



Cisco Application Control Engine Module Getting Started Guide

Software Version A2(1.0)
March 2008

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-11864-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)

Cisco Application Control Engine Module Getting Started Guide
Copyright © 2008, Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface v

Audience vi

How to Use This Guide vi

Related Documentation vii

Symbols and Conventions x

Obtaining Documentation, Obtaining Support, and Security Guidelines xi

Notices 1-xii

 OpenSSL/Open SSL Project 1-xii

 License Issues 1-xii

1-xvi

CHAPTER 1

Overview 1-1

Routing and Bridging 1-2

Administering the ACE 1-2

Virtualization 1-4

Server Load Balancing 1-5

ACE Security 1-5

Secure Sockets Layer 1-6

CHAPTER 2

Configuring the ACE and Performing Basic VIP Load Balancing 2-1

Initially Configuring the ACE 2-2

 Configuring VLANs for the ACE Using Cisco IOS Software 2-2

 Sessioning and Logging in to the ACE 2-4

- Assigning a Name to the ACE 2-5
- Assigning an IP Address to the ACE 2-5
- Configuring a Default Route 2-6
- Configuring Remote Access to the ACE 2-7
- Accessing the ACE through a Telnet Session 2-10
- Configuring Basic VIP Load Balancing on the ACE 2-11
 - Configuring Real Servers 2-11
 - Configuring a Server Farm 2-13
 - Configuring the VIP Traffic Policy 2-15
 - Configuring an ACL 2-18
 - Verifying the VIP Load-Balancing Configuration 2-20
- Where to Go Next 2-21



Preface

This guide provides the following information:

- An overview of the major functions and features of the Cisco Application Control Engine (ACE) module
- Instructions on how to initially configure the ACE in a Catalyst 6500 series switch or a Cisco 7600 series router, hereinafter referred to as the switch or router, respectively, to allow traffic and basic virtual IP (VIP) load balancing. Note that the Cisco 7600 series router supports the ACE20-MOD-K9 module only.
- References to tasks that you can perform on the ACE and where to find the information in the documentation set.

This preface contains the following major sections:

- [Audience](#)
- [How to Use This Guide](#)
- [Related Documentation](#)
- [Symbols and Conventions](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#)
- [Notices](#)

Audience

This guide is intended for the following trained and qualified service personnel who are responsible for configuring the ACE:

- Web master
- System administrator
- System operator

How to Use This Guide

This guide is organized as follows:

Chapter	Description
Chapter 1, Overview	Provides an overview of the major functions and features of the ACE
Chapter 2, Configuring the ACE and Performing Basic VIP Load Balancing	Provides procedures to initially configure the ACE to allow the passing of traffic, remote access, and basic VIP load balancing

Related Documentation

In addition to this document, the ACE documentation set includes the following documents:

Document Title	Description
<i>Release Note for the Cisco Application Control Engine Module</i>	Provides information about operating considerations, caveats, and command-line interface (CLI) commands for the ACE.
<i>Cisco Application Control Engine Module Hardware Installation Note</i>	Provides information for installing the ACE into the Catalyst 6500 series switch or a Cisco 7600 series router (an ACE20-MOD-K9 module only).
<i>Cisco Application Control Engine Module Administration Guide</i>	Describes how to perform the following administration tasks on the ACE: <ul style="list-style-type: none"> • Setting up the ACE • Establishing remote access • Managing software licenses • Configuring class maps and policy maps • Managing the ACE software • Configuring SNMP • Configuring redundancy • Configuring the XML interface • Upgrading the ACE software
<i>Cisco Application Control Engine Module Virtualization Configuration Guide</i>	Describes how to operate your ACE in a single context or in multiple contexts.

Document Title	Description
<i>Cisco Application Control Engine Module Routing and Bridging Configuration Guide</i>	<p>Describes how to configure the following routing and bridging tasks on the ACE:</p> <ul style="list-style-type: none"> • VLAN interfaces • Routing • Bridging • Dynamic Host Configuration Protocol (DHCP)
<i>Cisco Application Control Engine Module Server Load-Balancing Configuration Guide</i>	<p>Describes how to configure the following server load-balancing tasks on the ACE:</p> <ul style="list-style-type: none"> • Real servers and server farms • Class maps and policy maps to load balance traffic to real servers in server farms • Server health monitoring (probes) • Stickiness • Firewall load balancing • TCL scripts
<i>Cisco Application Control Engine Module Security Configuration Guide</i>	<p>Describes how to perform the following ACE security configuration tasks:</p> <ul style="list-style-type: none"> • Security access control lists (ACLs) • User authentication and accounting using a Terminal Access Controller Access Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS), or Lightweight Directory Access Protocol (LDAP) server • Application protocol and HTTP deep packet inspection • TCP/IP normalization and termination parameters • Network address translation (NAT)

Document Title	Description
<i>Cisco Application Control Engine Module SSL Configuration Guide</i>	Describes how to configure the following Secure Sockets Layer (SSL) tasks on the ACE: <ul style="list-style-type: none"> • SSL certificates and keys • SSL initiation • SSL termination • End-to-end SSL
<i>Cisco Application Control Engine Module System Message Guide</i>	Describes how to configure system message logging on the ACE. This guide also lists and describes the system log (syslog) messages generated by the ACE.
<i>Cisco Application Control Engine Module Command Reference</i>	Provides an alphabetical list and descriptions of all CLI commands by mode, including syntax, options, and related commands.
<i>Cisco CSM-to-ACE Conversion Tool User Guide</i>	Describes how to use the CSM-to-ACE conversion tool to migrate Cisco Content Switching Module (CSM) running- or startup-configuration files to the ACE.
<i>Cisco CSS-to-ACE Conversion Tool User Guide</i>	Describes how to use the CSS-to-ACE conversion tool to migrate Cisco Content Services Switches (CSS) running- or startup-configuration files to the ACE.

Symbols and Conventions

This publication uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in boldface . Bold text also indicates a command in a paragraph.
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> . Italic text also indicates the first occurrence of a new term, book title, emphasized text.
[]	Elements in square brackets are optional.
{ x y z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in <i>screen font</i> .
boldface screen font	Information you must enter in a command line is in boldface screen font .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

1. A numbered list indicates that the order of the list items is important.
 - a. An alphabetical list indicates that the order of the secondary list items is important.
- A bulleted list indicates that the order of the list topics is unimportant.
 - An indented list indicates that the order of the list subtopics is unimportant.

Notes use the following conventions:



Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Cautions use the following conventions:



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following conventions:

For additional information about CLI syntax formatting, refer to the *Cisco Application Control Engine Module Command Reference*.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

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

Notices

The following notices pertain to this software license.

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

Original SSLeay License:

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

This package is an SSL implementation written by Eric Young (ey@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

Overview

The Cisco Application Control Engine (ACE) module performs high-performance server load balancing (SLB) among groups of servers, server farms, firewalls, and other network devices, based on Layer 3 as well as Layer 4 through Layer 7 packet information. The ACE module can also terminate and initiate SSL-encrypted traffic so that it can perform intelligent load balancing while ensuring secure end-to-end encryption.

The following sections provide an overview of the major functions and features on the ACE:

- [Routing and Bridging](#)
- [Administering the ACE](#)
- [Virtualization](#)
- [Server Load Balancing](#)
- [ACE Security](#)
- [Secure Sockets Layer](#)

Routing and Bridging

The ACE does not have any external physical interfaces to receive traffic from clients and servers. Instead, it uses internal VLAN interfaces.

First, you must assign VLANs from the supervisor in the Catalyst 6500 series switch or a Cisco 7600 series router (an ACE20-MOD-K9 module only) to the ACE.

After the ACE is booted, it downloads the VLANs from the supervisor. You can then configure the interfaces as either routed or bridged as needed.

The ACE supports these protocols:

- Address Resolution Protocol (ARP)—Allows the ACE to manage and learn the mapping of IP to Media Access Control (MAC) information to forward and transmit packets.
- Dynamic Host Configuration Protocol (DHCP)—Provides configuration parameters to DHCP clients. You can configure the ACE as a DHCP relay agent; it can forward the requests and responses negotiations between the DHCP clients and the server.

For more information, see the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

Administering the ACE

In addition to standard administration tasks, such as establishing remote access and managing software licenses and the ACE software, the ACE allows you to perform advanced administration tasks such as using traffic policies to classify traffic flow and the action to take for the type of traffic. Traffic policies are as follows:

- Class maps—Classify inbound network traffic destined to, or passing through, the ACE based on a series of flow match criteria specified by a class map. Each class map defines network traffic that is of interest to you.
- Policy maps—Define a series of actions (functions) that you want applied to traffic configured for a class map.
- Service policy—Attaches the traffic policy to each specified VLAN interface. The ACE evaluates all network traffic on the specified interface according to the actions specified in the named traffic policy.

The ACE uses the individual traffic policies to implement the following functions:

- Remote access using Secure Shell (SSH) or Telnet
- Server load balancing (Layer 3, Layer 4, and Layer 7)
- Network Address Translation (NAT)
- HTTP deep packet inspection, application protocol inspection, and FTP command inspection
- SSL security services between a web browser (the client) and the HTTP connection (the server)
- TCP/IP normalization and termination

Simple Network Management Protocol (SNMP) allows you to query the ACE for Cisco Management Information Bases (MIBs) and to send event notifications to a network management system (NMS).

An XML interface on the ACE allows you to transfer, configure, and monitor objects in the ACE. This interface allows you to easily shape or extend the CLI query and reply data in XML format.

Redundancy provides fault tolerance for the stateful switchover of flows. Redundancy offers increased uptime and a more robust network by providing seamless switchover of flows in case an ACE becomes unresponsive. Redundancy is designed especially for the following network applications that require fault tolerance:

- Mission-critical enterprise applications
- Banking and financial services
- E-commerce
- Long-lived flows such as FTP and HTTP file transfers

For more information, see the *Cisco Application Control Engine Module Administration Guide*.

Virtualization

The virtualization tools allow you to manage the system resources and users of the ACE, as well as the services provided to your customers.

Virtualization provides the following features:

- **Contexts**—The objects that divide the virtualized environment. You can operate ACE in a single context or in multiple contexts. Multiple contexts use virtualization to partition your ACE into multiple virtual devices or contexts. Each context behaves like an independent device with its own policies, interfaces, domains, server farms, real servers, and administrators. Each context also has its own management VLAN that you can access using Telnet or SSH.
- **Domains**—A namespace in which a user operates and each user is associated with at least one domain. The role assigned to a user determines the operations that a user can perform on the objects in a domain and the command set available to that user. When you create a context, the ACE automatically creates a default domain for that context.
- **Role-based access control (RBAC)**—A mechanism that determines the commands and resources available to each user. A role defines a set of permissions for accessing the objects and resources in a context and the actions that you can perform on them.
- **Resource classes**—The means by which you manage context access to ACE resources, such as concurrent connections or bandwidth rate. The ACE is preconfigured with a default resource class that it applies to the Admin context and any user context upon creation.

For more information, see the *Cisco Application Control Engine Module Virtualization Configuration Guide*.

Server Load Balancing

Server load balancing (SLB) on the ACE provides the following features:

- Network traffic policies for SLB
- Real servers and server farms
- Health monitoring through probes, as well as TCL scripts
- Stickiness (connection persistence)
- Firewall load balancing (FWLB) to load-balance traffic from the Internet through a firewall to a data center or intranet

For more information, see the *Cisco Application Control Engine Module Server Load-Balancing Configuration Guide*.

ACE Security

The ACE contains the following security features:

- Security access control lists (ACLs) to provide basic security for your network by filtering traffic and controlling network connections
- User authentication and accounting using a Terminal Access Controller Access Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS), or Lightweight Directory Access Protocol (LDAP) server to perform user authentication and accounting (AAA) services to provide a higher level of security for users accessing the ACE
- HTTP deep packet inspection, File Transfer Protocol (FTP) command request inspection, and application inspection of Domain Name System (DNS), FTP, HTTP, Internet Control Message Protocol (ICMP), or Real-Time Streaming Protocol (RTSP)
- TCP/IP normalization and IP fragmentation to protect your ACE and the data center from attacks. It also describes IP reassembly and UDP parameters
- NAT to protect your data center by hiding private addresses from public networks

For more information, see the *Cisco Application Control Engine Module Security Configuration Guide*.

Secure Sockets Layer

SSL protocol on the ACE provides encryption technology for the Internet, ensuring secure transactions, such as the transmission of credit card numbers for e-commerce web sites. SSL provides the secure transaction of data between a client and a server through a combination of privacy, authentication, and data integrity. SSL relies upon certificates and private-public key exchange pairs for this level of security.

The ACE provides the following SSL features:

- A special set of SSL commands to perform the SSL cryptographic functions between a client and a server. The SSL functions include server authentication, private-key and public-key generation, certificate management, and data packet encryption and decryption.
- SSL termination to configure an ACE context for a front-end application in which the ACE operates as an SSL server communicating with a client.
- SSL initiation to configure an ACE context for a back-end application in which the ACE operates as a client communicating with an SSL server.
- End-to-end SSL to configure an ACE context for both SSL termination and SSL initiation. You can configure the ACE for end-to-end SSL when you have an application that requires establishing a secure SSL channel between the client, the ACE, and the SSL server.

For more information, see the *Cisco Application Control Engine Module SSL Configuration Guide*.



CHAPTER 2

Configuring the ACE and Performing Basic VIP Load Balancing

This chapter provides procedures to configure the ACE to allow traffic and perform basic VIP load balancing. It also includes document references for more detailed configuration information.

Before performing the procedures in this chapter, you should install the ACE in the Catalyst 6500 series switch or a Cisco 7600 series router. For information on how to install the ACE, see the *Cisco Application Control Engine Module Installation Note*.

This chapter contains the following major sections:

- [Initially Configuring the ACE](#)
- [Configuring Basic VIP Load Balancing on the ACE](#)
- [Where to Go Next](#)

Initially Configuring the ACE

The initial configuration of the ACE allows you to do the following tasks:

- Pass traffic from the supervisor engine in the Catalyst 6500 series switch or a Cisco 7600 series router (an ACE20-MOD-K9 module only) to the ACE
- Allow network connectivity
- Perform remote management through Telnet

This section describes how to accomplish these tasks:

- [Configuring VLANs for the ACE Using Cisco IOS Software](#)
- [Sessioning and Logging in to the ACE](#)
- [Assigning a Name to the ACE](#)
- [Assigning an IP Address to the ACE](#)
- [Configuring a Default Route](#)
- [Configuring Remote Access to the ACE](#)
- [Accessing the ACE through a Telnet Session](#)

Configuring VLANs for the ACE Using Cisco IOS Software

Before the ACE can receive traffic from the supervisor engine in the Catalyst 6500 series switch or a Cisco 7600 series router (an ACE20-MOD-K9 module only), you must create VLAN groups on the supervisor engine, and then assign the groups to the ACE. After you configure the VLAN groups on the supervisor engine for the ACE, you can configure the VLAN interfaces on the ACE.

In Cisco IOS software, you can create one or more VLAN groups, and then assign the groups to the ACE. For example, you can assign all the VLANs to one group, or you can create a group for each customer.

You cannot assign the same VLAN to multiple groups; however, you can assign multiple groups to an ACE. VLANs that you want to assign to multiple ACEs, for example, can reside in a separate group from VLANs that are unique to each ACE.

**Note**

Before you begin, contact your network administrator to determine which VLANs and addresses are available for use by the ACE.

To configure the VLANs for the ACE using the Cisco IOS software, perform the following steps:

- Step 1** Connect to the supervisor engine to open a session. For example, use Telnet to connect to the supervisor engine at the IP address 172.19.110.5, enter:

```
linux$ telnet 172.19.110.5
User Access Verification
```

```
Password: cisco
Router#
```

- Step 2** Assign VLANs to a group by using the **svclc vlan-group** *group_number* *vlan_range* command in configuration mode. You can assign a maximum of 16 VLAN groups on an ACE. For example, to create three VLAN groups, 50 with a VLAN range of 55 to 57, 51 with a VLAN range of 75 to 86, and 52 with a VLAN 100, enter:

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

- Step 3** Assign the VLAN groups to the ACE by using the **svc module** *slot_number* **vlan-group** *group_number_range* command. For example, to assign VLAN-groups 50 and 52 to the ACE in slot 5, and VLAN-group 51 and 52 to the ACE in slot 8, enter:

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

- Step 4** View the group configuration for the ACE and the associated VLANs by using the **show svclc vlan-group** command. For example, enter:

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

- Step 5** View VLAN group numbers for all modules, by using the **show svc module** command. For example, enter:

```
Router# show svc module
```

Sessioning and Logging in to the ACE

To initially session and log in to the ACE, perform the following steps:

- Step 1** Session into the ACE from the supervisor engine by using the **session** command from the supervisor engine. For example, to session into the ACE in slot 5, enter:

```
Router# session slot 5 processor 0
```

- Step 2** At the login prompt, log into the ACE by entering the login username and password. By default, the username and password are **admin**. For example, enter:

```
switch login: admin
Password: admin
```

You are ready to use the ACE CLI when the following prompt appears:

```
switch/Admin#
```

To change the default login username and password, see the *Cisco Application Control Engine Module Administration Guide*.

- Step 3** Prevent this current session from timing out by using the **terminal session-timeout** command and setting it to 0. By default, a session on the ACE is automatically logged out after 5 minutes of inactivity. For example, enter:

```
switch/Admin# terminal session-timeout 0
```

- Step 4** Disable the inactivity timeout when you log in to the ACE again by using the **login timeout** command in configuration mode as follows:

- a.** Access configuration mode by using the **configure** command in Exec mode. For example, enter:

```
switch/Admin# configure
Enter configuration commands, one per line. End with CNTL/Z
switch/Admin(config)#
```

- b.** Disable the inactivity timer by setting the **login timeout** command to 0. For example, enter:

```
switch/Admin(config)# login timeout 0
```

Assigning a Name to the ACE

The hostname is used for the command-line prompts and default configuration filenames. If you establish sessions to multiple devices, the hostname helps you track where you enter commands. By default, the hostname for the ACE is `switch`.

Change the hostname for the ACE by using the `host` command. Enter a case-sensitive name that contains from 1 to 32 alphanumeric characters. For example, to change the hostname of the ACE from `switch` to `host1`, enter:

```
switch/Admin(config)# hostname host1
```

The prompt appears with the new hostname:

```
host1/Admin(config)#
```

Assigning an IP Address to the ACE

After you assign the VLANs to the ACE, you can assign an IP address to the ACE for client connectivity over the network.



Note

The ACE requires a route back to the client before it can forward a request to a server. Otherwise, a flow cannot be established.

Use the `show vlans` command in Exec mode for the Admin context to display the ACE VLANs downloaded from the supervisor engine. Because `show` commands are available in Exec mode, you can use these commands from any configuration mode by including the `do` command. For example, enter:

```
host1/Admin(config)# do show vlans
Vlans configured on SUP for this module
vlan55-57 vlan100
```

To configure a VLAN interface on the ACE and access interface mode to configure the interface attributes, perform the following steps:

- Step 1** Access interface configuration mode for the VLAN by using the `interface vlan` command. For example, to create VLAN 55, enter:

```
host1/Admin(config)# interface vlan 55
host1/Admin(config-if)#
```

- Step 2** Assign an IP address to a VLAN interface for client connectivity by using the **ip address** command. For example, to set the IP address of 172.19.110.8 255.255.255.192 for the ACE, enter:

```
host1/Admin(config-if)# ip address 172.19.110.8 255.255.255.192
```

- Step 3** Provide a description for the interface by using the **description** command. For example, enter:

```
host1/Admin(config-if)# description Client side connectivity
```

- Step 4** Enable the interface by using the **no shutdown** command. For example, enter:

```
host1/admin(config-if)# no shutdown
```

- Step 5** Verify that VLAN 55 is up by using the **show interface** command. For example, enter:

```
host1/admin(config-if)# do show interface vlan 55
```

- Step 6** Verify the network connectivity by using the **ping** command. For example, enter:

```
host1/admin(config-if)# do ping 172.19.110.1
```

- Step 7** Display the ARP table by using the **show arp** command. For example, enter:

```
host1/admin(config-if)# do show arp
```

- Step 8** Reenter configuration mode by using the **exit** command. For example, enter:

```
host1/admin(config-if)# exit  
host1/admin(config)#
```

Configuring a Default Route

The default route identifies the IP address where the ACE sends all IP packets for which it does not have a route. To set a default route, use the **ip route dest_ip_prefix netmask gateway_ip_address** command.

For example, to set the IP address and subnet mask for the default route (0.0.0.0/0) and the default gateway to 172.19.110.1, an address on the same network as VLAN 55, enter:

```
host1/Admin(config)# ip route 0.0.0.0 0.0.0.0 172.19.110.1
```

To display the ACE routing table, use the **show ip route** command. For example, enter:

```
host1/Admin(config)# do show ip route
```

Configuring Remote Access to the ACE

Before remote network access can occur on the ACE, you must create a configuration that includes the following features:

- A class map to specify the traffic allowed access to an ACE interface
- A policy map to decide what to do with the class-map traffic
- A service policy to apply the policy map to an interface

To configure remote network management, perform the following steps:

-
- Step 1** Create a class map by using the **class-map type management** command. For example, to create a management type class map named **REMOTE_ACCESS** that matches any traffic and to access class map configuration mode, enter:

```
host1/Admin(config)# class-map type management match-any REMOTE_ACCESS
host1/Admin(config-cmap-mgmt)#
```

- Step 2** Provide a description for the class map by using the **description** command. For example, enter:

```
host1/Admin(config-cmap-mgmt)# description Remote access traffic match
```

- Step 3** Configure the match protocol that permits network management traffic by using the **match protocol** command. For example, to permit traffic based on the protocol of SSH, Telnet, and ICMP for any source address, enter:

```
host1/Admin(config-cmap-mgmt)# match protocol telnet any
host1/Admin(config-cmap-mgmt)# match protocol ssh any
host1/Admin(config-cmap-mgmt)# match protocol icmp any
```

- Step 4** Reenter configuration mode by using the **exit** command. For example, enter:

```
host1/Admin(config-cmap-mgmt)# exit
host1/Admin(config)#
```

- Step 5** Create a policy map for traffic destined to an ACE interface and access policy map management configuration mode by using the **policy-map type management first-match** command. For example, to create the REMOTE_MGMT_ALLOW_POLICY policy map, enter:

```
host1/Admin(config)# policy-map type management first-match
REMOTE_MGMT_ALLOW_POLICY
host1/Admin(config-pmap-mgmt) #
```

- Step 6** Apply the class map to this policy and access policy map class configuration mode by using the **class** command. For example, to apply the previously created REMOTE_ACCESS class map to this policy, enter:

```
host1/Admin(config-pmap-mgmt) # class REMOTE_ACCESS
host1/Admin(config-pmap-mgmt-c) #
```

- Step 7** Allow the ACE to receive the configured class map management protocols by using the **permit** command. For example, enter:

```
host1/Admin(config-pmap-mgmt-c) # permit
```

- Step 8** Reenter configuration mode by using the **exit** command. For example, enter:

```
host1/Admin(config-pmap-mgmt-c) # exit
host1/Admin(config-pmap-mgmt) # exit
host1/Admin(config) #
```

- Step 9** Access interface configuration mode for the VLAN to which you want to apply the policy map. For example, access the interface configuration mode for VLAN 55, enter:

```
host1/Admin(config) # interface vlan 55
host1/Admin(config-if) #
```

- Step 10** Apply the policy map to the interface by using the **service-policy input** command. For example, to apply the REMOTE_MGMT_ALLOW_POLICY policy map to the interface, enter:

```
host1/Admin(config-if) # service-policy input REMOTE_MGMT_ALLOW_POLICY
```

- Step 11** View the applied service policy on the interface by using the **show service-policy** command. For example, to display the REMOTE_MGMT_ALLOW_POLICY policy applied to the interface, enter:

```
host1/Admin(config-if) # do show service-policy
REMOTE_MGMT_ALLOW_POLICY
```

- Step 12** Save your configuration changes from the running configuration to the startup configuration.

```
host1/Admin(config-if)# do copy running-config startup-config
```

- Step 13** Display the running configuration by using the **show running-config** command. For example, enter:

```
host1/Admin# show running-config
Generating configuration....

login timeout 0
hostname host1

class-map type management match-any REMOTE_ACCESS
  10 match protocol telnet any
  20 match protocol ssh any
  30 match protocol icmp any

policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
  class REMOTE_ACCESS
    permit

interface vlan 55
  ip address 172.19.110.8 255.255.255.192
  description Client side connectivity
  service-policy input REMOTE_MGMT_ALLOW_POLICY
  no shutdown

ip route 0.0.0.0 0.0.0.0 172.19.110.1
```

Accessing the ACE through a Telnet Session

After you have completed the previous configurations, you should be able to use Telnet to access the ACE using its IP address. To use Telnet to access the ACE, perform the following steps:

-
- Step 1** Connect to the supervisor engine to open another session. For example, enter
- ```
linux$ telnet 172.19.110.5
User Access Verification

Password: cisco
Router#
```
- Step 2** Use Telnet to verify that you can access the ACE interface. For example, to access the ACE from the VLAN IP address of 172.19.110.8, enter:
- ```
Router# telnet 172.19.110.8
Trying 172.19.110.8 ... Open
```
- Step 3** At the prompt, log in to the ACE. Enter the **admin** login username and the **admin** password. For example, enter:
- ```
host1 login: admin
Password:
Cisco Application Control Software (ACSW)
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2006, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.
host1/Admin#
```
- Step 4** Display the Telnet session by using the **show telnet** command. For example, enter:
- ```
host1/Admin# show telnet
```
-

Configuring Basic VIP Load Balancing on the ACE

A basic load-balancing configuration allows the ACE to perform the following tasks:

- Match VIP destined traffic flows
- Load balance these flows to real servers on the network

Class maps classify client traffic destined to a VIP address. The ACE load balances traffic to a server farm and selects one of the real servers to respond to the client request.

This section provides the following topics to accomplish these tasks:

- [Configuring Real Servers](#)
- [Configuring a Server Farm](#)
- [Configuring the VIP Traffic Policy](#)
- [Configuring an ACL](#)
- [Verifying the VIP Load-Balancing Configuration](#)

Configuring Real Servers

Real servers are dedicated physical servers that you typically configure in groups called server farms. These servers provide services to clients, for example, HTTP or XML content. You identify real servers with names and characterize them with IP addresses, connection limits, and weight values.

To configure real servers on the ACE, perform the following steps:

- Step 1** Enter configuration mode by using the **configure** command in Exec mode. For example, enter:

```
host/Admin# config  
Enter configuration commands, one per line. End with CNTL/Z  
host1/Admin(config)#
```

- Step 2** Create a real server and access real server host configuration mode by using the **rserver** command. For example, to create a real server named SERVER1 as a host type (the default), enter:

```
host1/Admin(config)# rserver SERVER1
host1/Admin(config-rserver-host)#
```

- Step 3** Enter a description of the real server by using the **description** command. For example, enter:

```
host1/Admin(config-rserver-host)# description web-one content server
```

- Step 4** Assign the real server IP address in dotted-decimal notation by using the **ip address** command. For example, to assign the IP address of 192.168.4.11, enter:

```
host1/Admin(config-rserver-host)# ip address 192.168.4.11
```

- Step 5** Place the real server in service by using the **inservice** command. For example, enter:

```
host1/Admin(config-rserver-host)# inservice
```

- Step 6** Reenter configuration mode by using the **exit** command. For example, enter:

```
host1/Admin(config-rserver-host)# exit
host1/Admin(config)#
```

- Step 7** Configure additional real servers by repeating Steps 2 through 5. For example, to add a real server named SERVER2 with an IP address of 192.168.4.12, enter:

```
host1/Admin(config)# rserver SERVER2
host1/Admin(config-rserver-host)# description web-two content server
host1/Admin(config-rserver-host)# ip address 192.168.4.12
host1/Admin(config-rserver-host)# inservice
```

- Step 8** Reenter configuration mode by using the **exit** command. For example, enter:

```
host1/Admin(config-rserver-host)# exit
host1/Admin(config)#
```

- Step 9** Display the configuration of the real servers by using the **show running-config rserver** command. For example, enter:

```
host1/Admin(config)# do show running-config rserver
```

Configuring a Server Farm

After you create and configure the real servers, add them to a server farm. To create a server farm, perform the following steps:

- Step 1** Create a server farm and access server farm host configuration mode by using the **serverfarm** command. For example, to create a server farm of type host (the default) named SFARM1, enter:

```
host1/Admin(config)# serverfarm SFARM1
host1/Admin(config-sfarm-host)#
```

- Step 2** Associate an existing real server with the server farm and enter server farm host real server configuration mode by using the **rserver** command. For example, to associate SERVER1 real server to the server farm, enter:

```
host1/Admin(config-sfarm-host)# rserver SERVER1
host1/Admin(config-sfarm-host-rs)#
```

- Step 3** Place the real server in service by using the **inservice** command. Otherwise the ACE considers it out of service and the server farm cannot receive or respond to client requests. For example, enter:

```
host1/Admin(config-sfarm-host-rs)# inservice
```

- Step 4** Reenter server farm host configuration mode by using the **exit** command. For example, enter:

```
host1/Admin(config-sfarm-host-rs)# exit
host1/Admin(config-sfarm-host)#
```

- Step 5** Associate the SERVER2 real server to the server farm. For example, enter:

```
host1/Admin(config-sfarm-host)# rserver SERVER2
host1/Admin(config-sfarm-host-rs)#
```

- Step 6** Place the real server in service. For example, enter:

```
host1/Admin(config-sfarm-host-rs)# inservice
```

- Step 7** Reenter configuration mode by using the **exit** command. For example, enter:

```
host1/Admin(config-sfarm-host-rs)# exit
host1/Admin(config-sfarm-host)# exit
host1/Admin(config)#
```

- Step 8** Verify that the real servers appears as operational, even though network connectivity had not been established by using the **show rserver** command. For example, to display the SERVER1 real server, enter:
- ```
host1/Admin(config)# do show rserver SERVER1
```
- Step 9** Add an interface to allow the ACE to communicate with the real servers by using the **interface vlan** command. For example, to configure VLAN 57 and access its configuration mode, enter:
- ```
host1/Admin(config)# interface vlan 57
host1/Admin(config-if)#
```
- Step 10** Configure the IP address that is associated with the real server addresses by using the **ip address** command. For example, to configure the IP address of 192.168.4.1 255.255.255.0, enter:
- ```
host1/Admin(config-if)# ip address 192.168.4.1 255.255.255.0
```
- Step 11** Provide a description for the interface by using the **description** command. For example, enter:
- ```
host1/Admin(config-if)# description Server-side Interface
```
- Step 12** Enable the interface by using the **no shutdown** command. For example, enter:
- ```
host1/admin(config-if)# no shutdown
```
- Step 13** Save the running configuration to the startup configuration. For example, enter:
- ```
host1/Admin(config-if)# do copy running-config startup-config
```
- Step 14** Reenter configuration mode by using the **exit** command. For example, enter:
- ```
host1/Admin(config-if)# exit
host1/Admin(config)#
```
- Step 15** Display how the ACE populates the ARP table with the real server (RSERVER) by using the **show arp** command. For example, enter:
- ```
host1/Admin(config)# do show arp
```
-

Configuring the VIP Traffic Policy

The ACE classifies incoming traffic with class maps that are associated with policy maps to perform an action based on the class map match. The simplest match is server load balancing based on a client's attempt to reach a virtual IP address and port. This type of match is a Layer 3 and Layer 4 traffic policy. It matches only the destination IP address and port and then makes the server load-balancing decision.

To create a VIP traffic policy, perform the following steps:

- Step 1** Create a Layer 7 SLB policy map that attempts to match class maps in the order in which they occur for load balancing by using the **policy-map type loadbalance first-match** command. For example, to create a load balancing policy map named `L7_VIP_LB_ORDER_POLICY`, enter:

```
host1/Admin(config)# policy-map type loadbalance first-match
L7_VIP_LB_ORDER_POLICY
host1/Admin(config-pmap-lb)#
```

- Step 2** For a simple load-balancing policy, assign the ACE default class map that has an implicit match any statement in it for matching any traffic classification. Use the **class class-default** command. For example, enter:

```
host1/Admin(config-pmap-lb)# class class-default
host1/Admin(config-pmap-lb-c)#
```

- Step 3** Add the server farm to this class by using the **serverfarm** command. For example, to add the previously created `SFARM1` server farm, enter:

```
host1/Admin(config-pmap-lb-c)# serverfarm SFARM1
```

- Step 4** Reenter configuration mode by using the **exit** command. For example, enter:

```
host1/Admin(config-pmap-lb-c)# exit
host1/Admin(config-pmap-lb)# exit
host1/Admin(config)#
```

- Step 5** Create a Layer 3 and Layer 4 load-balancing class map by using the **class-map** command. For example, to create a class map named `L4_VIP_ADDRESS_CLASS`, enter:

```
host1/Admin(config)# class-map L4_VIP_ADDRESS_CLASS
host1/Admin(config-cmap)#
```

- Step 6** Define a VIP address match statement by using the **match virtual-address** command. For example, to define a match statement for the IP address 172.19.110.9 for any IP protocol, enter:
- ```
host1/Admin(config-cmap)# match virtual-address 172.19.110.9 any
```
- Step 7** Reenter configuration mode by using the **exit** command. For example, enter:
- ```
host1/Admin(config-cmap)# exit
host1/Admin(config)#
```
- Step 8** Create a Layer 3 and Layer 4 multi-match policy map to direct classified incoming requests to the load-balancing policy map by using the **policy-map multi-match** command. For example, to create the policy map named L4_LB_VIP_POLICY, enter:
- ```
host1/Admin(config)# policy-map multi-match L4_LB_VIP_POLICY
host1/Admin(config-pmap)#
```
- Step 9** Associate the Layer and Layer 4 class map that defines the VIP address with the policy map by using the **class** command. For example, to associate the previously created L4\_VIP\_ADDRESS\_CLASS class map, enter
- ```
host1/Admin(config-pmap)# class L4_VIP_ADDRESS_CLASS
host1/Admin(config-pmap-c)#
```
- Step 10** Associate the Layer 7 load-balancing policy map with the Layer 3 and Layer 4 policy map by using the **loadbalance** command. This association determines the actions that the ACE takes when network traffic matches a class map. For example, to associate the previously created L7_VIP_LB_ORDER_POLICY policy map, enter:
- ```
host1/Admin(config-pmap-c)# loadbalance policy L7_VIP_LB_ORDER_POLICY
```
- Step 11** Enable a VIP for load-balancing operations by using the **loadbalance vip inservice** command. For example, enter:
- ```
host1/Admin(config-pmap-c)# loadbalance vip inservice
```
- Step 12** Reenter configuration mode by using the **exit** command. For example, enter:
- ```
host1/Admin(config-pmap-c)# exit
host1/Admin(config-pmap)# exit
host1/Admin(config)# exit
```

- Step 13** Access the client-facing interface to which you want to apply the multi-match policy map by using the **interface vlan** command. For example, to access interface configuration mode for VLAN 55, enter:

```
host1/Admin(config)# interface vlan 55
host1/Admin(config-if)#
```

- Step 14** Apply the multi-match policy map by using the **service-policy input** command. For example, to apply the L4\_LB\_VIP\_POLICY policy map, enter:

```
host1/Admin(config-if)# service-policy input L4_LB_VIP_POLICY
```

- Step 15** Reenter configuration mode by using the **exit** command. For example, enter:

```
host1/Admin(config-if)# exit
host1/Admin(config)#
```

- Step 16** Save the running configuration to the startup configuration.

```
host1/Admin(config)# do copy running-config startup-config
```

- Step 17** Verify that the ACE will respond to traffic to the VIP address by using the **show service-policy** command. This command displays whether the VIP state is inservice. For example, to display the service policy state for the L4\_LB\_VIP\_POLICY policy map, enter:

```
host1/Admin(config)# do show service-policy L4_LB_VIP_POLICY
```

---

## Configuring an ACL

An access control list (ACL) provides an extra layer of security on the services that the ACE provides. For traffic destined to a class map that is applied to a multi-match policy map, you must configure an ACL and apply it to an interface. Otherwise, the ACE denies all traffic on the interface.

To configure an ACL, perform the following steps:

- 
- Step 1** Create an ACL for the interface by using the **access-list** command. For example, to create an ACL named ALL for access control on IP traffic through the ACE extended ACL and permit the forwarding of any source IP address to any destination address, enter:

```
host1/Admin(config)# access-list ALL line 10 extended permit ip any any
```

- Step 2** Access interface configuration mode for the interface configured with the multi-match policy map by using the **interface vlan** command. For example, to access interface configuration mode for VLAN 55, enter:

```
host1/Admin(config)# interface vlan 55
host1/Admin(config-if)#
```

- Step 3** Apply the ACL to the interface by using the **access-group input** command. For example, to apply the previously created ALL ACL, enter:

```
host1/Admin(config-if)# access-group input ALL
```

- Step 4** Reenter Exec mode by using the **end** command.

```
host1/Admin(config-if)# end
host1/Admin#
```

- Step 5** Verify that the ACL is applied and is active by using the **show access-list** command. For example, enter:

```
host1/Admin# show access-list ALL
```

- Step 6** Save the running configuration to the startup configuration.

```
host1/Admin# copy running-config startup-config
```

- Step 7** Display the configuration information by using the **show running-config** command.



---

**Note** In this example, the basic load-balancing configuration is bolded.

---

For example, enter:

```
host1/Admin# show running-config
Generating configuration....

login timeout 0
hostname host1

access-list ALL line 10 extended permit any ip any any

rserver SERVER1
 description web-one content server
 ip address 192.168.4.11
 inservice

rserver SERVER2
 description web-two content server
 ip address 192.168.4.12
 inservice

serverfarm SFARM1
 rserver SERVER1
 inservice
 rserver SERVER2
 inservice

class-map type management match-any REMOTE_ACCESS
 10 match protocol telnet any
 20 match protocol ssh any
 30 match protocol icmp any
class-map match-all L4_VIP_ADDRESS_CLASS
 10 match virtual-address 172.19.110.9 any

policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
 class REMOTE_ACCESS
 permit

policy-map type loadbalance first-match L7_VIP_LB_ORDER_POLICY
 class CLASS-DEFAULT
 serverfarm SFARM1
```

```

policy-map multi-match L4_LB_VIP_POLICY
 class L4_VIP_ADDRESS_CLASS
 loadbalance vip inservice
 loadbalance policy L7_VIP_LB_ORDER_POLICY

interface vlan 55
 ip address 172.19.110.8 255.255.255.192
 description Client side connectivity
 access-group input ALL
 service-policy input REMOTE_MGMT_ALLOW_POLICY
 service-policy input L4_LB_VIP_POLICY
 no shutdown
interface vlan 57
 ip address 192.168.4.1 255.255.255.0
 description Server-side Interface
 no shutdown

ip route 0.0.0.0 0.0.0.0 172.19.110.1

```

---

## Verifying the VIP Load-Balancing Configuration

To verify the load-balancing configuration, use the **show service-policy** command to display the incrementing of the counters as connections are handled. For example, to display the counters for the `L4_LB_VIP_POLICY` policy map, enter:

```

host1/Admin# show service-policy L4_LB_VIP_POLICY
Interface: vlan 55
 service-policy: L4_LB_VIP_POLICY
 class: L4_VIP_ADDRESS_CLASS
 loadbalance:
 L7 policy: L7_VIP_LB_ORDER_POLICY, VIP state: INSERVICE
 curr conns : 0 , hit count : 20
 dropped conns : 0
 client pkt count : 100 , client byte count: 13000
 server pkt count : 127 , server byte count: 92381

```

You can also verify access to the real servers by using a Telnet session to connect to the VIP address. If you are able to receive the login and password prompt from the ACE, access to the real servers is available through the VIP address. For example, enter:

```
linux$ telnet 172.19.110.9
Trying 172.19.110.9... Open
```

```
host1 login: admin
Password:
```

## Where to Go Next

After you have configured the ACE to allow traffic and remote access, and configured it for basic load balancing, you can configure more advanced features on the ACE.

[Table 2-1](#) lists additional advanced ACE features, including document references where you can obtain configuration information. For information on the ACE command-line interface and commands for each mode, see the *Cisco Application Control Engine Module Command Reference*.

**Table 2-1 Additional ACE Features**

| Advanced Feature                                                                | For more information, see...                                                                                                          |
|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Application protocol inspection                                                 | <i>Cisco Application Control Engine Module Security Configuration Guide</i><br>Chapter 3, Configuring Application Protocol Inspection |
| Connection persistence using HTTP-cookie, HTTP header, or IP netmask stickiness | <i>Cisco Application Control Engine Module Server Load-Balancing Configuration Guide</i><br>Chapter 5, Configuring Stickiness         |
| Health monitoring including probes                                              | <i>Cisco Application Control Engine Module Server Load-Balancing Configuration Guide</i><br>Chapter 4, Configuring Health Monitoring  |

**Table 2-1 Additional ACE Features (continued)**

| <b>Advanced Feature</b>                                                            | <b>For more information, see...</b>                                                                                                                           |
|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Layer 7 server load-balancing traffic policy, including class maps and policy maps | <i>Cisco Application Control Engine Module Server Load-Balancing Configuration Guide</i><br>Chapter 3, Configuring Traffic Policies for Server Load Balancing |
| Network Address Translation (NAT)                                                  | <i>Cisco Application Control Engine Module Security Configuration Guide</i><br>Chapter 5, Configuring Network Address Translation                             |
| Redundancy                                                                         | <i>Cisco Application Control Engine Module Administration Guide</i><br>Chapter 7, Configuring Redundant ACE Modules                                           |
| SSL functionality                                                                  | <i>Cisco Application Control Engine Module SSL Configuration Guide</i>                                                                                        |
| TCP/IP normalization                                                               | <i>Cisco Application Control Engine Module Security Configuration Guide</i><br>Chapter 4, Configuring TCP/IP Normalization and IP Reassembly Parameters       |
| User authentication and accounting                                                 | <i>Cisco Application Control Engine Module Security Configuration Guide</i><br>Chapter 2, Configuring Authentication and Accounting Services                  |
| Virtualization and role-based access control (RBAC)                                | <i>Cisco Application Control Engine Module Virtualization Configuration Guide</i>                                                                             |