検証を行いません。ARP インスペクションの詳細については、「ARP インスペクションのイネーブル化」を参照してください。

送信元 MAC の検証を設定するには、インターフェイス コンフィギュレーション モードで **arp inspection** 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。

arp inspection validate src-mac [**flood** | **no-flood**]

オプションは、次のとおりです。

- **flood** — インターフェイスでの ARP 転送をイネーブルにし、一致しない送信元 MAC アドレスを持つ ARP パケットをブリッジ グループ内のすべてのインターフェイスに転送します。これは、送信元 MAC の検証をイネーブルにした場合のデフォルトのオプションです。
- **no-flood** — インターフェイスでの ARP 転送をディセーブルにし、一致しない送信元 MAC アドレスを持つ ARP パケットをドロップします。

（注）　**flood** オプションまたは **no-flood** オプションの入力の有無にかかわらず、ARP パケットの送信元 MAC アドレスがイーサネット ヘッダーの MAC アドレスと一致しない場合、送信元 MAC の検証は失敗し、ACE は **show arp statistics** コマンドの Smac-validation Failed カウンタを増分します。

たとえば、送信元 MAC の検証をイネーブルにして、一致しない送信元 MAC アドレスを持つ ARP パケットをドロップするように ACE を設定するには、次のコマンドを入力します。

```
host1/Admin(config-if)# arp inspection validate src-mac no-flood
```

送信元 MAC の検証をディセーブルにするには、次のコマンドを入力します。

```
host1/Admin(config-if)# no arp inspection validate src-mac no-flood
```

ARP 学習間隔の設定

デフォルトでは、学習済みホスト アドレスの既存の ARP エントリをリフレッシュする間隔は 14400 秒です。間隔を設定するには、コンフィギュレーション モードで **arp learned-interval** コマンドを使用します。このコマンドはコンテキストごとに設定します。このコマンドの構文は次のとおりです。

arp learned-interval *seconds*

seconds 引数は、学習済みアドレスに対する ARP 要求の間隔（秒）です。60 ～ 31536000 の値を入力します。デフォルト値は 14400 です。

たとえば、学習間隔を 800 秒に設定するには、次のように入力します。

```
host1/Admin(config)# arp learned-interval 800
```

学習間隔をデフォルトの 14400 秒にリセットするには、**no arp learned-interval** 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 arp learned-interval
```

ARP エントリの複製のディセーブル化

デフォルトでは、ARP エントリの複製はイネーブルです。ARP エントリの複製をディセーブルにするには、コンフィギュレーション モードで **arp sync disable** 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。

arp sync disable

たとえば、ARP エントリの複製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)# arp sync disable
```

ARP エントリの複製を再びイネーブルにするには、**no arp sync disable** 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 arp sync disable
```

ARP 同期メッセージの時間間隔の指定

デフォルトでは、学習済みホストに対する ARP 同期メッセージの時間間隔は 5 秒です。時間間隔を指定するには、コンフィギュレーション モードで **arp sync-interval** 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。

arp sync-interval *number*

number 引数は、時間間隔を定義します。1 ～ 3600 秒（1 時間）までの整数値を入力します。デフォルトは 5 秒です。

たとえば、時間間隔を 100 秒に設定するには、次のように入力します。

```
host1/Admin(config)# arp sync-interval 100
```

デフォルト値の 5 秒に戻すには、**no arp sync-interval** 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 arp sync-interval
```

gratuitous ARP パケットのレート リミットの設定

デフォルトでは、ACE が送信する gratuitous ARP のレート リミットは 512 パケット / 秒（pps）です。レート リミットを設定するには、コンフィギュレーション モードで **arp ratelimit** 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有効です。レート リミットは、コンテキストごとではなく、モジュールに適用されます。

このコマンドの構文は次のとおりです。

arp ratelimit *number*

number 引数は、レート リミットを pps で定義します。100 ～ 8192 の整数値を入力します。デフォルト値は 512 です。

（注） レート リミットは、新しい設定、モジュールのリブート、および MAC アドレスの変更の際にローカル アドレスに送信されるすべての gratuitous ARP に適用されます。

たとえば、レート リミットを 1000 pps に設定するには、次のように入力します。

```
host1/Admin(config)# arp ratelimit 1000
```

デフォルト値の 512 pps に戻すには、**no arp ratelimit** 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 arp ratelimit
```

ARP 情報の表示

ARP のアドレス マッピング、統計情報、およびタイムアウト間隔を表示できます。詳細については、次のトピックを参照してください。

- IP-to-MAC アドレス マッピングの表示
- ARP 統計情報の表示
- ARP インスペクションの設定の表示
- ARP タイムアウト値の表示

（注）　**show arp 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。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。

IP-to-MAC アドレス マッピングの表示

ARP テーブル内の現在アクティブな IP-to-MAC アドレス マッピングを表示するには、EXEC モードで **show arp** 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 arp

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

表 4-1　show arp コマンドの出力フィールドの説明

フィールド	説明
Context	現在のコンテキスト
IP ADDRESS	ARP マッピングに使用するシステムの IP アドレス
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
Interface	このエントリのインターフェイス名
Type	ARP エントリのタイプ。出力されるタイプは LEARNED、GATEWAY、INTERFACE、VSERVER、RSERVER、および NAT です。

表 4-1　show arp コマンドの出力フィールドの説明（続き）

フィールド	説明
Encap	このホストに対する隣接エントリのポインタ（存在する場合）。レイヤ 2 およびスイッチ ヘッダーの書き換え情報
Next ARP(s)	このダイナミック ARP エントリが有効な時間（秒）
Status	システムのステータス。出力される値は up または down です。

たとえば、次のように入力します。

```
host1/admin# show arp
```

ARP 統計情報の表示

グローバルに、または特定の VLAN に関して ARP 統計情報を表示するには、EXEC モードで **show arp statistics** 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 arp statistics [**vlan** *vlan_number*]

オプションの *vlan_number* 引数を指定すると、特定の VLAN の ARP 統計情報が表示されます。このオプションを指定せずにこのコマンドを使用した場合、すべての VLAN インターフェイスの ARP 統計情報が表示されます。

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

表 4-2　show arp statistics コマンドの出力フィールドの説明

フィールド	説明
RX Packets	受信した ARP パケット
RX Errors	受信した ARP パケットでのエラー数
TX Packets	送信した ARP パケット
TX Errors	送信した ARP パケットでのエラー数
Bridged Packets	ブリッジングされた ARP パケットの数
Bridged Errors	ブリッジングされたエラーの数
Requests Recvd	受信した ARP 要求

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

フィールド	説明
Requests Sent	送信した ARP 要求の数
Response Recvd	受信した ARP 応答
Response Sent	送信した ARP 応答の数
Packets Dropped	ドロップされた ARP パケットの数
Inspect Failed	ARP インスペクションに失敗したパケットの数
Collision Detected	検出されたコリジョンの数
Gratuitous ARP sent	送信した gratuitous ARP パケットの数
Hosts learned	学習済みホストの数
Smac-validation failed	イーサネット ヘッダー内の送信元 MAC アドレスと、受信した ARP パケットの ARP ペイロード内にある送信者の MAC アドレスとの不一致を ACE が検出した回数
Resolution requests	解決要求の数
Encap-miss msg	一致する ARP エントリがまったく含まれないパケットの数。学習済み ARP エントリはそれぞれ Encap に対応する必要があります。一致するエントリがパケットに含まれない場合、ACE では Encap の不整合とみなします。
Pings attempted for Encap-miss msg	既存のブリッジ グループのサブネット上にはない宛先パケット IP アドレスに対する Encap の不整合が発生した場合に ACE が ping を試行する必要があると認識する回数
Pings quenched for Encap-miss msg	ある宛先パケット IP アドレスに対する Encap の不整合が非常に短い間隔で繰り返し発生する場合に、その宛先パケット IP アドレスに対する ping の試行を ACE が抑制する回数
Pings rejected for Encap-miss msg	ある宛先 IP アドレスに対する Encap の不整合が多過ぎる場合に、その宛先 IP アドレスに対する ping の試行を ACE が拒否する回数。クエンチされる ping と似ていますが、これらは独自の不整合です。

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

フィールド	説明
Pings Encap-miss responded to	不整合が発生した IP アドレスに送信された実際の ping の数。このカウンタに表示される数は、Encap-miss msg カウンタで試行された ping の数と一致している必要があります。
Replication Counters	
Msg Received	スタンバイ ACE が受信した ARP 複製メッセージの数
Hosts Replicated	ARP 複製が成功し、エントリがスタンバイ上で作成されたホストの数
Replication Failed	スタンバイ ACE 上で複製が失敗したホストの数
Replication Ignored	エントリがすでに存在する可能性があるため、スタンバイ上で複製メッセージが無視されたホストの数

たとえば、次のように入力します。

```
host1/admin# show arp statistics
```

show ip traffic コマンドを使用すると、ARP トラフィックの統計情報を表示することもできます。このコマンドを使用すると、受信および送信されたパケットの数、関連エラー、要求、および応答について表示できます。

ARP インスペクションの設定の表示

ARP インスペクションの設定を表示するには、EXEC モードで **show arp inspection** 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 arp inspection

表 4-3 に、**show arp inspection** コマンドの出力フィールドを示します。

表 4-3　show arp inspection コマンドの出力フィールドの説明

フィールド	説明
Context	現在のコンテキストの名前
ARP Inspection	ARP インスペクションがイネーブルかどうかのステータス
Flooding	フラッディングがイネーブルかどうかのステータス

ARP タイムアウト値の表示

ARP タイムアウト値を表示するには、EXEC モードで **show arp timeout** 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 arp timeout

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

表 4-4　show arp timeout コマンドの出力フィールドの説明

フィールド	説明
Refresh Time	キャッシュ エントリを検証するために ACE に送信される ARP 要求の間隔（秒）
Learned Address	ACE が学習済みホストに対する ARP 要求を送信する間隔（秒）
Configured Address	ACE が設定済みホストに ARP リフレッシュ要求を送信する間隔（秒）。デフォルトの間隔は 300 秒です。
Retry Rate	ACE がホストに ARP 再試行を送信する間隔（秒）
Max Retries per Host	ACE がホストにダウンというフラグを付けるまでに ARP を試行する回数

ARP テーブルからの ARP 学習済みエントリのクリア

ARP キャッシュ テーブルから ARP 学習済みエントリをクリアするには、**clear arp** 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 arp [**no-refresh**]

オプションの **no-refresh** キーワードを指定すると、エントリに対する ARP を実行せずに、キャッシュ テーブル内の学習済み ARP エントリをクリアします。このオプションを指定せずにこのコマンドを使用した場合、エントリに対して ARP が実行されます。

たとえば、学習済み ARP エントリをクリアして、エントリに対する ARP を実行するには、次のように入力します。

```
host1/Admin# clear arp
```

ARP 統計情報のクリア

ARP 統計情報カウンタをクリアするには、**clear arp statistics** 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 arp statistics [**vlan** *number*]

オプションの **vlan** *number* 引数を指定すると、特定のインターフェイスの統計情報カウンタをクリアできます。このオプションを指定せずにこのコマンドを使用した場合、すべてのインターフェイスのすべてのカウンタがクリアされます。

たとえば、ARP 統計情報カウンタをグローバルにクリアするには、次のように入力します。

```
host1/Admin# clear arp statistics
```