



CHAPTER 3

Enabling Remote Access to the ACE



Note

The information in this chapter applies to both the ACE module and the ACE appliance unless otherwise noted. All features described in this chapter are supported with IPv6 unless otherwise noted.

This chapter describes how to configure remote access to the ACE by establishing a remote connection by using the Secure Shell (SSH) or Telnet protocols. It also describes how to configure the ACE to provide direct access to a user context from SSH. This chapter also covers how to configure the ACE to receive ICMP messages from a host.

This chapter contains the following major sections:

- [Guidelines and Restrictions](#)
- [Default Settings](#)
- [Enabling Remote Access to the ACE](#)
- [Displaying Remote Access Session Information](#)
- [Configuration Example for Enabling Remote Access to the ACE](#)



Note

For information about how to make a direct connection using a dedicated terminal attached to the Console port on the front of the ACE, configure terminal display attributes, and configure terminal line settings for accessing the ACE by console or virtual terminal connection, see either [Chapter 1, Setting Up the ACE Module](#) or [Chapter 2, Setting Up the ACE Appliance](#).

Guidelines and Restrictions

The guidelines and restrictions for the remote access function are as follows:

- If you configure an ACL on an interface to block certain traffic and a management policy on that same interface allows that traffic, the management policy overrides the ACL and the ACE allows the traffic.
- Telnet Management Sessions—The ACE supports a maximum 16 concurrent Telnet management sessions for the Admin context and 4 concurrent Telnet management sessions for each user context. The ACE supports a total maximum of 256 concurrent Telnet sessions. Telnet is not supported with IPv6.

- **SSH Management Sessions**—The ACE supports a maximum of 16 concurrent SSH management sessions for the Admin context and 4 concurrent SSH management sessions for each user context. The ACE supports a total maximum of 256 concurrent SSH sessions. SSH is not supported with IPv6.
The ACE can generate the DSA and RSA keys required to establish an SSH session and encrypt and decrypt messages. The keys are generated in pairs—one public key and one private key. The global administrator performs the key generation in the Admin context. All contexts associated with the ACE share the common key. There is only a single host-key pair.
- **ICMP Messages**—By default, the ACE does not allow ICMP messages to be received by an ACE interface or to pass through the ACE interface. ICMP is an important tool for testing your network connectivity; however, network hackers can also use ICMP to attack the ACE or your network. We recommend that you allow ICMP during your initial testing, but then disallow it during normal operation. ICMPv6 is supported.

Default Settings

Table 3-1 lists the default settings for the ACE remote access function.

Table 3-1 Default Remote Access Parameters

Parameters	Default
Concurrent Telnet management sessions per context	Admin context: 16 User context: 4 (each)
Concurrent SSH management sessions per context	Admin context: 16 User context: 4 (each)
Ability of an ACE interface to receive ICMP messages or allow ICMP messages to pass through it	Disabled
Status of the following match protocol command protocols: http, https, icmp, kalap-udp, snmp, ssh, telnet, and xml-https (ACE appliance only).	Disabled

Enabling Remote Access to the ACE

This section describes the tasks associated with enabling remote access to the ACE and includes the following topics:

- [Task Flow for Enabling Remote Access to the ACE](#)
- [Configuring Remote Network Management Traffic Services](#)
- [Configuring the Maximum Number of Telnet Management Sessions](#)
- [Configuring SSH Management Session Parameters](#)
- [Terminating an Active User Session](#)
- [Enabling ICMP Messages to the ACE](#)
- [Directly Accessing a User Context Through SSH](#)

Task Flow for Enabling Remote Access to the ACE

Follow these steps to enable IPv6 remote access to the ACE:

- Step 1** If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, log directly in to, or change to, the correct context.

```
host1/Admin# changeto C1
host1/C1#
```

The rest of the examples in this table use the Admin context, unless otherwise specified. For details on creating contexts, see the *Virtualization Guide, Cisco ACE Application Control Engine*.

- Step 2** Enter configuration mode.

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

- Step 3** Create a class map that permits network management traffic to be received by the ACE based on the ICMPv6 and the client source IP address.

```
host1/Admin(config)# class-map type management match-all ICMPv6_ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol icmpv6 source-address 2001:DB8:1::/64
or
host1/Admin(config-cmap-mgmt)# match protocol icmpv6 anyv6
host1/Admin(config-cmap-mgmt)# exit
host1/Admin(config)#
```

- Step 4** Configure a policy map that allows ICMPv6 traffic.

```
host1/Admin(config)# policy-map type management first-match
ICMPv6_REMOTE_MGMT_ALLOW_POLICY
host1/Admin(config-pmap-mgmt)# class ICMPv6_ALLOW_CLASS
or
host1/Admin(config-pmap-mgmt)# class ipv6 class-default
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config)#
```

- Step 5** Attach the traffic policy to a single VLAN interface or globally to all VLAN interfaces in the same context. For example, to specify an interface VLAN and apply the remote management policy map to the VLAN, enter:

```
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# ipv6 enable
host1/Admin(config-if)# ip address 2001:DB8:1::/64
host1/Admin(config-if)# service-policy input REMOTE_MGMT_ALLOW_POLICY
host1/Admin(config-if)# exit
```

- Step 6** (Optional) Save your configuration changes to Flash memory.

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

Follow these steps to enable IPv4 remote access to the ACE:

- Step 1** If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, log directly in to, or change to, the correct context.

```
host1/Admin# changeto C1
host1/C1#
```

The rest of the examples in this table use the Admin context, unless otherwise specified. For details on creating contexts, see the *Virtualization Guide, Cisco ACE Application Control Engine*.

Step 2 Enter configuration mode.

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

Step 3 Create a class map that permits network management traffic to be received by the ACE based on the network management protocol (SSH or Telnet) and client source IP address.

```
host1/Admin(config)# class-map type management match-all SSH-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol ssh source-address 172.16.10.0
255.255.255.254
host1/Admin(config-cmap-mgmt)# exit
host1/Admin(config)#
host1/Admin(config)# class-map type management match-all TELNET-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol telnet source-address 172.16.10.0
255.255.255.254
host1/Admin(config-cmap-mgmt)# exit
host1/Admin(config)#
```

Step 4 Configure a policy map that activates the SSH and Telnet management protocol classifications.

```
host1/Admin(config)# policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
host1/Admin(config-pmap-mgmt)# class SSH-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# class TELNET-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# exit
host1/Admin(config)#
```

Step 5 Attach the traffic policy to a single VLAN interface or globally to all VLAN interfaces in the same context. For example, to specify an interface VLAN and apply the remote management policy map to the VLAN, enter:

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip address 172.16.1.100 255.255.0.0
host1/Admin(config-if)# service-policy input REMOTE_MGMT_ALLOW_POLICY
host1/Admin(config-if)# exit
```

Step 6 (Optional) Configure the maximum number of Telnet sessions allowed for each context.

```
host1/Admin(config)# telnet maxsessions 3
```

Step 7 (Optional) Configure the maximum number of SSH sessions allowed for each context.

```
host1/Admin(config)# ssh maxsessions 3
```

Step 8 If you have global administrator privileges, use the **ssh key** command to generate the SSH private key and the corresponding public key for use by the SSH server. There is only one host-key pair. For example, to generate an RSA1 key pair in the Admin context, enter:

```
host1/Admin(config)# ssh key rsa1 768
generating rsa1 key(768 bits).....
.
generated rsa1 key
```

Step 9 (Optional) Save your configuration changes to Flash memory.

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

Step 10 (Optional) Terminate an active SSH or Telnet session for the active context by using one of the following commands in Exec mode:

- **clear ssh** {*session_id* | **hosts**}
- **clear telnet** *session_id*

```
host1/Admin# clear ssh 345
```

Configuring Remote Network Management Traffic Services

This section provides an overview on creating a class map, policy map, and service policy for remote network access to the ACE. The following items summarize the role of each function in configuring remote network management access to the ACE:

- Class map—Provides the remote network traffic match criteria to permit traffic based on:
 - Remote access network management protocols (SSH, Telnet, or ICMP)
 - Client source IP address
- Policy map—Enables remote network management access for a traffic classification that matches the criteria listed in the class map.
- Service policy—Activates the policy map and attaches the traffic policy to an interface or globally on all interfaces.

Telnet and SSH remote access sessions are established to the ACE on a per context basis. For details on creating users and contexts, see the *Virtualization Guide, Cisco ACE Application Control Engine*.

This section contains the following topics:

- [Creating and Configuring a Remote Management Class Map](#)
- [Creating a Layer 3 and Layer 4 Remote Access Policy Map](#)
- [Applying a Service Policy Globally to All VLAN Interfaces in the Same Context](#)
- [Applying a Service Policy to a Specific VLAN Interface](#)

Creating and Configuring a Remote Management Class Map

This section describes how to create a Layer 3 and Layer 4 class map to classify the remote network management traffic received by the ACE. The class map permits network management traffic to be received by the ACE by identifying the incoming IP protocols that the ACE can receive as well as the client source IP address and subnet mask as the matching criteria. You define the allowed network traffic to manage security for protocols such as SSH, Telnet, and ICMP. You also determine how the ACE evaluates multiple match statements operations when multiple match criteria exist in a class map.

The class map identifies the remote network access management protocols that can be received by the ACE. You configure the associated policy map to permit access to the ACE for the specified management protocols. As part of the network management access traffic classification, you also specify either a client source host IP address and subnet mask as the matching criteria or instruct the ACE to allow any client source address for the management traffic classification.

Detailed Steps

	Command	Purpose
Step 1	<pre>config</pre> <p>Example: host1/Admin# config host1/Admin(config)#</p>	Enters global configuration mode.
Step 2	<pre>class-map type management [match-all match-any] map_name</pre> <p>Example: host1/Admin(config)# class-map type management match-all SSH-TELNET_ALLOW_CLASS host1/Admin(config-cmap-mgmt)#</p>	<p>Creates a Layer 3 and Layer 4 class map to classify the remote network management traffic received by the ACE.</p> <p>The keywords, arguments, and options are as follows:</p> <ul style="list-style-type: none"> • match-all match-any—(Optional) Determines how the ACE evaluates Layer 3 and Layer 4 network management traffic when multiple match criteria exist in a class map. The class map is considered a match if the match commands meet one of the following conditions: <ul style="list-style-type: none"> – match-all—(Default) All of the match criteria listed in the class map are satisfied to match the network traffic class in the class map, typically match commands of the same type. – match-any—Any one of the match criteria listed in the class map is satisfied to match the network traffic class in the class map, typically match commands of different types. • <i>map_name</i>—Specifies the name assigned to the class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. <p>The CLI enters the class map management configuration mode.</p>
	<pre>no class-map type management [match-all match-any] map_name</pre> <p>Example: host1/Admin(config)# no class-map type management match-all SSH-TELNET_ALLOW_CLASS</p>	(Optional) Removes a Layer 3 and Layer 4 network management class map from the ACE.

Command	Purpose
<p>Step 3</p> <p>(ACE module only)</p> <pre>[line_number] match protocol {http https icmp icmpv6 kalap-udp snmp ssh telnet} {any anyv6 source-address {ipv6_address/prefix_length ipv4_address mask}}</pre> <p>(ACE appliance only)</p> <pre>[line_number] match protocol {http https icmp icmpv6 kalap-udp snmp ssh telnet xml-https} {any anyv6 source-address {ipv6_address/prefix_length ipv4_address mask}}</pre> <p>Example:</p> <pre>ACE_1/Admin(config-cmap-mgmt)# match protocol ssh source-address 172.16.10.0 255.255.255.254 ACE_1/Admin(config-cmap-mgmt)# match protocol telnet source-address 172.16.10.0 255.255.255.254</pre>	<p>Classifies the remote network management traffic received by the ACE. Include one or more of the match protocol commands to configure the match criteria for the class map.</p> <p>The keywords and arguments are as follows:</p> <ul style="list-style-type: none"> line_number—(Optional) Assists you in editing or deleting individual match commands. Enter an integer from 2 to 255 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements. http—Specifies the Hypertext Transfer Protocol (HTTP). The configuration of the HTTP management protocol is described in Chapter 9, Configuring the XML Interface. https—Specifies the secure (SSL) Hypertext Transfer Protocol (HTTP). The configuration of the HTTPS management protocol is described in Chapter 9, Configuring the XML Interface. (ACE appliance only) HTTPS is used for connectivity with the Device Manager GUI on the ACE appliance using port 443. icmp—Specifies Internet Control Message Protocol messages to the ACE. The configuration of the ICMP management protocol is described in the “Enabling ICMP Messages to the ACE” section. icmpv6—Specifies Internet Control Message Protocol Version 6 messages to the ACE. The configuration of the ICMPv6 management protocol is described in the “Enabling ICMP Messages to the ACE” section. kalap-udp—Specifies management access using KAL-AP over UDP. The configuration of the KAL-AP management access is described in the “Configuring Health Monitoring” chapter of the <i>Server Load-Balancing Guide, Cisco ACE Application Control Engine</i>. snmp—Specifies the Simple Network Management Protocol (SNMP). The configuration of the SNMP management protocol is described in Chapter 8, Configuring SNMP. ssh—Specifies a Secure Shell (SSH) remote connection to the ACE. The ACE supports the SSH remote shell functionality provided in SSH Version 1 and supports DES and 3DES ciphers. The configuration of the SSH management protocol is described in the “Configuring SSH Management Session Parameters” section. <p>Note SSH v1.x and v2 are entirely different protocols and are not compatible. Make sure that you use an SSH v1.x client when accessing the ACE.</p>

Command	Purpose
<pre>(ACE module only) [line_number] match protocol {http https icmp icmpv6 kalap-udp snmp ssh telnet} {any anyv6 source-address {ipv6_address/prefix_length ipv4_address mask}}</pre> <pre>(ACE appliance only) [line_number] match protocol {http https icmp icmpv6 kalap-udp snmp ssh telnet xml-https} {any anyv6 source-address {ipv6_address/prefix_length ipv4_address mask}}</pre>	<ul style="list-style-type: none"> • telnet—Specifies a Telnet remote connection to the ACE. The configuration of the Telnet management protocol is described in the “Configuring the Maximum Number of Telnet Management Sessions” section. • (ACE appliance only) xml-https—Specifies HTTPS as transfer protocol to send and receive XML documents between the ACE and a Network Management System (NMS). Communication is performed using port 10443. You can enable both https and xml-https in a Layer 3 and Layer 4 network management class map. The use of the HTTPS management protocol for XML usage is described in Chapter 9, Configuring the XML Interface. • any—Specifies any IPv4 client source address for the management traffic classification. • anyv6—Specifies any IPv6 client source address for the management traffic classification. • source-address—Specifies a client source host IP address and subnet mask as the network traffic matching criteria. As part of the classification, the ACE implicitly obtains the destination IP address from the interface on which you apply the policy map. • <i>ipv6_address</i>—Source IPv6 address of the client. • <i>/prefix_length</i>—Specifies how many of the most significant bits (MSBs) of the IPv6 address are used for the network identifier. Enter a forward slash character (/) followed by an integer from 1 to 128. The default is /128. If you use the optional oui64 keyword, you must enter a prefix-length and the prefix must be less than or equal to /64. • <i>ipv4_address</i>—Source IPv4 address of the client. • <i>mask</i>—Subnet mask of the client in dotted-decimal notation.
<pre>(ACE module only) no match protocol {http https icmp icmpv6 kalap-udp snmp ssh telnet} {any anyv6 source-address {ipv6_address/prefix_length ipv4_address mask}}</pre> <pre>(ACE appliance only) no match protocol {http https icmp icmpv6 kalap-udp snmp ssh telnet xml-https} {any anyv6 source-address {ipv6_address/prefix_length ipv4_address mask}}</pre> <p>Example: ACE_1/Admin(config-cmap-mgmt)# no match protocol ssh source-address 192.168.10.1 255.255.255.0</p>	<p>(Optional) Deselects the specified network management protocol match criteria from the class map.</p>

	Command	Purpose
Step 4	description <i>text</i> Example: host1/Admin(config-cmap-mgmt)# description Allow Telnet access to the ACE	Provides a brief summary about the Layer 3 and Layer 4 remote management class map.
	no description <i>text</i> Example: host1/Admin(config-cmap-mgmt)# no description	(Optional) Removes the description from the class map.
Step 5	do copy running-config startup-config Example: ACE_1/Admin(config-cmap-mgmt)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Creating a Layer 3 and Layer 4 Remote Access Policy Map

This section describes how to create a Layer 3 and Layer 4 policy map for a Layer 3 and Layer 4 traffic classification with actions to define the network management traffic received by the ACE. The general steps to configure a Layer 3 and Layer 4 network traffic policy are as follows:

- Configure a Layer 3 and Layer 4 policy map that defines the different actions that are applied to the IP management traffic received by the ACE. The ACE executes the specified action only for traffic that meets the first matching classification with a policy map. The ACE does not execute any additional actions.
- Optionally, provide a brief description about the Layer 3 and Layer 4 remote management policy map.
- Specify a Layer 3 and Layer 4 traffic class that you created with the **class-map** command to associate network traffic with the traffic policy.
- Allow the network management traffic that is listed in the Layer 3 and Layer 4 class map to be received or rejected by the ACE.

Detailed Steps

	Command	Purpose
Step 1	config Example: host1/Admin# config host1/Admin(config)#	Enters global configuration mode.
Step 2	policy-map type management first-match <i>map_name</i> Example: host1/Admin(config)# policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY host1/Admin(config-pmap-mgmt) #	Configures a Layer 3 and Layer 4 policy map that defines the different actions that are applied to the IP management traffic received by the ACE. The <i>map_name</i> argument specifies the name assigned to the Layer 3 and Layer 4 network management policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. When you use this command, you will access policy map management configuration mode.
	no policy-map type management first-match <i>map_name</i> Example: host1/Admin(config)# no policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY	(Optional) Removes a policy map from the ACE.
Step 3	description <i>text</i> Example: host1/Admin(config-pmap-mgmt) # description Allow Telnet access to the ACE	Provides a brief summary about the Layer 3 and Layer 4 remote management policy map. The <i>text</i> argument specifies the description that you want to provide. Enter an unquoted text string with a maximum of 240 alphanumeric characters.
	no description Example: host1/Admin(config-pmap-mgmt) # no description	(Optional) Removes a description from the policy map.

Command	Purpose
<p>Step 4</p> <pre>class {name1 [insert-before name2] class-default class-default-v6}</pre> <p>Example: host1/Admin(config-pmap-mgmt)# class L4_REMOTE_ACCESS_CLASS host1/Admin(config-pmap-mgmt-c)# </p>	<p>Specifies a Layer 3 and Layer 4 traffic class created with the class-map command to associate network traffic with the traffic policy.</p> <p>The arguments, keywords, and options are as follows:</p> <ul style="list-style-type: none"> • name1—Name of a previously defined Layer 3 and Layer 4 traffic class, configured with the class-map command, to associate traffic to the traffic policy. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. • insert-before name2—(Optional) Places the current class map ahead of an existing class map or inline match condition specified by the name2 argument in the policy map configuration. The ACE does not save the sequence reordering as part of the configuration. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. • class-default—Specifies the IPv4 class-default class map for the Layer 3 and Layer 4 traffic policy. This class map is a reserved class map created by the ACE. You cannot delete or modify this class. All IPv4 network traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified IPv4 classifications match, the ACE then matches the action specified under the class class-default command. The class-default class map has an implicit match any statement in it and is used to match any IPv4 traffic classification. The class-default class map has an implicit match any statement that matches all IPv4 traffic. • class-default-v6—Specifies the IPv6 class-default class map for the Layer 3 and Layer 4 traffic policy. This class map is a reserved class map created by the ACE. You cannot delete or modify this class. All IPv6 network traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications match, the ACE then matches the action specified under the class class-default-v6 command. The class-default class map has an implicit match any statement in it and is used to match any IPv6 traffic classification. The class-default-v6 class map has an implicit match any statement that matches all IPv6 traffic. <p>This command enters the policy map management class configuration mode.</p>
<pre>no class {name1 [insert-before name2] class-default class-default-v6}</pre> <p>Example: host1/Admin(config-pmap-mgmt)# no class L4_REMOTE_ACCESS_CLASS </p>	<p>(Optional) Remove a class map from a Layer 3 and Layer 4 policy map.</p>

	Command	Purpose
Step 5	<p>permit deny</p> <p>Example: host1/Admin(config-pmap-mgmt-c)# permit</p>	<p>Allows the network management traffic listed in the Layer 3 and Layer 4 class map to be received or rejected by the ACE as follows:</p> <ul style="list-style-type: none"> • Use the permit command in policy map class configuration mode to allow the remote management protocols listed in the class map to be received by the ACE. • Use the deny command in policy map class configuration mode to refuse the remote management protocols listed in the class map to be received by the ACE.
Step 6	<p>do copy running-config startup-config</p> <p>Example: host1/Admin(config-pmap-mgmt-c)# do copy running-config startup-config</p>	<p>(Optional) Copies the running configuration to the startup configuration.</p>

Examples

The following example shows how to create a Layer 3 and Layer 4 remote network traffic management policy map that permits SSH, Telnet, and ICMP connections to be received by the ACE:

```
host1/Admin(config)# policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
host1/Admin(config-pmap-mgmt)# class SSH_ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# class TELNET_ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# class ICMP_ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
```

The following example shows how to create a policy map that restricts an ICMP connection by the ACE:

```
host1/Admin(config)# policy-map type management first-action ICMP_RESTRICT_POLICY
host1/Admin(config-pmap-mgmt)# class ICMP_ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# deny
```

IPv6 Example

The following example shows how to create a policy map that matches any IPv6 traffic by using the class-default-v6 class map:

```
host1/Admin(config)# policy-map type management first-action MATCH_ANYV6_POLICY
host1/Admin(config-pmap-mgmt)# class class-default-v6
host1/Admin(config-pmap-mgmt-c)# permit
```

IPv4 Example

The following example shows how to create a policy map that matches any IPv6 traffic by using the class-default-v6 class map:

```
host1/Admin(config)# policy-map type management first-action MATCH_ANYV6_POLICY
host1/Admin(config-pmap-mgmt)# class class-default
host1/Admin(config-pmap-mgmt-c)# permit
```

Applying a Service Policy Globally to All VLAN Interfaces in the Same Context

This section describes how to apply a previously created policy map globally to all VLAN interfaces in the same context.

Note the following guidelines when applying a service policy:

- Policy maps, applied globally in a context, are internally applied on all interfaces existing in the context.
- A policy activated on an interface overwrites any specified global policies for overlapping classification and actions.

You can remove a traffic policy map from a VLAN by using either of the following methods:

- Individually from the last VLAN interface on which you applied the service policy
- Globally from all VLAN interfaces in the same context

The ACE automatically resets the associated service policy statistics to provide a new starting point for the service policy statistics the next time that you attach a traffic policy to a specific VLAN interface or globally to all VLAN interfaces in the same context.



Note

To apply the policy map to a specific VLAN interface only, see the [“Applying a Service Policy to a Specific VLAN Interface”](#) section.

Guidelines and Restrictions

The ACE allows only one policy of a specific feature type to be activated on a given interface and only in the input direction.

Detailed Steps

	Command	Purpose
Step 1	<code>config</code> Example: host1/Admin# config host1/Admin(config)#	Enters global configuration mode.
Step 2	<code>service-policy input policy_name</code> Example: host1/Admin(config)# service-policy input REMOTE_MGMT_ALLOW_POLICY	Applies the remote access policy map globally to all of the VLANs associated with a context. The <i>policy_name</i> argument is the name of a previously defined policy map, configured with a previously created policy-map command. The name can be a maximum of 40 alphanumeric characters.
	<code>no service-policy input policy_name</code> Example: host1/Admin(config)# no service-policy input REMOTE_MGMT_ALLOW_POLICY	(Optional) Removes the remote access traffic policy globally from all VLANs associated with a context.
Step 3	<code>do copy running-config startup-config</code> Example: host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Command	Purpose
<p>Step 4</p> <pre>do show service-policy [policy_name [detail]]</pre> <p>Example: host1/Admin(config)# do show service-policy REMOTE_MGMT_ALLOW_POLICY</p>	<p>(Optional) Displays service policy statistics for all policy maps or a specific Layer 3 and Layer 4 remote network traffic management policy map.</p> <p>The keywords, options, and arguments are as follows:</p> <ul style="list-style-type: none"> <i>policy_name</i>—(Optional) Existing policy map that is currently in service (applied to an interface) as an unquoted text string with a maximum of 64 alphanumeric characters. If you do not enter the name of an existing policy map, the ACE displays information and statistics for all policy maps. detail—(Optional) Displays a more detailed listing of policy map statistics and status information. <p>Note The ACE updates the counters that the show service-policy command displays after the applicable connections are closed.</p>
<p>Step 5</p> <pre>do clear service-policy policy_name</pre> <p>Example: host1/Admin(config)# do clear service-policy REMOTE_MGMT_ALLOW_POLICY</p>	<p>(Optional) Clears the service policy statistics for a policy map.</p> <p>For the <i>policy_name</i> argument, enter the identifier of an existing policy map that is currently in service (applied to an interface).</p>

Applying a Service Policy to a Specific VLAN Interface

This section describes how to apply a previously created policy map to a specific VLAN interface. A policy activated on an interface overwrites any specified global policies for overlapping classification and actions.

You can remove a traffic policy map from a VLAN by using either of the following methods:

- Individually from the last VLAN interface on which you applied the service policy
- Globally from all VLAN interfaces in the same context (see the [“Applying a Service Policy Globally to All VLAN Interfaces in the Same Context”](#) section).

The ACE automatically resets the associated service policy statistics to provide a new starting point for the service policy statistics the next time that you attach a traffic policy to a specific VLAN interface or globally to all VLAN interfaces in the same context.



Note

To apply the policy map globally to all VLAN interfaces in the same context, see the [“Applying a Service Policy Globally to All VLAN Interfaces in the Same Context”](#) section.

Guidelines and Restrictions

The ACE allows only one policy of a specific feature type to be activated on a given interface and only in the input direction.

Detailed Steps

	Command	Purpose
Step 1	config Example: host1/Admin# config host1/Admin(config)#	Enters global configuration mode.
Step 2	interface vlan <i>number</i> Example: host1/Admin(config)# interface vlan 50 host1/Admin(config-if)#	(Optional) Specifies the VLAN to which the remote access policy map is to be applied. The <i>number</i> argument specifies the VLAN. This command enters the interface configuration mode. Note If you want to process ICMPv6 traffic on this interface, you must enter the ipv6 enable command in interface configuration mode.
Step 3	service-policy input <i>policy_name</i> Example: host1/Admin(config-if)# service-policy input REMOTE_MGMT_ALLOW_POLICY no service-policy input <i>policy_name</i> Example: host1/Admin(config-if)# no service-policy input REMOTE_MGMT_ALLOW_POLICY	Attaches the remote access policy map to the specified VLAN only. The <i>policy_name</i> argument specifies the policy map name. To apply the policy map globally to all of the VLANs associated with a context, see the “Applying a Service Policy Globally to All VLAN Interfaces in the Same Context” section.
Step 4	do copy running-config startup-config Example: host1/Admin(config-if)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Command	Purpose
<p>Step 5</p> <pre>do show service-policy [policy_name [detail]]</pre> <p>Example: host1/Admin(config-if)# do show service-policy REMOTE_MGMT_ALLOW_POLICY</p>	<p>(Optional) Displays service policy statistics for all policy maps or a specific Layer 3 and Layer 4 remote network traffic management policy map.</p> <p>The keywords, options, and arguments are as follows:</p> <ul style="list-style-type: none"> <i>policy_name</i>—(Optional) Existing policy map that is currently in service (applied to an interface) as an unquoted text string with a maximum of 64 alphanumeric characters. If you do not enter the name of an existing policy map, the ACE displays information and statistics for all policy maps. detail—(Optional) Displays a more detailed listing of policy map statistics and status information. <p>Note The ACE updates the counters that the show service-policy command displays after the applicable connections are closed.</p>
<p>Step 6</p> <pre>do clear service-policy policy_name</pre> <p>Example: host1/Admin(config-if)# do clear service-policy REMOTE_MGMT_ALLOW_POLICY</p>	<p>(Optional) Clears the service policy statistics for a policy map.</p> <p>For the <i>policy_name</i> argument, enter the identifier of an existing policy map that is currently in service (applied to an interface).</p>

Examples

The following example shows how to specify an interface VLAN for IPv6 and apply the remote access policy map to a VLAN:

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ipv6 enable
host1/Admin(config-if)# ip address 2001:DB8:1::/64
host1/Admin(config-if)# service-policy input REMOTE_MGMT_ALLOW_POLICY
```

The following example shows how to specify an interface VLAN for IPv4 and apply the remote access policy map to a VLAN:

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip address 172.16.1.100 255.255.0.0
host1/Admin(config-if)# service-policy input REMOTE_MGMT_ALLOW_POLICY
```

The following example shows how to display service policy statistics for the REMOTE_MGMT_ALLOW_POLICY policy map:

```
host1/Admin# show service-policy REMOTE_MGMT_ALLOW_POLICY
Status      : ACTIVE
Description: Allow mgmt protocols
-----
Context Global Policy:
  service-policy: REMOTE_MGMT_ALLOW_POLICY
```


Configuring the Maximum Number of Telnet Management Sessions

This section describes how to control the maximum number of Telnet sessions allowed for each context. Telnet remote access sessions are established on the ACE per context. You can create a context, assign an interface and IP address to it, and then log into the ACE by using Telnet to connect to that IP address. This capability allows you to specify a particular context when accessing the ACE. For details on creating users and contexts, see the *Virtualization Guide, Cisco ACE Application Control Engine*.

Guidelines and Restrictions

The ACE supports a total maximum of 256 concurrent Telnet sessions. The ACE supports a maximum 16 concurrent Telnet management sessions for the Admin context and 4 concurrent Telnet management sessions for each user context.

Detailed Steps

	Command	Purpose
Step 1	config Example: host1/Admin# config host1/Admin(config)#	Enters global configuration mode.
Step 2	telnet maxsessions <i>max_sessions</i> Example: host1/Admin(config)# telnet maxsessions 3	(Optional) Specifies the maximum number of concurrent Telnet sessions allowed for the associated context. The <i>max_sessions</i> argument sets the maximum number of concurrent Telnet sessions allowed. The range is from 1 to 16 Telnet sessions for the Admin context and from 1 to 4 Telnet sessions for each user context. The defaults are 16 (Admin context) and 4 (user context).
	no telnet maxsessions Example: host1/Admin(config)# no telnet maxsessions	(Optional) Reverts to the default maximum number of Telnet sessions for the context.
Step 3	do show telnet maxsessions [<i>context_name</i>] Example: host1/Admin(config)# do show telnet maxsessions Maximum Sessions Allowed is 4	(Optional) Displays the maximum number of enabled Telnet sessions. Only context administrators can view Telnet session information associated with a particular context. The optional <i>context_name</i> argument is the name of the context for which you want to view the maximum number of Telnet sessions. The <i>context_name</i> argument is case sensitive.
Step 4	do copy running-config startup-config Example: host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Configuring SSH Management Session Parameters

This section describes how to configure the SSH management session parameters. SSH remote access sessions are established on the ACE per context. You can create a context, assign an interface and IP address to it, and then log into the ACE by using SSH to connect to that IP address. This capability allows you to specify a particular context when accessing the ACE. For details on creating users and contexts, see the *Virtualization Guide, Cisco ACE Application Control Engine*.

This section contains the following topics:

- [Configuring Maximum the Number of SSH Sessions](#)
- [Generating SSH Host Key Pairs](#)

Configuring Maximum the Number of SSH Sessions

This section describes how to control the maximum number of SSH sessions allowed for each context.

Guidelines and Restrictions

The ACE supports a total maximum of 256 concurrent SSH sessions. The ACE supports a maximum 16 concurrent SSH management sessions for the Admin context and 4 concurrent SSH management sessions for each user context.

Detailed Steps

	Command	Purpose
Step 1	config Example: host1/Admin# config host1/Admin(config)#	Enters global configuration mode.
Step 2	ssh maxsessions <i>max_sessions</i> Example: host1/Admin(config)# ssh maxsessions 3	(Optional) Specifies the maximum number of concurrent SSH sessions allowed for the associated context. The <i>max_sessions</i> argument sets the maximum number of concurrent SSH sessions allowed. The range is from 1 to 16 SSH sessions for the Admin context and from 1 to 4 SSH sessions for each user context. The defaults are 16 (Admin context) and 4 (user context).
	no ssh maxsessions Example: host1/Admin(config)# no ssh maxsessions	(Optional) Reverts to the default maximum number of SSH sessions for the context.

	Command	Purpose
Step 3	do show ssh maxsessions [<i>context_name</i>] Example: host1/Admin(config)# do show ssh maxsessions Maximum Sessions Allowed is 4	(Optional) Displays the maximum number of enabled SSH sessions. Only context administrators can view SSH session information associated with a particular context. The optional <i>context_name</i> argument specifies the name of the context for which the context administrator wants to view the maximum number of SSH sessions. The <i>context_name</i> argument is case sensitive.
Step 4	do copy running-config startup-config Example: host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Generating SSH Host Key Pairs

This section describes how to generate an SSH host key pair. The ACE supports remote login over an SSH session that uses private and public key pairs to perform authentication for the context. DSA and RSA keys are generated in pairs—one public key and one private key. With this method of remote connection, use a generated private and public key pair to participate in a secure communication by encrypting and decrypting messages.

The global administrator performs the key generation in the Admin context. All contexts associated with the ACE share the common key. There is only a single host-key pair.

Ensure that you have an SSH host-key pair with the appropriate version before enabling the SSH service (see the “[Configuring Remote Network Management Traffic Services](#)” section). The SSH service accepts three types of key pairs for use by SSH versions 1 and 2. Generate the SSH host key pair according to the SSH client version used. The number of bits specified for each key pair ranges from 768 to 4096.

Detailed Steps

	Command	Purpose
Step 1	changeto Admin Example: host1/context3# changeto Admin host1/Admin#	(Optional) Changes to the Admin context. If you are the administrator or another user authorized in the Admin context, use this command in Exec mode to move to the Admin context. An administrator can perform all allowable functions within the Admin context.
Step 2	config Example: host1/Admin# config host1/Admin(config)#	Enters global configuration mode.

	Command	Purpose
Step 3	hostname <i>name</i> Example: host1/Admin(config)# hostname host1 host1/Admin(config)#	Sets the hostname. This setting is used in the generation of the key. The <i>name</i> argument specifies a new hostname for the ACE. Enter a case-sensitive text string that contains from 1 to 32 alphanumeric characters. For more information about setting the host name, see the “Assigning a Name to the ACE Module” or “Assigning a Name to the ACE Appliance” .
Step 4	ssh key { <i>dsa</i> <i>rsa</i> <i>rsa1</i> } [<i>bits</i> [<i>force</i>]] Example: host1/Admin(config)# ssh key rsa1 1024	Generates the SSH private key and the corresponding public key. The arguments, keywords, and options are as follows: <ul style="list-style-type: none"> • dsa—Generates the DSA key pair for the SSH version 2 protocol. • rsa—Generates the RSA key pair for the SSH version 2 protocol. • rsa1—Generates the RSA1 key pair for the SSH version 1 protocol. • <i>bits</i>—(Optional) Number of bits for the key pair. For DSA, the range is from 768 to 2048. For RSA and RSA1, the range is from 768 to 4096. The greater the number of bits that you specify, the longer it takes to generate the key. The default is 1024. • force—(Optional) Forces the generation of a DSA or RSA key even when previous keys exist. If the SSH key pair option is already generated for the required version, use the force option to overwrite the previously generated key pair.
	no ssh key { <i>dsa</i> <i>rsa</i> <i>rsa1</i> } Example: host1/Admin(config)# no ssh key rsa1	(Optional) Removes the SSH host key pair.
Step 5	do show ssh key [<i>dsa</i> <i>rsa</i> <i>rsa1</i>] Example: host1/Admin(config)# do show ssh key rsa	(Optional) Displays the host key pair details for the specified key or for all keys if you do not specify a key.
Step 6	do copy running-config startup-config Example: host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.
Step 7	exit Example: host1/Admin(config)# exit host1/Admin#	(Optional) Returns to the Exec mode prompt.
Step 8	clear ssh hosts Example: host1/Admin# clear ssh hosts	(Optional) Clears the public keys of all trusted host. These keys are either sent to an SSH client by an SSH server or are entered manually. When a SSH connection is made from the ACE, the SSH client receives the public key and stores it locally.

Examples

The following example shows the **show ssh key** command output:

```
host1/Admin # show ssh key
*****
could not retrieve rsal key information
*****
rsa Keys generated:Tue Mar 7 19:37:17 2006

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEA4v4DQ8aN1482qDTRju9G07hEIxCgTWanPm+WOCU1kihZ
QNd5ZwA50CBAJSfIIIIB4iED6iQbh0kbXSneCvTb5mVoish2wvJrETpIDIEGxxh/jWVsU/MeBbA/7o5tv
gCeT6p7pGF5oUNYFP0OeZ9BiIWDc4jBmYEQLEqJHP+MhSFE=

bitcount:1024
fingerprint:
f5:55:00:18:bc:af:41:74:b6:bc:aa:8e:46:31:74:4f
*****
dsa Keys generated:Tue Dec 20 19:37:17 2005

ssh-dss AAAAB3NzaC1kc3MAAACBAPqDdEqU+0gNtKRXM+DQAXnvcB+H89nq8jA4WgJ7uQcuDCLaG7Lq
jtKtLtJjA6aZVywsQWQ6n4kTlkavZy3cj6PUBSyqvmCTsaYyYo4UQ6CKrK9V+NsfgzTSLWTH8iDUvYjL
c3nU51QEKjy7mPsQeX31y1M1rhp8qhkBMKxkc49XAAAFQCPM0QJrq6+kkaghJpeNxeXhUH9HwAAIEA
keZ1ZJM6sfKqJDYPLHkTro+lpbV9uR4VyYoZmSoehi/LmSaZDq+Mc8UN1LM+i5vkOgnKcearD91M4/hK
zZGYx5hJ0iYCKj/ny2a5p/8HK152cnsOAg6ebkiTTWAprcWrcHDS/1mcaI5GzLrZCd1XW5gBFZtMTJGs
tICmVWjibewAAACBAJQ66zdZQqYiCwtZfmakridEGDtlV6ixIDjBNgb84q1j+Y1XMzqLL0D4oMSb7idE
L3BmhQYQW7hkTK0oS4kVawI1VmW2kvrqoGQnLNQRMvisAXuJWkklLn6vWPGZze8KoALv0GXxsOv2gk/z
TDk01oCaTVw//bXJtoVRgI1WXLIP

bitcount:1024
fingerprint:
8e:13:5c:3e:1a:9c:7a:ed:d0:84:eb:96:12:db:82:be
*****
```

Terminating an Active User Session

This section describes how to terminate an active SSH or Telnet session for the active context.

Detailed Steps

	Command	Purpose
Step 1	show {ssh session-info telnet} Example: host1/Admin# show ssh session-info	(Optional) Displays the session information, including the session ID, of all current SSH or Telnet sessions. The keywords are as follows: <ul style="list-style-type: none"> • ssh session-info—Displays SSH session information. • telnet—Displays Telnet session information.
Step 2	clear {ssh telnet} session_id Example: host1/Admin# clear ssh 345	Terminates a current SSH or Telnet session depending on which command you enter. The argument and keyword are as follows: <ul style="list-style-type: none"> • ssh—Selects an SSH session type. • telnet—Selects a Tenet session type. • session_id—Specifies the identifier of the SSH or Telnet session to disconnect.

Enabling ICMP Messages to the ACE

This section describes how to enable ICMP messages on the ACE. By default, the ACE does not allow ICMP messages to be received by an ACE interface or to pass through the ACE interface. ICMP is an important tool for testing your network connectivity; however, network hackers can also use ICMP to attack the ACE or your network. We recommend that you allow ICMP during your initial testing, but then disallow it during normal operation. The ACE supports both ICMPv4 and ICMPv6.

To permit or deny address(es) to reach an ACE interface with ICMP messages, either from a host to the ACE, or from the ACE to a host which requires the ICMP reply to be allowed back, configure one of the following:

- Class map to provide the ICMP network traffic match criteria for the ACE.
- Policy map to enable ICMP network management access to and from the ACE.
- Service policy to activate the policy map, attach the traffic policy to an interface or globally on all interfaces, and specify the direction in which the policy should be applied.

See the “[Configuring Remote Network Management Traffic Services](#)” section for details on configuring a network management class map, policy map, and service policy for the ACE.

To allow ICMP messages to pass through the ACE, configure an ICMP ACL to permit or deny network connections based on the ICMP type (for example, echo, echo-reply, or unreachable). See the *Security Guide, Cisco ACE Application Control Engine* for details.



Note

If you want only to allow the ACE to ping a host (and allow the echo reply back to the interface), but not allow hosts to ping the ACE, enable the ICMP application protocol inspection function instead of defining a class map and policy map. See the *Security Guide, Cisco ACE Application Control Engine* for details.

Examples

The following example shows how to allow the ACE to receive ICMPv6 pings:

```
host1/Admin(config)# class-map type management match-all ICMPv6_ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# description Allow ICMPv6 packets
host1/Admin(config-cmap-mgmt)# match protocol icmpv6 source-address 2001:DB8:1::/64
host1/Admin(config-cmap-mgmt)# exit
host1/Admin(config)# policy-map type management first-action ICMPv6_ALLOW_POLICY
host1/Admin(config-pmap-mgmt)# class ICMPv6_ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# exit
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ipv6 enable
host1/Admin(config-if)# ip address 2001:DB8:2::/64
host1/Admin(config-if)# service-policy input ICMPv6_ALLOW_POLICY
```

The following example shows how to allow the ACE to receive ICMPv4 pings:

```
host1/Admin(config)# class-map type management match-all ICMP-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# description Allow ICMP packets
host1/Admin(config-cmap-mgmt)# match protocol icmp source-address 172.16.10.0
255.255.255.254
host1/Admin(config-cmap-mgmt)# exit
host1/Admin(config)# policy-map type management first-action ICMP_ALLOW_POLICY
host1/Admin(config-pmap-mgmt)# class ICMP-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# exit
```

```

host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip address 172.16.1.100 255.255.0.0
host1/Admin(config-if)# service-policy input ICMP_ALLOW_POLICY

```

Directly Accessing a User Context Through SSH

This section describes how to configure a user context and enable direct login access to that user context from a remote SSH session. To perform this procedure, you must be the global administrator and in the Admin context. The ACE does not support SSH with IPv6 for remote access.

Task Flow

Follow these steps to first configure the ACE to provide direct access to a user context from SSH and then access the user context:

- Step 1** Create a user context by entering the following command:

```

host1/Admin(config)# context C1
host1/Admin(config-context)#

```

See the *Virtualization Guide, Cisco ACE Application Control Engine*.

- Step 2** Associate an existing VLAN with the user context so that the context can receive traffic classified for it by entering the following command:

```

host1/Admin(config-context)# allocate-interface vlan 100

```

See the *Routing and Bridging Guide, Cisco ACE Application Control Engine*.

- Step 3** Generate the SSH host key pair by entering the following command:

```

host1/Admin(config)# ssh key rsa1 768
generating rsa1 key(768 bits).....
.
generated rsa1 key

```

See the “[Generating SSH Host Key Pairs](#)” section.

- Step 4** Change to the C1 context that you created in Step 1 and enter configuration mode in that context by entering the following commands:

```

host1/Admin(config-context)# do changeto C1
host1/C1(config-context)# exit
host1/C1(config)#

```

Only users authenticated in the Admin context can use the **changeto** command.

- Step 5** Configure the VLAN interface that you allocated to the user context in Step 2 by entering the following commands:

```

host1/C1(config)# interface vlan 50
host1/C1(config-if)# ip address 192.168.1.1 255.255.255.0
host1/C1(config-if)# no shutdown
host1/C1(config-if)# exit
host1/C1(config)#

```

For example, assign an IP address to the interface and reenable the interface within the context with the **no shutdown** command. See the *Routing and Bridging Guide, Cisco ACE Application Control Engine*.

- Step 6** Create an SSH remote management policy and apply the associated service policy to all VLAN interfaces or just to the VLAN interface allocated to the user context by entering the following commands:

```
host1/C1(config)# class-map type management match-all SSH-ALLOW_CLASS
host1/C1(config-cmap-mgmt)# match protocol ssh source-address 172.16.10.0 255.255.255.254
host1/C1(config-cmap-mgmt)# exit
host1/C1(config)#
host1/C1(config)# policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
host1/C1(config-pmap-mgmt)# class SSH-ALLOW_CLASS
host1/C1(config-pmap-mgmt-c)# permit
host1/C1(config-pmap-mgmt-c)# exit
host1/C1(config-pmap-mgmt)# exit
host1/C1(config)# interface vlan 50
host1/C1(config-if)# ip address 192.168.1.1 255.255.255.0
host1/C1(config-if)# service-policy input REMOTE_MGMT_ALLOW_POLICY
host1/C1(config-if)# exit
host1/C1(config)#
```

See the “[Configuring Remote Network Management Traffic Services](#)” section.

- Step 7** Create an IP route by entering the following command:

```
host1/C1(config)# ip route 0.0.0.0 255.255.255.0 192.168.4.8
```

See the *Security Guide, Cisco ACE Application Control Engine*.

- Step 8** Follow these steps to directly access the user context from an SSH client:

- a. From the SSH client, establish a remote SSH session to the IP address of the user context VLAN interface.
- b. Enter the password for the user context VLAN interface. The ACE CLI prompt appears in Exec mode of the user context.

```
host1/C1#
```

Displaying Remote Access Session Information

This section describes how to display remote access session information and includes the following topics:

- [Displaying Telnet Session Information](#)
- [Displaying SSH Session Information](#)
- [Displaying Other Remote Access Session Information](#)

Displaying Telnet Session Information

To display a Telnet session, perform the following task:

Command	Purpose
<code>show telnet [context_name]</code>	Displays information related to the Telnet session. Only the context administrator can view Telnet information associated with a particular context. The optional <i>context_name</i> argument is the name of the context for which you want to view specific Telnet session information. The <i>context_name</i> argument is case sensitive.

Table 3-2 describes the fields in the `show telnet` command output.

Table 3-2 Field Descriptions for the `show telnet` Command

Field	Description
SessionID	Unique session identifier for the Telnet session.
Remote Host	IP address and port of the remote Telnet client.
Active Time	Time since the Telnet connection request was received by the ACE.

Displaying SSH Session Information

To display an SSH session, perform the following task:

Command	Purpose
<code>show ssh session-info [context_name]</code>	Displays information related to the SSH session. Only context administrators can view SSH session information associated with a particular context. The optional <i>context_name</i> argument is the name of the context for which you want to view specific SSH session information. The <i>context_name</i> argument is case sensitive.

Table 3-3 describes the fields in the `show ssh session-info` command output.

Table 3-3 Field Descriptions for the `show ssh session-info` Command

Field	Description
SessionID	Unique session identifier for the SSH session.
Remote Host	IP address and port of the remote SSH client.
Active Time	Time since the SSH connection request was received by the ACE.

Displaying Other Remote Access Session Information

To display other remote access configuration information, perform one of the following tasks:

Command	Purpose
<code>show running-config</code>	Displays the running configuration.
<code>show ssh key [dsa rsa rsa1]</code>	Displays the host key pair details for the specified key or for all keys if you do not specify a key. See the “Generating SSH Host Key Pairs” section.
<code>show ssh maxsessions [context_name]</code>	Displays the maximum number of enabled SSH sessions. Only context administrators can view SSH session information associated with a particular context. See the “Configuring Maximum the Number of SSH Sessions” section.
<code>show telnet maxsessions [context_name]</code>	Displays the maximum number of enabled Telnet sessions. Only context administrators can view Telnet session information associated with a particular context. See the “Configuring the Maximum Number of Telnet Management Sessions” section.

Configuration Example for Enabling Remote Access to the ACE

The following CLI example shows how to configure remote access to the ACE through the use of class maps, policy maps, and service policies with IPv6 management traffic.

-
- Step 1** Create and configure an access control list. The sample access control list shown in this step allows network traffic from any source. For details about configuring an access control list, see the *Security Guide, Cisco ACE Application Control Engine*.
- ```
host1/Admin(config)# access-list ACL1 line 10 extended permit ip anyv6 anyv6
```
- Step 2** Create and configure a class map for network management traffic.
- ```
host1/Admin(config)# class-map type management match-any IPv6 L4_REMOTE_MGT_CLASS
host1/Admin(config-cmap-mgmt)# description Allows ICMPv6 protocol
host1/Admin(config-cmap-mgmt)# 2 match protocol icmpv6 anyv6
host1/Admin(config-cmap-mgmt)# exit
host1/Admin(config)#
```
- Step 3** Create and configure a management policy map that activates the SSH and Telnet management protocol classifications.
- ```
host1/Admin(config)# policy-map type management first-match L4_REMOTE-MGT_POLICY
host1/Admin(config-pmap-mgmt)# class L4_REMOTE-MGT_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# exit
host1/Admin(config)#
```
- Step 4** Alternatively, create and configure a management policy map that matches and permits any IPv6 traffic:
- ```
host1/Admin(config)# policy-map type management first-match L4_REMOTE-MGT_POLICY
host1/Admin(config-pmap-mgmt)# class class-default-v6
```

```

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

```

- Step 5** Apply the traffic policy to a specific VLAN interface or globally to all VLAN interfaces and enable the interface.

Apply to a specific VLAN interface:

```

host1/Admin(config) # interface vlan 100
host1/Admin(config-if) # ipv6 enable
host1/Admin(config-if) # ip address 2001:DB8:1::/64
host1/Admin(config-if) # access-group input ACL1
host1/Admin(config-if) # service-policy input L4_REMOTE-MGT_POLICY
host1/Admin(config-if) # no shutdown
host1/Admin(config-if) # exit
host1/Admin(config) #

```

Apply globally to all VLAN interface:

```

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

```

- Step 6** Save the configuration to Flash memory.

```

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

```

The following example shows how to configure remote access to the ACE through the use of class maps, policy maps, and service policies with IPv4 management traffic.

- Step 1** Enter the configuration mode and set the maximum number of Telnet and SSH sessions.

```

host1/Admin# config
host1/Admin(config) # telnet maxsessions 3
host1/Admin(config) # ssh maxsessions 3

```

- Step 2** Create and configure an access control list. The sample access control list shown in this step allows network traffic from any source. For details about configuring an access control list, see the *Security Guide, Cisco ACE Application Control Engine*.

```

host1/Admin(config) # access-list ACL1 line 10 extended permit ip any any

```

- Step 3** Create and configure a class map for network management traffic.

```

host1/Admin(config) # class-map type management match-any L4_REMOTE-MGT_CLASS
host1/Admin(config-cmap-mgmt) # description Allows Telnet, SSH, and ICMP protocols
host1/Admin(config-cmap-mgmt) # 2 match protocol telnet any
host1/Admin(config-cmap-mgmt) # 3 match protocol ssh any
host1/Admin(config-cmap-mgmt) # 4 match protocol icmp any
host1/Admin(config-cmap-mgmt) # exit
host1/Admin(config) #

```

- Step 4** Create and configure a policy map that activates the SSH and Telnet management protocol classifications.

```

host1/Admin(config) # policy-map type management first-match L4_REMOTE-MGT_POLICY
host1/Admin(config-pmap-mgmt) # class L4_REMOTE-MGT_CLASS
host1/Admin(config-pmap-mgmt-c) # permit
host1/Admin(config-pmap-mgmt-c) # exit
host1/Admin(config-pmap-mgmt) # exit
host1/Admin(config) #

```

- Step 5** Apply the traffic policy to a specific VLAN interface or globally to all VLAN interfaces and enable the interface.

Apply to a specific VLAN interface:

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip address 192.168.1.1 255.255.255.0
host1/Admin(config-if)# access-group input ACL1
host1/Admin(config-if)# service-policy input L4_REMOTE-MGT_POLICY
host1/Admin(config-if)# no shutdown
host1/Admin(config-if)# exit
host1/Admin(config)#
```

Apply globally to all VLAN interface:

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

- Step 6** Generate the SSH private key and corresponding public key for use by the SSH server.

```
host1/Admin(config)# ssh key rsa1 1024 force
```

- Step 7** Save the configuration to Flash memory.

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