Cisco Application Control Engine モジュール ルーティング / ブリッジング コンフィギュレーション ガイド

Software Version A2(1.0)
March 2008

Text Part Number: OL-11866-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

**本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。
米国サイト掲載ドキュメントとの差異が生じる場合があるため、正式な内容については米国サイトのドキュメントを参照ください。
また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。**

Cisco Application Control Engine モジュール ルーティング/ ブリッジング コンフィギュレーション ガイド

CONTENTS

はじめに

このマニュアルでは、Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータ（以下、スイッチまたはルータ）向けの Cisco Application Control Engine（ACE）モジュールのルーティング機能およびブリッジング機能の設定方法について説明します。

また、次の ACE 設定タスクの実行方法についても説明します。

- VLAN の設定
- ルーティングの設定
- ブリッジングの設定
- Address Resolution Protocol（ARP; アドレス解決プロトコル）の設定
- Dynamic Host Configuration Protocol（DHCP）の設定

ここで説明する主な内容は、次のとおりです。

対象読者

このマニュアルは、次の役割を担い ACE の設定を担当する、訓練を受けた認定サービス技術者を対象としています。

- Web マスター
- システム管理者
- システム オペレータ

マニュアルの構成

このマニュアルの構成は次のとおりです。

章	説明
第 1 章「VLAN インターフェイスの設定」	ACE 上での VLAN の設定方法について説明します。
第 2 章「ACE のルート設定」	デフォルト ルートおよびスタティック ルートの設定方法について説明します。
第 3 章「トラフィックのブリッジング」	透過（ブリッジ）モードおよび Bridge Group Virtual Interface（BVI; ブリッジ グループ仮想インターフェイス）の設定方法について説明します。
第 4 章「ARP の設定」	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。
第 5 章「DHCP リレーの設定」	DHCP リレー エージェントの設定方法について説明します。
付録 A「アドレス、プロトコル、およびポートの概要」	以下に関する参考資料が記載されています。 • IP アドレスおよびサブネット マスク • プロトコルおよびアプリケーション • TCP および UDP ポート • ICMP タイプ

関連資料

ACE には、このマニュアルに加え、次のマニュアルが付属しています。

マニュアル タイトル	説明
『*Release Note for the Cisco Application Control Engine Module*』	ACE の動作に関する考慮事項、警告、および CLI コマンドについて説明しています。
『*Cisco Application Control Engine Module Hardware Installation Note*』	ACE を Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータに搭載する方法について説明しています。
『*Cisco Application Control Engine Module Getting Started Guide*』	ACE の初期設定および設定タスクの実行方法について説明しています。
『*Cisco Application Control Engine Module Administration Guide*』	ACE で次の管理タスクを実行する方法について説明しています。 • ACE の設定 • リモート アクセスの確立 • ソフトウェア ライセンスの管理 • クラス マップとポリシー マップの設定 • ACE ソフトウェアの管理 • SNMP の設定 • 冗長性の設定 • XML インターフェイスの設定 • ACE ソフトウェアのアップグレード
『*Cisco Application Control Engine Module Virtualization Configuration Guide*』	単一のコンテキストまたは複数のコンテキストで ACE を稼働する方法について説明しています。

マニュアル タイトル	説明
『*Cisco Application Control Engine Module Server Load-Balancing Configuration Guide*』	ACE で、次のサーバ ロード バランシングに関するタスクを設定する方法について説明しています。 • リアル サーバおよびサーバ ファーム • サーバ ファーム内のリアル サーバ間でトラフィックをロード バランシングするためのクラス マップとポリシー マップ • サーバ ヘルス モニタリング（プローブ） • スティッキ性 • ファイアウォール負荷分散 • TCL スクリプト
『*Cisco Application Control Engine Module Security Configuration Guide*』	次の ACE セキュリティ機能の設定方法について説明しています。 • セキュリティ Access Control List（ACL; アクセス コントロール リスト） • TACACS+（Terminal Access Controller Access Control System Plus）、Remote Authentication Dial-In User Service（RADIUS）、または Lightweight Directory Access Protocol（LDAP）サーバを使用したユーザ認証とアカウンティング • アプリケーション プロトコルと HTTP ディープ パケット インスペクション • TCP/IP 正規化および終了パラメータ • Network Address Translation（NAT; ネットワーク アドレス変換）

マニュアル タイトル	説明
『*Cisco Application Control Engine Module SSL Configuration Guide*』	ACE で、次の Secure Sockets Layer（SSL）機能を設定する方法について説明しています。 • SSL 認証および SSL キー • SSL 開始 • SSL 終了 • エンドツーエンド SSL
『*Cisco Application Control Engine Module System Message Guide*』	ACE でシステム メッセージのロギングを設定する方法について説明しています。また、ACE によって生成されるシステム ログ（syslog）メッセージの一覧とそれぞれの説明も記載されています。
『*Cisco Application Control Engine Module Command Reference*』	すべての CLI コマンドをモード別にアルファベット順で一覧し、それぞれについて、構文、オプション、および関連コマンドを含めた説明が記載されています。
『*Cisco CSM-to-ACE Conversion Tool User Guide*』	Cisco Content Switching Module（CSM）と ACE 間の変換ツールを使用して、CSM の実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルを ACE に移行する方法について説明しています。
『*Cisco CSS-to-ACE Conversion Tool User Guide*』	Cisco Content Services Switch（CSS）と ACE 間の変換ツールを使用して、CSS の実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルを ACE に移行する方法について説明しています。

記号と表記法

このマニュアルでは、次の表記法を使用しています。

表記	説明
太字	コマンド、コマンド オプション、およびキーワードは**太字**で示しています。本文中のコマンドも太字で示しています。
イタリック体	ユーザが値を指定する引数は、*イタリック体*で示しています。また、新しい用語の初出箇所、書籍のタイトル、強調するテキストもイタリック体で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{ x | y | z }	必ずどれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
ストリング	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。
`screen` フォント	システムが表示する端末セッションおよび情報は、`screen` フォントで示しています。
太字の **`screen`** フォント	コマンドラインでユーザが入力しなければならない情報は、**太字**の **`screen`** フォントで示しています。
イタリック体 の *`screen`* フォント	ユーザが値を指定する引数は、*イタリック体* の *`screen`* フォントで示しています。
^	^ 記号は、Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します。
< >	パスワードのように出力されない文字は、かぎカッコ（< >）で囲んで示しています。

（注）は、次のように表しています。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意は、次のように表しています。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

CLI のシンタックス形式についての詳細は、『*Cisco Application Control Engine Module Command Reference*』を参照してください。

マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン

マニュアルの入手方法、テクニカル サポート、マニュアルに関するフィードバックの提供、セキュリティ ガイドライン、および推奨エイリアスと一般的なシスコのマニュアルに関する情報については、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。『*What's New in Cisco Product Documentation*』には、シスコの新規および改訂版の技術マニュアルの一覧が示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。

Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register/

オープン ソース ライセンスの利用に対する謝辞

本ソフトウェア ライセンスでの利用に対して、以下のとおり謝辞を表します。

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

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。

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。

CHAPTER 3

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、ACE 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 2 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 Application Control Engine Module 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 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 4 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 3-1 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 3-1　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、Admin 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 Application Control Engine Module 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 3-1　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 Application Control Engine Module 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 3-1　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
- ブリッジ グループ VLAN への ACL の割り当て
- インターフェイスのイネーブル化

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 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 を許可または拒否することができます。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 Application Control Engine Module 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
- BVI の IP アドレスの設定
- エイリアス IP アドレスの設定
- ピア IP アドレスの設定
- BVI の説明の設定
- BVI のイネーブル化

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 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 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 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されます。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 モジュールに自動的に同期させます。

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 mask*

ip_address mask 引数は、ピア モジュールのアドレスとサブネット マスクです。

ピア モジュールの 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 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
```

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 1 章「VLAN インターフェイスの設定」の表 1-1 を参照してください。

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
```

CHAPTER 5

DHCP リレーの設定

この章では、Dynamic Host Configuration Protocol（DHCP）サーバが DHCP クライアントに設定パラメータを提供する方法について説明します。DHCP を使用すると、ホスト IP アドレス、デフォルト ゲートウェイ、および DNS サーバを含む各種のネットワーク設定を行うことができます。DHCP クライアントおよび関連サーバが同じ IP ネットワークまたはサブネットに存在しない場合でも、DHCP リレー エージェントはそれらの間で DHCP メッセージを送信できます。DHCP リレー エージェントは、DHCP クライアントおよびサーバ間のインターフェイスとして動作します。また、クライアント要求を受信し、クライアントのリンク情報など、サーバがクライアントにアドレスを割り当てる際に必須となる設定データを追加します。DHCP サーバが応答すると、DHCP リレー エージェントは DHCP クライアントへ応答を転送します。

（注） ACE は共有 VLAN 上で受信した DHCP ブロードキャスト パケットに対する DHCP リレーをサポートしません。

この章の主な内容は、次のとおりです。

- DHCP サーバおよびクライアントの概要
- DHCP リレー設定のクイック スタート
- DHCP リレー エージェントの設定
- DHCP リレーの設定および統計情報の表示

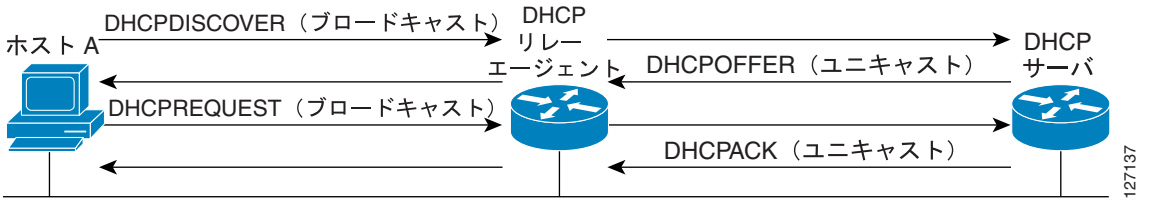
DHCP サーバおよびクライアントの概要

DHCP は、TCP/IP ネットワーク上のホストへ動的に構成情報を受け渡すためのフレームワークを提供します。DHCP クライアントは、IP アドレスなどの設定パラメータを取得するために DHCP を使用するインターネット ホストです。

DHCP リレー エージェントは、クライアントおよびサーバ間で DHCP パケットを転送する任意のホストです。リレー エージェントは、クライアントおよびサーバが物理的に同一のサブネット上にない場合に、それらの間で要求および応答を転送するために使用します。リレー エージェントによる転送は、通常の IP ルータでの転送とは区別されます。通常の IP ルータでの転送では、IP データグラムがネットワーク間で透過的にスイッチングされます。これとは対照的に、リレー エージェントは DHCP メッセージを受信したあと、新しい DHCP メッセージを生成してその他のインターフェイスに送信します。

図 5-1 に、DHCP クライアントが DHCP サーバに対して IP アドレスを要求した場合に発生する基本的な手順を示します。クライアントであるホスト A が DHCPDISCOVER ブロードキャスト メッセージを送信して、DHCP サーバを検索します。リレー エージェントが、DHCP クライアントおよびサーバ間でパケットを転送します。DHCP サーバは、DHCPOFFER ユニキャスト メッセージによって、IP アドレス、MAC アドレス、ドメイン名、IP アドレスのリースといった設定パラメータをクライアントに提供します。

図 5-1　DHCP サーバに対する IP アドレス要求



DHCP リレー設定のクイック スタート

表 5-1 は、ACE に DHCP リレー機能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。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 5-1 以降のセクションを参照してください。

表 5-1　DHCP リレー設定のクイック 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。必要な場合は、適切なコンテキストに直接ログイン（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、Admin 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 Application Control Engine Module Virtualization Configuration Guide*』を参照してください。

2. **config** と入力して、コンフィギュレーション モードを開始します。
`host1/Admin# config`
`Enter configuration commands, one per line. End with CNTL/Z`
`host1/Admin(config)#`

3. DHCP リレー エージェントをイネーブルにして、関連コンテキストまたは VLAN インターフェイス上のクライアントからの DHCP 要求を受け入れるようにします。 `host1/Admin(config)# ip dhcp relay enable`
4. DHCP リレー エージェントがクライアント要求を転送する DHCP サーバの IP アドレスを指定します。 `host1/Admin(config)# ip dhcp relay server 192.168.20.1`

表 5-1　DHCP リレー設定のクイック スタート（続き）

作業およびコマンド例
5. （任意）転送されたメッセージにすでにリレー情報が含まれていた場合に DHCP サーバが実行すべき作業を認識できるように、DHCP サーバにリレー エージェント情報の再転送ポリシーを設定します。 `host1/Admin(config)# ip dhcp relay information policy replace`

6. （任意）設定変更をフラッシュ メモリに保存します。
`host1/Admin(config)# exit`
`host1/Admin# copy running-config startup-config`

DHCP リレー エージェントの設定

ここでは、ACE に DHCP リレー エージェントを設定する方法について説明します。DHCP リレー エージェントとして設定された ACE は、DHCP クライアントおよびサーバ間でネゴシエートされる要求と応答を転送する役割を担います。デフォルトでは、DHCP リレー エージェントはディセーブルです。DHCP リレー エージェントをイネーブルにする場合、DHCP サーバを設定する必要があります。

DHCP リレー エージェントは、次のように ACE のコンテキスト レベルおよび VLAN インターフェイス レベルの両方で設定できます。

- DHCP リレー エージェントをコンテキスト レベルで設定すると、設定はコンテキストに関連付けられたすべてのインターフェイスに適用されます。
- DHCP リレー エージェントを VLAN インターフェイス レベルで設定すると、設定は特定のインターフェイスにのみ適用され、残りのインターフェイスは、コンテキスト レベルの設定に戻されます。

ここで説明する内容は、次のとおりです。

DHCP リレーのイネーブル化

ip dhcp relay enable コマンドを使用すると、関連付けられたコンテキストまたは VLAN インターフェイスのクライアントから DHCP 要求を受け入れ、DHCP リレー エージェントをイネーブルにすることができます。DHCP リレーによって、関連付けられた VLAN インターフェイスまたはコンテキストに対して、**ip dhcp relay server** コマンドで指定された DHCP サーバ アドレスへのパケット転送が開始されます。

このコマンドの構文は次のとおりです。

ip dhcp relay enable

たとえば、コンテキストに関連付けられたすべてのインターフェイスへの DHCP リレーをイネーブルにするには、次のように入力します。

```
host1/Admin(config)# ip dhcp relay enable
```

たとえば、VLAN インターフェイス レベルで DHCP リレー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 50
host1/Admin(config-if)# ip dhcp relay enable
```

コンテキストに関連付けられたすべてのインターフェイスへの DHCP リレー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)# no ip dhcp relay enable
```

VLAN インターフェイス上で DHCP リレー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 ip dhcp relay enable
```

DHCP サーバの IP アドレスの指定

ip dhcp relay server コマンドを使用すると、DHCP リレー エージェントがクライアント要求を転送する DHCP サーバの IP アドレスを設定できます。

このコマンドの構文は次のとおりです。

ip dhcp relay server *ip_address*

ip_address 引数では、DHCP サーバの IP アドレスを指定します。ドット付き 10 進表記でアドレスを入力します（たとえば、192.168.20.1）。

たとえば、コンテキストに関連付けられたすべてのインターフェイスに対して DHCP リレー サーバの IP アドレスを設定するには、次のように入力します。

```
host1/Admin(config)# ip dhcp relay enable
host1/Admin(config)# ip dhcp relay server 192.168.20.1
```

たとえば、VLAN インターフェイス レベルで DHCP リレー サーバの IP アドレスを設定するには、次のように入力します。

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip dhcp relay enable
host1/Admin(config-if)# ip dhcp relay server 192.168.20.1
```

DHCP サーバの 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 dhcp relay server 192.168.20.1
```

リレー エージェント情報の再転送ポリシーの設定

コンフィギュレーション モードで **ip dhcp relay information policy** コマンドを使用すると、転送されたメッセージにすでにリレー情報が含まれていた場合に DHCP リレー エージェントが実行すべき作業を認識するように設定できます。デフォルトの再転送ポリシーでは、DHCP リレー パケットをドロップするように設定されています。

（注） リレー エージェント情報の再転送ポリシーは、VLAN インターフェイス レベルで設定することはできません。この機能は、コンテキストと関連付けられたすべてのインターフェイスに対してグローバルにのみ設定できます。

このコマンドの構文は次のとおりです。

ip dhcp relay information policy {**keep** | **replace**}

キーワードは次のとおりです。

- **keep** ― DHCP リレー エージェントで既存の情報を変更しないことを指定します。
- **replace** ― DHCP リレー エージェントで既存の情報を上書きすることを指定します。

たとえば、コンテキストと関連付けられたすべてのインターフェイスに対して、既存の情報を置き換えるようにリレー エージェント情報の再転送ポリシーを設定するには、次のように入力します。

```
host1/Admin(config)# ip dhcp relay information policy replace
```

DHCP リレー パケットをドロップするデフォルトのリレー情報ポリシーに戻すには、次のように入力します。

```
host1/Admin(config)# no ip dhcp relay information policy replace
```

DHCP リレーの設定および統計情報の表示

show ip dhcp relay コマンドを使用すると、DHCP リレー エージェント用に収集された構成情報および統計情報を表示できます。DHCP リレーには 3 つの **show** コマンドがあります。

- **show ip dhcp relay conf** ― DHCP 構成情報を表示します。
- **show ip dhcp relay information policy** ― リレー エージェント情報の再転送ポリシーに関するステータスを表示します。
- **show ip dhcp relay statistics** ― DHCP リレー統計情報を表示します。

このコマンドの出力値は、**clear ip dhcp relay statistics** コマンドを入力するまで増分します。

たとえば、リレー エージェント情報の再転送ポリシーの設定ステータスを表示するには、次のように入力します。

```
host/Admin# show ip dhcp relay information policy
DHCP Relay reforwarding policy configured = REPLACE
```

DHCP リレー統計情報をすべてクリアするには、**clear ip dhcp relay statistics** 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# clear ip dhcp relay statistics
```

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

表 5-2　show ip dhcp relay conf コマンドの出力フィールドの説明

フィールド	説明
Context level configuration	コンテキスト レベルの DHCP リレー エージェントに関する構成情報
Status	コンテキスト レベルの DHCP サーバの動作ステータス：Enabled または Disabled
Server	コンテキスト レベルの DHCP サーバの IP アドレス
Interface level configuration	VLAN インターフェイス レベルの DHCP リレー エージェントに関する構成情報
VLAN	割り当てられたインターフェイス VLAN 番号

表 5-2　show ip dhcp relay conf コマンドの出力フィールドの説明（続き）

フィールド	説明
Interface ID	VLAN のインターフェイス ID
Status	VLAN インターフェイス レベルの DHCP サーバの動作ステータス：Enabled または Disabled
Server	VLAN インターフェイス レベルの DHCP サーバの IP アドレス

表 5-3 に、**show ip dhcp relay statistics** コマンドの出力フィールドを示します。

表 5-3　show ip dhcp relay statistics コマンドの出力フィールドの説明

フィールド	説明
Context level configuration	コンテキスト レベルの DHCP リレー エージェントに関する統計情報
Number of BOOTREQUEST packets relayed	DHCP サーバへ転送された BOOTREQUEST パケットの増分数
Number of DHCPDISCOVER packets relayed	DHCP サーバへ転送された DHCPDISCOVER パケットの増分数
Number of DHCPREQUEST packets relayed	DHCP サーバへ転送された DHCPREQUEST パケットの増分数
Number of DHCPDECLINE packets relayed	DHCP サーバへ転送された DHCPDECLINE パケットの増分数
Number of DHCPRELEASE packets relayed	DHCP サーバへ転送された DHCPRELEASE パケットの増分数
Number of DHCPINFORM packets relayed	DHCP サーバへ転送された DHCPINFORM パケットの増分数
Number of BOOTREPLY packets relayed	DHCP サーバへ転送された BOOTREPLY パケットの増分数
Number of DHCPOFFER packets relayed	DHCP サーバへ転送された DHCPOFFER パケットの増分数
Number of DHCPACK packets relayed	DHCP サーバへ転送された DHCPACK パケットの増分数

表 5-3　show ip dhcp relay 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
Number of DHCPNAK packets relayed	DHCP サーバへ転送された DHCPNAK パケットの増分数
Number of failures while relaying	DHCP リレー エージェントから DHCP サーバへのパケット転送中に発生した障害数
Interface level configuration	VLAN インターフェイス レベルの DHCP リレー エージェントに関する統計情報

APPENDIX A

アドレス、プロトコル、およびポートの概要

この付録では、次の項目に関する簡単な説明を示します。

- IP アドレスおよびサブネット マスク
- プロトコルおよびアプリケーション
- TCP ポートおよび UDP ポート
- ICMP タイプ

IP アドレスおよびサブネット マスク

ここでは、ACE での IP アドレスの使用方法について説明します。IP アドレスは、ドット付き 10 進表記で表記される 32 ビットの数値です。2 進数から 10 進数に変換された 4 つの 8 ビット フィールド（オクテット）が、ドットで区切られて表記されます。IP アドレスの最初の部分はホストが属するネットワークを表し、後ろの部分はそのネットワークの特定のホストを表します。ネットワーク番号フィールドはネットワーク プレフィクスと呼ばれます。特定のネットワークに属するすべてのホストは同じネットワーク プレフィクスを共有しますが、それぞれ固有のホスト番号が必要です。クラスフル IP の場合、アドレスのクラスによってネットワーク プレフィクスとホスト番号との境界の位置が定められています。

ここで説明する内容は、次のとおりです。

クラス

IP ホスト アドレスは、クラス A、クラス B、クラス C の 3 種類のアドレス クラスに分けられます。クラスによって、ネットワーク プレフィクスとホスト番号との境界が 32 ビット アドレス内のそれぞれどこに置かれるかが固定的に定義されています。クラス D アドレスは、マルチキャスト IP 用に予約されています。各クラスについて次に説明します。

- クラス A アドレス（1.xxx.xxx.xxx ～ 126.xxx.xxx.xxx）では、第 1 オクテットだけをネットワーク プレフィクスとして使用します。
- クラス B アドレス（128.0.xxx.xxx ～ 191.255.xxx.xxx）では、第 2 オクテットまでをネットワーク プレフィクスとして使用します。
- クラス C アドレス（192.0.0.xxx ～ 223.255.255.xxx）では、第 3 オクテットまでをネットワーク プレフィクスとして使用します。

クラス A アドレスには 16,777,214 個のホスト アドレスが含まれ、クラス B アドレスには 65,534 個のホストが含まれるため、サブネット マスクを使用してこれらの大規模なネットワークを小さいサブネットに分けることができます。

プライベート ネットワーク

ネットワークに多数のアドレスが必要で、それらのアドレスをインターネットでルーティングする必要がない場合、Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）の推奨するプライベート IP アドレスを使用することができます（RFC 1918 を参照）。アドバタイズしてはいけないプライベートネットワークとして、次のアドレス範囲が指定されています。

- 10.0.0.0 ～ 10.255.255.255
- 172.16.0.0 ～ 172.31.255.255
- 192.168.0.0 ～ 192.168.255.255

サブネット マスク

サブネット マスクによって、1 つのクラス A、B、または C ネットワークを複数のネットワークに変換することができます。サブネット マスクを使うと、ホスト番号のビットをネットワーク プレフィクスに追加して、拡張ネットワーク プレフィクスを作成できます。たとえば、クラス C ネットワーク プレフィクスは、常に IP アドレスの最初の 3 つのオクテットで構成されます。しかしクラス C 拡張ネットワーク プレフィクスは、第 4 オクテットの一部も使用します。

サブネット マスクについては、ドット付き 10 進表記の代わりに 2 進表記を使うと理解しやすくなります。サブネット マスクのビットは、インターネット アドレスと 1 対 1 で対応しています。

- IP アドレス内の対応するビットが拡張ネットワーク プレフィクスに含まれる場合、サブネット マスクのビットは 1 になります。
- IP アドレス内の対応するビットがホスト番号に含まれる場合、サブネット マスクのビットは 0 になります。

例 1 ― クラス B アドレス 129.10.0.0 の第 3 オクテット全部を、ホスト番号ではなく拡張ネットワーク プレフィクスの一部として使用する場合、サブネットマスク 11111111.11111111.11111111.00000000 を指定します。サブネット マスクによって、クラス B アドレスがクラス C アドレスと同等になり、ホスト番号は最後のオクテットだけで構成されます。

例 2 ― 第 3 オクテットの一部だけを拡張ネットワーク プレフィクスに使用する場合、サブネット マスクを 11111111.11111111.11111000.00000000 のように指定します。この例では、第 3 オクテットの 5 ビットだけが拡張ネットワーク プレフィクスに使用されます。

サブネット マスクは、ドット付き 10 進マスクまたは */ ビット*（「スラッシュ *ビット数*」）マスクで表記できます。例 1 の場合、ドット付き 10 進マスクを使用すると、2 進表記の各オクテットを 10 進数に変換して 255.255.255.0 になります。*/ ビット数* マスクの場合は、1 の個数を指定するので、/24 になります。例 2 の場合、10 進数だと 255.255.248.0、/ ビットだと /21 になります。

また、第 3 オクテットの一部を拡張ネットワーク プレフィクスに使うことで、複数のクラス C ネットワークを 1 つの大きなネットワーク（または *スーパーネット*）にまとめることができます。192.168.0.0/20 はその一例です。

ここで説明する内容は、次のとおりです。

- サブネット マスクの判別
- サブネット マスクで使用するアドレスの判別

サブネット マスクの判別

必要なホスト数に適したサブネット マスクを判別するには、表 A-1 を参照してください。

表 A-1　ホスト、ビット、およびドット付き 10 進マスク

ホスト[1]	/ ビット マスク	ドット付き 10 進マスク
16,777,216	/8	255.0.0.0（クラス A ネットワーク）
65,536	/16	255.255.0.0（クラス B ネットワーク）
32,768	/17	255.255.128.0
16,384	/18	255.255.192.0
8,192	/19	255.255.224.0
4,096	/20	255.255.240.0
2,048	/21	255.255.248.0
1,024	/22	255.255.252.0

表 A-1　ホスト、ビット、およびドット付き 10 進マスク（続き）

ホスト[1]	/ ビット マスク	ドット付き 10 進マスク
512	/23	255.255.254.0
256	/24	255.255.255.0（クラス C ネットワーク）
128	/25	255.255.255.128
64	/26	255.255.255.192
32	/27	255.255.255.224
16	/28	255.255.255.240
8	/29	255.255.255.248
4	/30	255.255.255.252
使用不可	/31	255.255.255.254
1	/32	255.255.255.255（単一ホスト アドレス）

1. サブネットの先頭と末尾の番号は予約されています。単一のホストを表す /32 は除きます。

サブネット マスクで使用するアドレスの判別

ここでは、クラス C およびクラス B 規模のネットワークでサブネット マスクを使用する場合に、使用できるネットワーク アドレスを判別する方法について示します。

- クラス C 規模のネットワーク アドレス
- クラス B 規模のネットワーク アドレス

クラス C 規模のネットワーク アドレス

ホスト数が 2 ～ 254 のネットワークでは、第 4 オクテットは 0 から始まるホスト アドレス数の倍数になります。次に、192.168.0.x の 8 ホストのサブネット（/29）の例を示します。

マスク /29（255.255.255.248）のサブネット	アドレスの範囲[1]
192.168.0.0	192.168.0.0 ～ 192.168.0.7
192.168.0.8	192.168.0.8 ～ 192.168.0.15
192.168.0.16	192.168.0.16 ～ 192.168.0.31

マスク /29（255.255.255.248）のサブネット	アドレスの範囲[1]
…	…
192.168.0.248	192.168.0.248 ～ 192.168.0.255

1. サブネットの先頭と末尾のアドレスは予約されています。最初のサブネットの例では、192.168.0.0 または 192.168.0.7 は使用できません。

クラス B 規模のネットワーク アドレス

ホスト数が 254 ～ 65,534 のネットワークでサブネット マスクを使用する場合、使用できるネットワーク アドレスを判別するには、すべての拡張ネットワーク プレフィクスについて第 3 オクテットの値を判別する必要があります。たとえば、10.1.*x*.0 などのアドレスをサブネット化するとします。このアドレスの 第 2 オクテットまでは、拡張ネットワーク プレフィクスに使用されるので固定です。第 4 オクテットはすべてのビットがホスト番号に使用されるので、0 になります。

第 3 オクテットの値を判別するには、次の手順に従います。

ステップ 1　65,536（第 3 および第 4 オクテットを使用した場合の総アドレス数）を必要なホスト アドレスの数で割り、ネットワークから作成できるサブネット数を算出します。

たとえば、65,536 をホスト数 4096 で割るとサブネット数は 16 になります。

したがって、クラス B 規模のネットワークには、それぞれ 4096 のアドレスを含む 16 のサブネットが存在できることになります。

ステップ 2　256（第 3 オクテットに含まれる値の数）をサブネット数で割り、第 3 オクテットの値の倍数を判別します。

この例では、256 ÷ 16 = 16 になります。

第 3 オクテットは、0 から始まる 16 の倍数になります。

したがって、ネットワーク 10.1 の 16 のサブネットは、次のようになります。

マスク /20（255.255.240.0）のサブネット	アドレスの範囲[1]
10.1.0.0	10.1.0.0 ～ 10.1.15.255
10.1.16.0	10.1.16.0 ～ 10.1.31.255
10.1.32.0	10.1.32.0 ～ 10.1.47.255
…	…
10.1.240.0	10.1.240.0 ～ 10.1.255.255

1. サブネットの先頭と末尾のアドレスは予約されています。最初のサブネットの例では、10.1.0.0 または 10.1.15.255 は使用できません。

プロトコルおよびアプリケーション

ここでは、ACE の設定に関連するプロトコルとアプリケーションについて説明します。ACE はルーテッド モードの場合、マルチキャスト プロトコルまたはルーティング プロトコルを通過させません。

使用できるリテラル値は、**ah**、**eigrp**、**esp**、**gre**、**icmp**、**igmp**、**igrp**、**ip**、**ipinip**、**nos**、**pcp**、**snp**、**tcp**、**udp** です。プロトコルを番号で指定することもできます。

表 A-2 に、プロトコルのリテラル値に対応する番号を示します。

表 A-2　プロトコルのリテラル値

リテラル	番号	説明
ah	51	IPv6 の Authentication Header（AH; 認証ヘッダー）、RFC 1826
eigrp	88	Enhanced Interior Gateway Routing Protocol（Enhanced IGRP）
esp	50	IPv6 の Encapsulated Security Payload（ESP）、RFC 1827
gre	47	Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）
icmp	1	Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）、RFC 792
igmp	2	Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）、RFC 1112
igrp	9	Interior Gateway Routing Protocol（IGRP）
ip	0	Internet Protocol（IP; インターネット プロトコル）
ipinip	4	IP-in-IP カプセル化
nos	94	Network Operating System（NOS; ネットワーク OS）、Novell NetWare
pcp	108	Payload Compression Protocol（PCP）
snp	109	Sitara Networks Protocol
tcp	6	Transmission Control Protocol（TCP）、RFC 793
udp	17	User Datagram Protocol（UDP; ユーザ データグラム プロトコル）、RFC 768

IANA の Web サイトで、プロトコル番号をオンラインで参照することができます。

http://www.iana.org/assignments/protocol-numbers

TCP ポートおよび UDP ポート

表 A-3 に、リテラル値およびポート番号を示します。どちらも ACE のコマンドで入力できます。次の点に注意してください。

- ACE では SQL*Net にポート 1521 を使用します。これは、Oracle で SQL*Net に使用されるデフォルト ポートです。ただし、この値は IANA のポート割り当てとは合致しません。
- ACE は、ポート 1645 と 1646 で Remote Authentication Dial-In User Service（RADIUS）を受信します。RADIUS サーバが標準ポート 1812 と 1813 を使用する場合は、**aaa-server**、**radius-authport**、および **aaa-server radius-acctport** コマンドを使用して、ACE がこれらのポートを使用するよう設定します。
- Domain Name System（DNS; ドメイン ネーム システム）アクセス用のポートを割り当てるには、**dns** ではなく **domain** を使用します。**dns** キーワードは、**dnsix** のポート番号に変換されます。

IANA の Web サイトで、ポート番号をオンラインで参照することができます。

http://www.iana.org/assignments/port-numbers

表 A-3　ポートのリテラル値

リテラル	プロトコル	番号	説明
aol	TCP	5190	AOL
bgp	TCP	179	Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）、RFC 1163
biff	UDP	512	メール システムがユーザに新しいメールを受信したことを通知するために使用
bootpc	UDP	68	Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）クライアント

表 A-3　ポートのリテラル値（続き）

リテラル	プロトコル	番号	説明
bootps	UDP	67	BOOTP サーバ
chargen	TCP	19	Character Generator
citrix-ica	TCP	1494	Citrix Independent Computing Architecture（ICA）プロトコル
cmd	TCP	514	**exec** と類似するが、**cmd** には自動認証がある
ctiqbe	TCP	2748	Computer Telephony Interface Quick Buffer Encoding（CTIQBE）
daytime	TCP	13	日時、RFC 867
discard	TCP, UDP	9	廃棄
domain	TCP, UDP	53	DNS
dnsix	UDP	195	DNSIX セッション管理モジュール監査リダイレクタ
echo	TCP, UDP	7	エコー
exec	TCP	512	リモート プロセスの実行
finger	TCP	79	Finger
ftp	TCP	21	File Transfer Protocol（FTP; ファイル転送プロトコル）、制御ポート
ftp-data	TCP	20	FTP、データ ポート
gopher	TCP	70	Gopher
https	TCP	443	HyperText Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）、SSL
hostname	TCP	101	NIC ホスト ネーム サーバ
ident	TCP	113	Ident 認証サービス
imap4	TCP	143	Internet Message Access Protocol（IMAP）バージョン 4
irc	TCP	194	Internet Relay Chat（IRC; インターネット リレー チャット）プロトコル

表 A-3　ポートのリテラル値（続き）

リテラル	プロトコル	番号	説明
isakmp	UDP	500	Internet Security Association and Key Management Protocol（ISAKMP）
kerberos	TCP, UDP	750	Kerberos
klogin	TCP	543	KLOGIN
kshell	TCP	544	Korn シェル
ldap	TCP	389	Lightweight Directory Access Protocol（LDAP）
ldaps	TCP	636	LDAP（SSL）
lpd	TCP	515	Line Printer Daemon（LPD）— プリンタ スプーラ
login	TCP	513	リモート ログイン
lotusnotes	TCP	1352	IBM Lotus Notes
mobile-ip	UDP	434	MobileIP エージェント
nameserver	UDP	42	ホスト ネーム サーバ
netbios-ns	UDP	137	NetBIOS ネーム サービス
netbios-dgm	UDP	138	NetBIOS データグラム サービス
netbios-ssn	TCP	139	NetBIOS セッション サービス
nntp	TCP	119	Network News Transfer Protocol（NNTP）
ntp	UDP	123	Network Time Protocol（NTP; ネットワーク タイム プロトコル）
pcanywhere-status	UDP	5632	pcAnywhere ステータス
pcanywhere-data	TCP	5631	pcAnywhere データ
pim-auto-rp	TCP, UDP	496	Protocol Independent Multicast（PIM）、逆経路フラッディング、dense（稠密）モード
pop2	TCP	109	Post Office Protocol（POP）— バージョン 2
pop3	TCP	110	POP — バージョン 3

表 A-3　ポートのリテラル値（続き）

リテラル	プロトコル	番号	説明
pptp	TCP	1723	ポイントツーポイント トンネリング プロトコル
radius	UDP	1645	RADIUS
radius-acct	UDP	1646	RADIUS（アカウンティング）
rip	UDP	520	Routing Information Protocol（RIP）
secureid-udp	UDP	5510	SecureID over UDP
smtp	TCP	25	Simple Mail Transport Protocol
snmp	UDP	161	Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）
snmptrap	UDP	162	SNMP ― トラップ
sqlnet	TCP	1521	Structured Query Language（SQL; 構造化照会言語）ネットワーク
ssh	TCP	22	Secure Shell（SSH; セキュア シェル）
sunrpc (rpc)	TCP, UDP	111	Sun Remote Procedure Call（RPC; リモート プロシージャ コール）
syslog	UDP	514	システム ログ
tacacs	TCP, UDP	49	TACACS+（Terminal Access Controller Access Control System Plus）
talk	TCP, UDP	517	Talk
telnet	TCP	23	RFC 854 Telnet
tftp	UDP	69	Trivial File Transfer Protocol（TFTP）
time	UDP	37	Time
uucp	TCP	540	UNIX-to-UNIX Copy Program（UUCP; UNIX 間コピー プログラム）
who	UDP	513	Who
whois	TCP	43	Who Is

表 A-3　ポートのリテラル値（続き）

リテラル	プロトコル	番号	説明
www	TCP	80	World Wide Web（WWW; ワールドワイド ウェブ）
xdmcp	UDP	177	X Display Manager Control Protocol（X DMCP）

ICMP タイプ

表 A-4 に、ACE のコマンドで入力できる ICMP タイプの番号および名前を示します。

表 A-4　ICMP タイプ

ICMP 番号	ICMP 名
0	echo-reply（エコー応答）
3	unreachable（到達不能）
4	source-quench（ソース クエンチ）
5	redirect（リダイレクト）
6	alternate-address（代替アドレス）
8	echo（エコー）
9	router-advertisement（ルータ アドバタイズメント）
10	router-solicitation（ルータ送信要求）
11	time-exceeded（時間超過）
12	parameter-problem（パラメータ問題）
13	timestamp-request（タイムスタンプ要求）
14	timestamp-reply（タイムスタンプ応答）
15	information-request（情報要求）
16	information-reply（情報応答）
17	mask-request（マスク要求）
18	mask-reply（マスク応答）
31	conversion-error（変換エラー）
32	mobile-redirect（モバイル リダイレクト）

INDEX

I

M

R

T

U

V

あ

え

か

き

く

こ

さ

し

す

せ

そ

た

て

と

は

ひ

ふ

へ

ほ

ま

も

よ

り

る

れ