



CHAPTER 44

Configuring Network Admission Control

This chapter describes how to configure network admission control (NAC) on the Catalyst 6500 series switches.

**Note**

For complete syntax and usage information for the commands that are used in this chapter, refer to the *Catalyst 6500 Series Switch Command Reference* publication.

**Note**

For information on configuring IEEE 802.1X authentication, see [Chapter 40, “Configuring 802.1X Authentication.”](#)

**Note**

For information on configuring MAC authentication bypass, see [Chapter 41, “Configuring MAC Authentication Bypass.”](#)

**Note**

For information on using port security to block input to an Ethernet, Fast Ethernet, or Gigabit Ethernet port when the MAC address of the station attempting to access the port is different from any of the MAC addresses that are specified for that port, see [Chapter 38, “Configuring Port Security.”](#) That chapter also provides information on using port security to filter the traffic that is destined to or received from a specific host that is based on the host MAC address.

**Note**

For information on configuring authentication, authorization, and accounting (AAA) to monitor and control access to the command-line interface (CLI) on the Catalyst 6500 series switches, see [Chapter 39, “Configuring the Switch Access Using AAA.”](#)

This chapter consists of these sections:

- [Configuring Network Admission Control with LAN Port IP, page 44-2](#)
- [Configuring Network Admission Control with LAN Port 802.1X, page 44-34](#)

Configuring Network Admission Control with LAN Port IP

These sections describe how to configure NAC with LAN port IP:

- [Understanding How Network Admission Control with LAN Port IP Works](#), page 44-2
- [LAN Port IP Posture Validation Summary](#), page 44-5
- [LAN Port IP Hardware and Software Requirements](#), page 44-6
- [LAN Port IP Configuration Guidelines and Restrictions](#), page 44-6
- [Configuring LAN Port IP](#), page 44-8
- [LAN Port IP CLI Command Examples](#), page 44-9
- [Configuring Policy-Based ACLs](#), page 44-21
- [Configuring Inaccessible Authentication Bypass](#), page 44-24
- [LAN Port IP Configuration Example](#), page 44-30
- [LAN Port IP Enhancements in Software Release 8.6\(1\) and Later Releases](#), page 44-32

Understanding How Network Admission Control with LAN Port IP Works

These sections provide an understanding of LAN port IP:

- [Overview](#), page 44-2
- [Virus Infections and Their Effect on Networks](#), page 44-3
- [How Network Admission Control Works](#), page 44-3
- [Network Access Device](#), page 44-3
- [Cisco Trust Agent](#), page 44-4
- [Cisco Secure ACS](#), page 44-4
- [Redirection](#), page 44-5

Overview

NAC addresses the increased threat and impact of worms and viruses to networked businesses. This feature is part of the Cisco Self-Defending Network Initiative that helps customers identify, prevent, and adapt to security threats.

In its initial phase, NAC enables switches and routers to restrict access privileges from an end point that is attempting to connect to a network. The access can be based on information about the end-point device, such as its current antivirus state (version of antivirus software, virus definitions, and version of scan engine).

NAC systems allow noncompliant devices to be denied access, placed in a quarantined area, or given restricted access to computing resources, which keeps insecure nodes from infecting the network.

The key component of the Cisco NAC program is the Cisco Trust Agent (CTA), which resides on an end-point system and communicates with Cisco switches and routers on the network. The CTA collects security state information, such as the type of antivirus software that is used, and communicates this information to Cisco switches and routers. The information is then relayed to a Cisco Secure Access Control Server (ACS) where access control decisions are made. The ACS directs the Cisco switch or router to perform enforcement against the end point.

Virus Infections and Their Effect on Networks

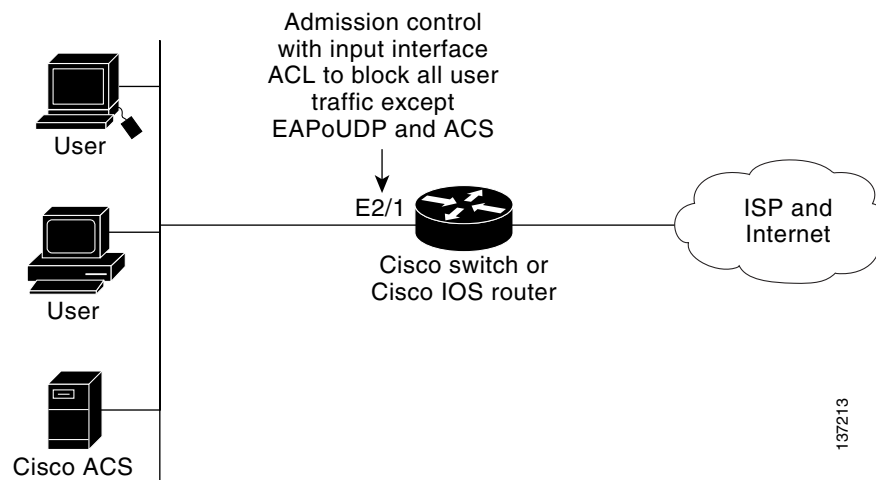
Virus infections are the single largest cause of serious security breaches for networks. Sources of virus infections are insecure end points (for example, PCs, laptops, and servers). Although the end points may have antivirus software installed, the software is often disabled. Even if the software is enabled, the end points may not have the latest virus definitions and scan engines. A larger security risk is from devices that do not have any antivirus software installed.

How Network Admission Control Works

End-point systems, or clients, are hosts on the network, such as PCs, laptops, workstations, and servers. The end-point systems are a potential source of virus infections, and their antivirus states need to be validated before they are granted network access. When an end point attempts an IP connection to a network through an upstream Cisco network access device (Cisco switch or router), the network access device challenges the end point for its antivirus state. The end-point systems run a client called Cisco Trust Agent, which collects antivirus state information from the end device and transports the information to the network access device. This information is then communicated to a Cisco Secure ACS where the antivirus state of the end point is validated and access control decisions are made and returned to network access devices. The network devices either permit, deny, or quarantine the end device. The Cisco Secure ACS may use back-end antivirus vendor-specific servers for evaluating the antivirus state of the end point.

Figure 44-1 shows how Cisco NAC works.

Figure 44-1 Cisco IOS Network Admission Control System



Network Access Device

A network access device (NAD) is a Cisco switch or router (a Layer 3 Extensible Authentication Protocol over UDP [EAPoUDP] access point) that provides connectivity to external networks, such as the Internet or remote enterprise networks.

Cisco Trust Agent

CTA is a specialized software that runs on end-point systems. CTA responds to challenges from the switch or router about the antivirus state of an end-point system. If an end-point system is not running the CTA, the network access device (switch or router) classifies the end-point system as “clientless.”

Cisco Secure ACS

Cisco Secure ACS provides authentication, authorization, and accounting services for NAC using RADIUS authentication. Cisco Secure ACS returns access control decisions to the network access device on the basis of the antivirus credentials of the end-point system.

Using RADIUS `cisco_av_pair` vendor-specific attributes (VSAs), you can set the following attribute-value pairs (AV pairs) on the Cisco Secure ACS. These AV pairs are sent to the network access device with other access-control attributes:

- `url-redirect`—Enables the AAA client to intercept an HTTP request and redirect it to a new URL. This redirection is useful if the result of posture validation indicates that the network access control end point requires an update or patch that you have made available on a remediation web server. For example, a user can be redirected to a remediation web server to download and apply a new virus Directory Administration Tool (DAT) file or an operating system patch as follows:

```
url-redirect=http://10.1.1.1
```

`URL-redirect` for audit support—The audit function is for hosts that do not have Cisco CTA enabled. The audit can be triggered by the ACS by sending down a policy required for audit when there is a clientless authentication done by the network access device (NAD). The audit is accomplished by sending down the audit server’s URL as the `URL-redirect` policy for the host. When HTTP traffic is seen from the host, it is given the URL of the audit server. The policy that is configured through policy-based ACLs (PBACLs) allows communication between the audit server and the host. The session timeout is typically small for the audit to complete and when this timeout expires, a revalidation occurs and the NAD sends the previously received state attribute to the ACS to bring down a new policy. If the audit is not finished during this session timeout, the ACS sends another short session timeout and this process continues until an audit posture token is received. If the process never completes or is taking too long, the audit server returns an “error” posture token to the ACS.

- `posture-token`—Enables Cisco Secure ACS to send a text version of a system posture token (SPT) that is derived by posture validation. The SPT is always sent in numeric format. Using the `posture-token` AV pair makes it easier to view the result of a posture validation request on the AAA client as follows:

```
posture-token=Healthy
```

Valid SPTs, in order from best to worst, are as follows:

- Healthy
- Checkup
- Quarantine
- Infected
- Unknown

Posture validation, or posture assessment, refers to the act of applying a set of rules to posture data to provide an assessment of the level of trust that you can place in an endpoint. The term posture is used to refer to the collection of attributes that play a role in the conduct and health of the endpoint

device that is seeking access to the network. Some of these attributes relate to the endpoint device-type and operating system; other attributes belong to various security applications that might be present on the endpoint, such as antivirus (AV) scanning software. The posture token is one of the conditions in the authorization rules for network access. Posture validation, together with traditional user authentication, provides a complete security assessment of the endpoint device and the user.

- `status-query-timeout`—Overrides the `status-query` default value of the AAA client with the value that you specify, in seconds, as follows:

```
status-query-timeout=150
```

For more information about AV pairs that are supported by Cisco software, see the documentation for the releases of software that are implemented on your AAA clients.

Redirection

NAC supports HTTP redirection that redirects any HTTP request from the end-point device to a specified redirect address. This support mechanism redirects all HTTP requests from a source to a specified web page (URL) to which the latest antivirus files can be downloaded. You must set the value of the `url-redirect` VSA on the ACS and, correspondingly, associate an access control entry in the downloadable ACL that permits the access of the end-point system to the redirect URL address.

LAN Port IP Posture Validation Summary

LAN port IP allows posture-validating end-user devices to access the network based on their posture. End-user devices are classified into one of five possible states after posture validation: healthy, checkup, quarantine, infected, or unknown. Network access is given depending on the device's posture.

LAN port IP enforcement mechanisms include URL redirection and auditing. PBACLs are used for enforcing network access.

The basic steps in posture validation are as follows:

1. The NAD learns the MAC and IP address bindings using ARP inspection and/or DHCP snooping.

**Note**

If you use DHCP triggering for posture validation, you must also enable ARP inspection. If ARP inspection is not enabled, the posture validation completes but the session is torn down within a few minutes because the ARP probe replies from the client are not seen by the EAP Over UDP (EOU) state machinery.

2. The NAD sends an EOU hello request to the host.
3. If the host is running CTA, it responds back with a hello response.
4. The NAD sends an EOU validate identity request.
5. The CTA responds back with an EOU validate response.
6. The NAD extracts the EAP packet from the EOU, embeds it in the RADIUS access request, and sends it to the authentication server (such as the ACS).
7. The ACS sends back an access challenge that is relayed back to the CTA in the form of an EOU validate packet.
8. Step 6 and Step 7 continue until the ACS sends a success or failure response for the posture validation session.

9. If it is a success, the ACS sends the posture token VSA and a policy associated with the posture that includes the PBACL groups, session timeout, status query timeout, and authenticated username.

If the host does not respond to the EOU hello requests that are sent by the NAD, the NAD (after a preconfigured number of attempts), declares the host as clientless (no CTA). The NAD does a pseudo authentication on behalf of the host and brings down a policy. Other posture validation mechanisms, such as an audit, may be triggered.

In the clientless mode, the NAD sends three EOU hello messages (by default) before declaring that the host does not have a CTA. This process could take 90 seconds for doing a clientless authentication and installing that policy. To avoid this delay on a port that you know does not have a CTA, you can set the port mode to bypass using the per-port CLI (enter the **set port eou mod/port bypass** command). When this action is done, the port immediately does a clientless authentication when it learns a new IP address.

Exceptions are hosts that should not attempt posture validation because they are not capable. When a host that has been specified as an exception is detected, a preconfigured policy is installed.

LAN Port IP Hardware and Software Requirements

Follow these hardware and software requirements when configuring LAN port IP:

- You must have a Catalyst 6500 series switch running software release 8.5(1) or later releases.
- You must have CTA installed on the end-point devices (for example, on PCs and laptops).
- You must have an ACS for AAA.

LAN Port IP Configuration Guidelines and Restrictions

Follow these configuration guidelines and restrictions when configuring LAN port IP:

- You must be familiar with configuring access control lists (ACLs) and policy-based ACLs (PBACLs).
- You should be familiar with configuring authentication, authorization, and accounting (AAA).
- LAN port IP works with other security features such as 802.1X, MAC authentication bypass, and web-based proxy authentication. The restrictions that apply to 802.1X ports also apply to LAN port IP ports as follows:
 - LAN port IP can be configured on access ports only; it cannot be configured on trunk ports.
 - LAN port IP ports cannot be part of an EtherChannel.
 - LAN port IP cannot be enabled with dynamic ports.
 - LAN port IP can be enabled on Ethernet ports only.
 - LAN port IP ports cannot be SPAN destination ports.
 - LAN port IP ports cannot be part of a private VLAN.



Note With software release 8.6(1) and later releases, LAN port IP ports can be part of a private VLAN. For more information, see the [“Configuring LAN Port IP on Private VLAN Ports” section on page 44-34.](#)

- LAN port IP, when enabled with any authentication feature such as 802.1X or MAC authentication bypass, is initialized only after the authentication is finished.

- 802.1X—802.1X authentication may apply a Layer 2 policy, such as a VLAN assignment, and can also bring Layer 3 policy attributes, such as policy-based ACLs (PBACLs), to a port. A LAN port IP policy consists only of the policy-group membership that is downloaded from the RADIUS server.
- Multihost and multiauthentication modes are not supported—802.1X with LAN port IP is supported only in single-host mode.
- Auxiliary VLANs—LAN port IP is supported on multi-VLAN access ports.
- Guest VLANs and the authentication failure VLAN—When LAN port IP is configured with these two features, the LAN port IP operation differs only in that the IP address that it gets for posture validation is from the guest VLAN or authentication failure VLAN.
- DHCP snooping and/or ARP inspection—IP learning is through ARP inspection or DHCP snooping. You must enable at least one of these features for LAN port IP to work. These features are required to trigger LAN port IP (you must map a PBACL containing the ACEs of these features to the VLAN that the LAN port IP port resides in). If you do not enable one of these features, a Layer 2 switch cannot learn new IP addresses that appear on a port.



Note If you use DHCP triggering for posture validation, you must also enable ARP inspection. If ARP inspection is not enabled, the posture validation completes but the session is torn down within a few minutes because the ARP probe replies from the client are not seen by the EOU state machinery.



Note Supervisor Engine 1 does not support ARP inspection. With a Supervisor Engine 1, you must enable DHCP snooping.

- Port security—LAN port IP works with port security. Only port security-validated MAC addresses are allowed to go through posture validation. If a port security violation occurs and results in a port shutdown, the LAN port IP state of the port is also cleared. When you configure an authentication feature, the authenticating feature gives the MAC address to port security to secure if it has been successfully authenticated and then LAN port IP is initialized.
- Security ACLs (VACLs)—Security ACLs are used as PBACLs and PBACLs are supported in VACL mode only with LAN port IP.
- MAC authentication bypass—LAN port IP is initialized only after a successful authentication using MAC authentication bypass, 802.1X, or web-based proxy authentication.
- Web-based proxy authentication—LAN port IP is initialized only after web-based proxy authentication completes verifying identity credentials. In the web-based proxy authentication state, a port waits indefinitely for authentication to complete. In this stage, only DHCP and DNS are allowed to go through. The ACL configured on the interface handles the redirecting of HTTP traffic. The PBACL configured on the interface should ensure that any other traffic is not allowed.

Configuring LAN Port IP

This section describes how to configure LAN port IP.



Note

To display LAN port IP configuration information and to clear LAN port IP configuration elements, see the “[LAN Port IP CLI Command Examples](#)” section on page 44-9. To configure policy-based ACLs (PBACLs), see the “[Configuring Policy-Based ACLs](#)” section on page 44-21.



Note

For assistance in following these configuration steps, see the “[LAN Port IP Configuration Example](#)” section on page 44-30.

To configure LAN port IP, perform these steps:

- Step 1** Enable LAN port IP globally on the switch by entering the **set eou {enable | disable}** command (the default is disabled).
- ```
Console> (enable) set eou enable
EoU globally enabled.
Console> (enable)
```
- Step 2** Enable LAN port IP on a per-port basis by entering the **set port eou mod/port {bypass | auto | disable | initialize | revalidate}** command.
- ```
Console> (enable) set port eou 7/1 auto
EoU enabled on 7/1
Console> (enable)
```
- Step 3** Define the RADIUS server and RADIUS key by entering the following commands:
- ```
set radius server ip_addr [auth-port port] [acct-port port] [primary]
set radius key key
```
- This example shows how to define the RADIUS server:
- ```
Console> (enable) set radius server 10.76.39.93 auth-port 1812 primary
10.76.39.93 with auth-port 1812 acct-port 1813 added to radius server table as primary
server.
Console> (enable)
```
- This example shows how to define the RADIUS key:
- ```
Console> (enable) set radius key cisco
Radius key set to cisco
Console> (enable)
```
- Step 4** Define a policy-based ACL (PBACL) and map it to a VLAN as follows:
- Enable DHCP snooping and/or ARP inspection:
 

```
set security acl ip acl-name permit dhcp-snooping
set security acl ip acl-name permit arp-inspection
```
  - Enable EAPoUDP redirection:
 

```
set security acl ip acl-name permit eapoudp
```

- c. Define other policy statements using policy groups that correspond to various LAN port IP states as follows:
- ```
set security acl ip NACACL permit ip group healthy_hosts any
set security acl ip NACACL deny ip group infected_hosts any
set security acl ip NACACL permit ip group exception_hosts any
set security acl ip NACACL permit ip group clientless_hosts host 10.76.39.100
```
- d. For URL redirection, apply this ACE at an appropriate position:
- ```
set security acl ip NACACL permit url-redirect
```
- Step 5** For clientless nonresponsive hosts (NRH hosts), enable the clientless functionality by entering the **set eou allow clientless enable** command.
- Step 6** Define a policy for NRH hosts. The specified groups should also be present in the ACL that is defined in the previous steps:
- ```
set policy name exception_policy group exception_hosts
```
- Step 7** Specify an exception host and assign the policy by entering the **set eou authorize ip 77.0.0.90 policy exception_policy** command.
- Step 8** Configure the RADIUS server. For RADIUS server configuration details, refer to the *Implementing Network Admission Control Phase One Configuration and Deployment* publication at this URL:
<http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/ImplNAC/ImpNAC.html>
 Ensure that the policy groups that are used in the ACLs are configured with the posture-token VSA, such as 26/9/1 sec:pg=healthy_hosts.
 If you define a policy group in ACS but the VACL that is mapped to the VLAN does not refer to that group, posture validation will fail because the policy installation fails.
- Step 9** Ensure that the sc0 interface is configured with a proper IP address by entering these commands:
- ```
set interface {sc0 | sl0 | sc1} {up | down}
set interface sc0 [vlan] [ip_addr/netmask [broadcast]]
```
- Step 10** Ensure that there is a default router in the VLAN to which the host is connected. If there is no default router, you need a static ARP on the host for the sc0 IP address.
- Step 11** If the host and the management interface (sc0) are in the same VLAN, and you have a VACL configured for that VLAN, you should configure an ACE to allow traffic to the RADIUS server from the switch IP address.

## LAN Port IP CLI Command Examples

This section describes how to configure the LAN port IP CLI:

- [Enabling or Disabling LAN Port IP Globally, page 44-10](#)
- [Enabling or Disabling the Bypassing of LAN Port IP Posture Validation for Clientless Hosts, page 44-11](#)
- [Statically Authorizing an IP Address as an Exception Host Device and Applying a Policy to the Device, page 44-11](#)

- [Statically Authorizing a MAC Address as an Exception Host Device and Applying a Policy to the Device, page 44-11](#)
- [Restarting a Host's State Machine, page 44-12](#)
- [Specifying the CTA Packet Retransmit Time and RADIUS Server Retransmit Time, page 44-12](#)
- [Revalidating a Host, page 44-13](#)
- [Enabling or Disabling EOU Logging for LAN Port IP Events, page 44-13](#)
- [Setting EAPOUDP-Related Timers, page 44-14](#)
- [Setting EOU Rate Limiting, page 44-14](#)
- [Enabling or Disabling EOU RADIUS Accounting, page 44-15](#)
- [Bypassing, Disabling, or Enabling LAN Port IP on a Per-Port Basis, page 44-15](#)
- [Initializing LAN Port IP on a Per-Port Basis, page 44-15](#)
- [Revalidating LAN Port IP on a Per-Port Basis, page 44-16](#)
- [Redirecting LAN Port IP Control Packets to the Supervisor Engine, page 44-16](#)
- [Displaying the Global EOU Configuration, page 44-16](#)
- [Displaying a Summary of the LAN Port IP State on All LAN Port IP-Enabled Ports, page 44-17](#)
- [Displaying a Summary of the LAN Port IP State on a Per-Port Basis, page 44-17](#)
- [Displaying Host-Specific Information, page 44-18](#)
- [Displaying EOU Authentication-Related Information, page 44-18](#)
- [Displaying the EOU Log, page 44-19](#)
- [Displaying the EOU Results on a Posture-Token Basis, page 44-19](#)
- [Clearing the LAN Port IP Configuration, page 44-19](#)
- [Clearing All the Host EOU Sessions, page 44-20](#)
- [Clearing the LAN Port IP Session for a Particular Host, page 44-20](#)
- [Clearing an IP Address from an Exception Group or Clearing an Exception Group, page 44-20](#)
- [Clearing EAPOUDP-Related Timers to Their Default Values, page 44-21](#)
- [Clearing the CTA Packet Retransmit Time, page 44-21](#)

## Enabling or Disabling LAN Port IP Globally

To globally enable or disable LAN port IP on the switch, perform this task in privileged mode (the default is disabled):

| Task                                                  | Command                                 |
|-------------------------------------------------------|-----------------------------------------|
| Globally enable or disable LAN port IP on the switch. | <code>set eou {enable   disable}</code> |

This example shows how to globally enable LAN port IP on the switch:

```
Console> (enable) set eou enable
EoU globally enabled.
Console> (enable)
```

## Enabling or Disabling the Bypassing of LAN Port IP Posture Validation for Clientless Hosts

To globally enable or disable the bypassing of the LAN port IP posture validation for clientless hosts, perform this task in privileged mode (the default is disable):

| Task                                                                                        | Command                                            |
|---------------------------------------------------------------------------------------------|----------------------------------------------------|
| Enable or disable the bypassing of the LAN port IP posture validation for clientless hosts. | <b>set eou allow clientless {enable   disable}</b> |

This example shows how to enable the bypassing of the LAN port IP posture validation for clientless hosts:

```
Console> (enable) set eou allow clientless enable
EoU Clientless hosts will be allowed
Console> (enable)
```

## Statically Authorizing an IP Address as an Exception Host Device and Applying a Policy to the Device

This command allows a specific IP address to be treated as an exception host and when that host is detected, it will dynamically install the policy specified by the policy name.



**Note**

If the policy template does not exist, entering these commands creates the policy template.

To statically authorize an IP device and apply an associated policy to the device, perform this task in privileged mode:

| Task                                                                            | Command                                                                                                                                                     |
|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Statically authorize an IP device and apply an associated policy to the device. | <b>set eou authorize ip <i>ip_addr</i> policy <i>policy_name</i></b><br><b>set eou authorize ip <i>ip_addr</i> <i>ip_mask</i> policy <i>policy_name</i></b> |

This example shows how to statically authorize an IP device and apply an associated policy to the device:

```
Console> (enable) set eou authorize ip 172.20.52.19 255.255.255.224 policy poll
Mapped IP address 172.20.52.0 IP mask 255.255.255.224 to policy name poll
Console> (enable)
```

## Statically Authorizing a MAC Address as an Exception Host Device and Applying a Policy to the Device

This command allows a specific MAC address to be treated as an exception host and when that host is detected, it will dynamically install the policy specified by the policy name.



**Note**

If the policy template does not exist, entering these commands creates the template.

To statically authorize a device using the device MAC address and apply an associated policy to the device, perform this task in privileged mode:

| Task                                                                                                     | Command                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Statically authorize a device using the device MAC address and apply an associated policy to the device. | <pre>set eou authorize mac-address mac_address policy policy_name set eou authorize mac-address mac_address mac_mask policy policy_name</pre> |

This example shows how to statically authorize a device using the device MAC address and apply an associated policy to the device:

```
Console> (enable) set eou authorize mac-address 03-56-B7-45-65-56 policy poll
Mapped MAC 03-56-b7-45-65-56 to policy name poll.
Console> (enable)
```

## Restarting a Host's State Machine

To restart a host's state machine, perform this task in privileged mode:

| Task                            | Command                                                                                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restart a host's state machine. | <pre>set eou initialize all set eou initialize authentication { clientless   eap   static } set eou initialize ip ip-address set eou initialize mac mac-address set eou initialize posture-token posture-token</pre> |

This example shows how to restart a host's state machine using the IP address:

```
Console> (enable) set eou initialize ip 172.20.52.19
Initializing Eou for ipAddress 172.20.52.19
Console> (enable)
```

## Specifying the CTA Packet Retransmit Time and RADIUS Server Retransmit Time

To specify the number of times that a packet is retransmitted to the CTA before declaring the CTA as nonresponsive, and to specify the RADIUS server retransmit time, perform this task in privileged mode (the default is 3 and the range is 1 through 10):

| Task                                                                                                                                                            | Command                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| Specify the number of times that a packet is retransmitted to the CTA before declaring the CTA as nonresponsive, and specify the RADIUS server retransmit time. | <pre>set eou max-retry max-retry</pre> |

This example shows how to specify the number of times that a packet is retransmitted to the CTA before declaring the CTA as nonresponsive, and specify the RADIUS server retransmit time:

```
Console> (enable) set eou max-retry 6
eou max-retry set to 6.
Console> (enable)
```

## Revalidating a Host

To revalidate a host, perform this task in privileged mode:

| Task               | Command                                                                                                                                                                                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Revalidate a host. | <pre><b>set eou revalidate all</b> <b>set eou revalidate authentication { clientless   eap   static }</b> <b>set eou revalidate ip ip-address</b> <b>set eou revalidate mac mac-address</b> <b>set eou revalidate posture-token posture-token</b></pre> |

This example shows how to revalidate all clientless hosts:

```
Console> (enable) set eou revalidate authentication clientless
Revalidate all clientless hosts
Console> (enable)
```

## Enabling or Disabling EOU Logging for LAN Port IP Events

To enable or disable EOU logging for LAN port IP events, perform this task in privileged mode (the default is disable):

| Task                                                  | Command                                                |
|-------------------------------------------------------|--------------------------------------------------------|
| Enable or disable EOU logging for LAN port IP events. | <pre><b>set eou logging { enable   disable }</b></pre> |

This example shows how to enable EOU logging for LAN port IP events:

```
Console> (enable) set eou logging enable
EoU Logging enabled
Console> (enable)
```

## Setting EAPOUDP-Related Timers

To set EAPOUDP-related timers, perform this task in privileged mode:

| Task                        | Command                                                                                                                                                                                                                                                                  |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Set EAPOUDP-related timers. | <pre>set eou timeout aaa <i>aaa-timeout</i> set eou timeout hold-period <i>hold-timeout</i> set eou timeout retransmit <i>retransmit-timeout</i> set eou timeout revalidation <i>revalidation-timeout</i> set eou timeout status-query <i>status-query-timeout</i></pre> |

The timer defaults and ranges are as follows:

- `aaa`—The default is 60 seconds; the range is 1 through 60 seconds.
- `hold-period`—The default is 180 seconds; the range is 60 through 86400 seconds.
- `retransmit`—The default is 3 seconds; the range is 1 through 60 seconds.
- `revalidation`—The default is 36000 seconds; the range is 5 through 86400 seconds.
- `status-query`—The default is 300 seconds; the range is 30 through 1800 seconds.

This example shows how to set the revalidation timer to 200 seconds:

```
Console> (enable) set eou timeout revalidation 200
Console> (enable)
```

## Setting EOU Rate Limiting

To set EOU rate limiting (the default is 0 and the range is 10 through 200), perform this task in privileged mode:



### Note

The default rate limit value of 0 disables rate limiting. With rate limiting disabled, there is no limit on simultaneous LAN port IP authentication sessions.

| Task                   | Command                                        |
|------------------------|------------------------------------------------|
| Set EOU rate limiting. | <pre>set eou rate-limit <i>ratelimit</i></pre> |

This example shows how to set EOU rate limiting to 40:

```
Console> (enable) set eou rate-limit 40
eou ratelimit set to 40.
Console> (enable)
```

## Enabling or Disabling EOU RADIUS Accounting

To enable or disable EOU RADIUS accounting, perform this task in privileged mode:

| Task                                     | Command                                             |
|------------------------------------------|-----------------------------------------------------|
| Enable or disable EOU RADIUS accounting. | <b>set eou radius-accounting {enable   disable}</b> |

This example shows how to enable EOU RADIUS accounting:

```
Console> (enable) set eou radius-accounting enable
Radius Accounting for Eou Enabled.
Console> (enable)
```

## Bypassing, Disabling, or Enabling LAN Port IP on a Per-Port Basis

You can bypass, disable, or enable LAN port IP on a per-port basis. Specifying **auto** mode enables LAN port IP automatically if a client is found.

To bypass, disable, specify auto mode, or set the aaa-fail policy for LAN port IP on a per-port basis, perform this task in privileged mode:

| Task                                                                                                | Command                                                                                            |
|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Bypass, disable, specify auto mode, or set the aaa-fail policy for LAN port IP on a per-port basis. | <b>set port eou mod/port {aaa-fail-policy   auto   bypass   disable   initialize   revalidate}</b> |

This example shows how to enable an aaa-fail policy on a port:

```
Console> (enable) set port eou 1/2 aaa-fail-policy test_policy
Policy test_policy mapped as aaa-fail-policy on port 1/2
Console> (enable)
```

This example shows how to enable LAN port IP on port 5/1:

```
Console> (enable) set port eou 5/1 auto
EoU enabled on 5/1
Console> (enable)
```

This example shows how to set port 7/1 to bypass mode:

```
Console> (enable) set port eou 7/1 bypass

Eou Bypass enabled on 7/1
Console> (enable)
```

## Initializing LAN Port IP on a Per-Port Basis

To initialize LAN port IP on a per-port basis, perform this task in privileged mode:

| Task                                        | Command                                 |
|---------------------------------------------|-----------------------------------------|
| Initialize LAN port IP on a per-port basis. | <b>set port eou mod/port initialize</b> |

This example shows how to initialize LAN port IP on port 7/1:

```
Console> (enable) set port eou 7/1 initialize
Initializing EoU for all hosts on port 7/1
Console> (enable)
```

## Revalidating LAN Port IP on a Per-Port Basis

To revalidate LAN port IP on a per-port basis, perform this task in privileged mode:

| Task                                        | Command                                 |
|---------------------------------------------|-----------------------------------------|
| Revalidate LAN port IP on a per-port basis. | <b>set port eou mod/port revalidate</b> |

This example shows how to revalidate LAN port IP on port 7/1:

```
Console> (enable) set port eou 7/1 revalidate
Re-validating EoU for all hosts on port 7/1
Console> (enable)
```

## Redirecting LAN Port IP Control Packets to the Supervisor Engine

To redirect all LAN port IP control packets to the supervisor engine (EAP over UDP packets), perform this task in privileged mode:

| Task                                                                                      | Command                                                                                          |
|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Redirect all LAN port IP control packets to the supervisor engine (EAP over UDP packets). | <b>set security acl ip acl_name permit eapoudp ip_mask [before   modify] ace_insert_position</b> |

This example shows how to redirect all LAN port IP control packets to the supervisor engine (EAP over UDP packets):

```
Console> (enable) set security acl ip test permit eapoudp mask1 before pos1
Successfully configured EAPoUDP ACL test. Use 'commit' command to save changes
```

## Displaying the Global EOU Configuration

To display the global EOU configuration, perform this task in normal mode:

| Task                                  | Command                |
|---------------------------------------|------------------------|
| Display the global EOU configuration. | <b>show eou config</b> |

This example shows how to display the global EOU configuration:

```
Console> (enable) show eou config
Eou Protocol Version : 1
Eou Global Config

Eou Global Enable : Enabled
Eou Clientless : Disabled
Eou Logging : Enabled
```

```

Eou Radius Accounting : Enabled
Eou MaxRetry : 3
Eou AAA timeout : 60
Eou Hold timeout : 180
Eou Retransmit timeout : 30
Eou Revalidation timeout : 3600
Eou Status Query timeout : 300
Eou Rate Limit : 40
Eou Udp Port : 21862

Ip Exception List and Policies

0.0.0.18 255.255.255.224 TEST

Console> (enable)

```

## Displaying a Summary of the LAN Port IP State on All LAN Port IP-Enabled Ports

To display a summary of the LAN port IP state on all LAN port IP-enabled ports, perform this task in normal mode:

| Task                                                                         | Command             |
|------------------------------------------------------------------------------|---------------------|
| Display a summary of the LAN port IP state on all LAN port IP-enabled ports. | <b>show eou all</b> |

This example shows how to display a summary of the LAN port IP state on all LAN port IP-enabled ports:

```

Console> (enable) show eou all
Eou Summary

Eou Global State = enabled

Currently Validating EOU Sessions = 0
mNo/pNo Host Ip Nac-Token Host_Fsm_State Username
----- -
Console> (enable)

```

## Displaying a Summary of the LAN Port IP State on a Per-Port Basis

To display a summary of the LAN port IP state on a per-port basis for LAN port IP-enabled ports, perform this task in normal mode:

| Task                                                                                          | Command                       |
|-----------------------------------------------------------------------------------------------|-------------------------------|
| Display a summary of the LAN port IP state on a per-port basis for LAN port IP-enabled ports. | <b>show port eou mod/port</b> |

This example shows how to display a summary of the LAN port IP state on port 7/1:

```

Console> (enable) show port eou 7/1
Port EOU-State IP Address MAC Address
----- -
7/1 bypass - -

Port FSM State Auth Type SQ-Timeout Session Timeout

```

```

7/1 - - - -
Port Posture URL Redirect

7/1 - -
Port Termination action Session id

7/1 - -
Console> (enable)

```

## Displaying Host-Specific Information

To display host-specific information, perform this task in normal mode:

| Task                               | Command                                                                               |
|------------------------------------|---------------------------------------------------------------------------------------|
| Display host-specific information. | <b>show eou host {ip   mac} value</b><br><b>show eou host mac_address mac_address</b> |

This example shows how to display host-specific information:

```

Console> (enable) show eou host 9.6.2.15
HostIP HostMac Port Posture-token

9.6.2.15 00-11-85-8d-bf-ab 2/5 Healthy
IP Address Eou State AuthType SQTimeout SessTimeout

9.6.2.15 authenticated eap 301 3600
Console> (enable)

```

## Displaying EOU Authentication-Related Information

To display the following authentication-related information, perform this task in normal mode:

- **clientless**—Display all clientless ports
- **eap**—Display all ports with EAP authentication
- **static**—Display all hosts in the exception list

| Task                                        | Command                                                    |
|---------------------------------------------|------------------------------------------------------------|
| Display authentication-related information. | <b>show eou authentication {clientless   eap   static}</b> |

This example shows how to display authentication-related information:

```

Console> (enable) show eou authentication eap
Host IP HostMac Port Posture-token

9.6.2.15 00-11-85-8d-bf-ab 2/5 Healthy
IP Address Eou State AuthType SQTimeout SessTimeout

9.6.2.15 authenticated eap 301 3600

```

```
Console> (enable)
```

## Displaying the EOU Log

To display the EOU log, perform this task in normal mode:

| Task                 | Command             |
|----------------------|---------------------|
| Display the EOU log. | <b>show eou log</b> |

This example shows how to display the EOU log:

```
Console> (enable) show eou log
LPIP-EVENT : New ip on port 3/12 9.9.150.21 from Arp-inspection
LPIP-ERROR : Failure to get host information for 9.9.143.20
LPIP-EVENT : Host 9.9.150.34 moved to EAPOUDP_TX_HELLO state
Console> (enable)
```

## Displaying the EOU Results on a Posture-Token Basis

To display the EOU results on a posture-token basis, perform this task in normal mode:

| Task                                              | Command                                            |
|---------------------------------------------------|----------------------------------------------------|
| Display the EOU results on a posture-token basis. | <b>show eou posture-token</b> <i>posture_token</i> |

## Clearing the LAN Port IP Configuration

To clear the LAN port IP configuration and return to default values, perform this task in privileged mode:

| Task                                                              | Command                 |
|-------------------------------------------------------------------|-------------------------|
| Clear the LAN port IP configuration and return to default values. | <b>clear eou config</b> |

This example shows how to clear the LAN port IP configuration and return to default values:

```
Console> (enable) clear eou config
This command will disable EoU on all ports and take EoU parameter values back to defaults.
Do you want to continue (y/n) [n]? y
Console> (enable)
```

## Clearing All the Host EOU Sessions

This command clears all the host EOU sessions learned on all the ports. It does not clear the EOU configuration.

To clear all the host EOU sessions learned on all the ports, perform this task in privileged mode:

| Task                                                      | Command              |
|-----------------------------------------------------------|----------------------|
| Clear all the host EOU sessions learned on all the ports. | <b>clear eou all</b> |

This example shows how to clear all the host EOU sessions learned on all the ports:

```
Console> (enable) clear eou all
Console> (enable)
```

## Clearing the LAN Port IP Session for a Particular Host

To clear the LAN port IP session for a particular host by MAC address or IP address, perform this task in privileged mode:

| Task                                                                              | Command                                                          |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------|
| Clear the LAN port IP session for a particular host by MAC address or IP address. | <b>clear eou host</b> { <i>ip-address</i>   <i>mac-address</i> } |

This example shows how to clear an EOU session for a host with a specified IP address:

```
Console> (enable) clear eou host 9.9.10.10
EOU session of host with IP 9.9.10.10 cleared.
Console> (enable)
```

## Clearing an IP Address from an Exception Group or Clearing an Exception Group

To clear an IP address from an exception group or clear an exception group, perform this task in privileged mode:

| Task                                                                     | Command                                                                                             |
|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Clear an IP address from an exception group or clear an exception group. | <b>clear eou authorize ip</b> <i>ip-address</i> <b>policy</b> <i>policy_name</i>                    |
|                                                                          | <b>clear eou authorize ip</b> <i>ip-address ip_mask</i> <b>policy</b> <i>policy_name</i>            |
|                                                                          | <b>clear eou authorize mac-address</b> <i>mac_address</i> <b>policy</b> <i>policy_name</i>          |
|                                                                          | <b>clear eou authorize mac-address</b> <i>mac_address mac_mask</i> <b>policy</b> <i>policy_name</i> |

This example shows how to clear an IP address from an exception group:

```
Console> (enable) clear eou authorize ip 10.1.1.1 255.255.255.240 policy pol1
Cleared host 10.1.1.1 255.255.255.240 from exception group and removed its policy mapping.
Console> (enable)
```

## Clearing EAPOUDP-Related Timers to Their Default Values

To clear EAPOUDP-related timers to their default values, perform this task in privileged mode:

| Task                                                  | Command                                                                                 |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Clear EAPOUDP-related timers to their default values. | <b>clear eou timeout [aaa   hold-period   retransmit   revalidation   status-query]</b> |

This example shows how to clear the hold-period timers to their default values:

```
Console> (enable) clear eou timeout hold-period
Console> (enable)
```

## Clearing the CTA Packet Retransmit Time

To clear the global CTA packet retransmit time, perform this task in privileged mode (this command sets the retransmit time back to the default value of 3):

| Task                                         | Command                    |
|----------------------------------------------|----------------------------|
| Clear the global CTA packet retransmit time. | <b>clear eou max-retry</b> |

This example shows how to clear the global CTA packet retransmit time:

```
Console> (enable) clear eou max-retry
Eou max-retry set to 3
Console> (enable)
```

## Configuring Policy-Based ACLs

This section describes how to configure policy-based ACLs (PBAcls):

- [Adding IP Addresses to Existing Policy Groups, page 44-22](#)
- [Adding a Policy Group to the Policy Template, page 44-22](#)
- [Clearing an IP Address from a Policy Group, page 44-22](#)
- [Clearing a Policy Group from a Policy Template, page 44-23](#)
- [Displaying Policy Group Information, page 44-23](#)
- [Displaying Policy Templates and Their Associated Policy Groups, page 44-24](#)

## Adding IP Addresses to Existing Policy Groups

This command allows you to add an IP address to an existing policy group. The command fails if the group name is not already present in the group database.

To add an IP address to an existing policy group, perform this task in privileged mode:

| Task                                           | Command                                                                       |
|------------------------------------------------|-------------------------------------------------------------------------------|
| Add an IP address to an existing policy group. | <b>set policy group</b> <i>group-name</i> <b>ip-address</b> <i>ip-address</i> |

This example shows how to add an IP address to an existing policy group:

```
Console> (enable) set policy group grp1 ip-address 100.1.1.1 255.255.255.255
Added IP 100.1.1.1/255.255.255.255 to policy group grp1.
Console> (enable)
```

## Adding a Policy Group to the Policy Template

You can add a policy group to the policy template. If a policy template does not exist, it is created. Similarly, if the policy group name does not exist, it is created.

To add a policy group to the policy template, perform this task in privileged mode:

| Task                                       | Command                                                                  |
|--------------------------------------------|--------------------------------------------------------------------------|
| Add a policy group to the policy template. | <b>set policy name</b> <i>policy-name</i> <b>group</b> <i>group-name</i> |

This example shows how to add a policy group to the policy template:

```
Console> (enable) set policy name poll1 group grp1
Added group grp1 to policy template poll1.
Console> (enable)
```

## Clearing an IP Address from a Policy Group

To clear an IP address from a policy group, perform this task in privileged mode:

| Task                                     | Command                                                                         |
|------------------------------------------|---------------------------------------------------------------------------------|
| Clear an IP address from a policy group. | <b>clear policy group</b> <i>group-name</i> <b>ip-address</b> <i>ip-address</i> |

This example shows how to clear an IP address from a policy group:

```
Console> (enable) clear policy group grp1 ip-address 100.1.1.1
Cleared IP 100.1.1.1 from policy group grp1.
Console> (enable)
```

## Clearing a Policy Group from a Policy Template

To clear a policy group from a policy template, perform this task in privileged mode:

| Task                                         | Command                                                                    |
|----------------------------------------------|----------------------------------------------------------------------------|
| Clear a policy group from a policy template. | <b>clear policy name</b> <i>policy-name</i> <b>group</b> <i>group-name</i> |

This example shows how to clear a policy group from a policy template:

```
Console> (enable) clear policy name poll group grp1
Cleared group grp1 from policy template poll.
Console> (enable)
```

## Displaying Policy Group Information

To display policy group information, perform this task in normal mode:

| Task                              | Command                                                     |
|-----------------------------------|-------------------------------------------------------------|
| Display policy group information. | <b>show policy group</b> { <b>all</b>   <i>group-name</i> } |

This example shows how to display policy group information:

```
Console> (enable) show policy group all
Group Name = grp1
Group Id = 1
No.of IP Addresses = 3
Src Type = ACL CLI
 List of Hosts in group.

 Interface = 0/0
 IPAddress = 100.1.1.1
 Src type = CONFIG

 Interface = 0/0
 IPAddress = 100.1.1.2
 Src type = CONFIG

Group Name = grp2
Group Id = 2
No.of IP Addresses = 0
Src Type = ACL CLI
Console> (enable)
```

## Displaying Policy Templates and Their Associated Policy Groups

To display policy templates and their associated policy groups, perform this task in normal mode:

| Task                                                         | Command                                             |
|--------------------------------------------------------------|-----------------------------------------------------|
| Display policy templates and their associated policy groups. | <b>show policy name</b> {all   <i>policy-name</i> } |

This example shows how to display policy templates and their associated policy groups:

```
Console> (enable) show policy name all
Policy Template poll
Security Policy Groups :grp1 grp2
Console> (enable)
```

## Configuring Inaccessible Authentication Bypass

When a switch cannot reach configured RADIUS servers and hosts cannot be authenticated, you can configure the switch to allow network access to the hosts connected to critical ports. A critical port is enabled by the inaccessible authentication bypass (IAB) feature.

When IAB is enabled, the switch checks the status of the configured RADIUS servers whenever the switch tries to authenticate a host connected to a critical port. If a server is available, the switch can authenticate the host. However, if all the RADIUS servers are unavailable, the switch grants network access to the host and puts the port in the critical-authentication state.

The operation function of the IAB feature depends on the authorization state of the port:

- If the port is unauthorized when a host connected to a critical port tries to authenticate and all servers are unavailable, the switch sends an EAP-success message to the host and puts the port in the critical-authentication state in the configured access VLAN.
- If the port is already authorized and reauthentication occurs, the switch puts the critical port in the critical-authentication state in the current VLAN, which might be the one previously assigned by the RADIUS server.
- If the RADIUS server becomes unavailable during an authentication exchange, the current exchanges times out, and the switch puts the critical port in the critical-authentication state during the next authentication attempt.

When the RADIUS server is available, all the ports in critical state are reinitialized if IAB initialization is enabled. Enable the IAB initialization feature by using the **set radius keepalive init [enable | disable]** command. The IAB initialization feature is disabled by default. If this feature is not enabled, the port waits until the reauthentication timer expires.

If IAB is enabled using the **set radius keepalive [enable | disable]** command, the switch sends periodic requests to the server. The interval between requests is configurable. Use the **set radius keepalivetimer time** command to set the timer. The server state can be in Init, CheckUp, Dead, or Alive state. During the initialization state, the first request is sent to all the RADIUS servers. The request waits for a response. If there is no response, the server state will be moved to Checkup. In the Checkup state, the switch sends two more requests to the server. If there is no response to the requests, the switch will be marked as “dead.” If there is a response to the request, the server will be marked as “alive.” To set the retry timer, use the **set radius timeout time** command to send a second request when there is no response to the first request.

The following sections describe how to configure IAB:

- [Enabling and Disabling Inaccessible Authentication Bypass, page 44-25](#)
- [Setting the AAA Fail Policy, page 44-25](#)
- [Setting the RADIUS Keepalive Timer, page 44-26](#)
- [Setting the RADIUS Auto-Initialize Feature, page 44-26](#)
- [Displaying the Critical Status of Features on a Port, page 44-27](#)
- [Displaying the AAA Fail Policy on a Port, page 44-27](#)
- [Displaying RADIUS Server Information, page 44-27](#)
- [Displaying the MAC Authorization Bypass Settings on a Port, page 44-28](#)
- [Displaying the Web Authorization Settings on a Port, page 44-28](#)
- [Displaying the EOU Settings on a Port, page 44-29](#)
- [Clearing Policy Mapping on a Port, page 44-29](#)

## Enabling and Disabling Inaccessible Authentication Bypass

To enable or disable IAB, perform this task in enable mode:

| Task                  | Command                                                                     |
|-----------------------|-----------------------------------------------------------------------------|
| Enable or disable IAB | <b>set port critical</b> <i>mod/port</i> [ <b>disable</b>   <b>enable</b> ] |

This example shows how to enable IAB:

```
Console> (enable) set port critical 5/1 enable
Port, 5/1 Critical feature enabled.
Console> (enable)
```

This example shows how to enable IAB:

```
Console> (enable) set port critical 5/1 disable
Port, 5/1 Critical feature disabled.
Console> (enable)
```

## Setting the AAA Fail Policy

To set the AAA fail policy, perform this task in enable mode:

| Task                     | Command                                                                       |
|--------------------------|-------------------------------------------------------------------------------|
| Set the AAA fail policy. | <b>set port eou</b> <i>mod/port</i> <b>aaa-fail-policy</b> <i>policy-name</i> |

This example shows how to set AAA fail policy for EOU:

```
Console> (enable) set port eou 12/1 aaa-fail-policy critical-eou-policy
Policy critical-eou-policy mapped as aaa-fail-policy on port 12/1
Console> (enable)
```

To set web-based proxy authentication on a port, perform this task in enable mode:

| Task                                          | Command                                                                                                      |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Set web-based proxy authentication on a port. | <b>set port webauth <i>mod/port</i> [aaa-fail-policy   disable   enable   initialize] <i>policy-name</i></b> |

This example shows how to enable webauth on a port:

```
Console> (enable) set port web-auth 5/1 enable
Port 5/1 Web-auth is enabled.
Console> (enable)
```

This example shows how to set AAA fail policy for webauth:

```
Console> (enable) set port web-auth 12/1 aaa-fail-policy critical-webauth-policy Policy
critical-webauth-policy set as web-auth aaa-fail-policy for port 12/1
Console> (enable)
```

## Setting the RADIUS Keepalive Timer

To enable or disable the RADIUS keepalive timer, perform this task in enable mode:

| Task                            | Command                                        |
|---------------------------------|------------------------------------------------|
| Set the RADIUS keepalive timer. | <b>set radius keepalive [enable   disable]</b> |

This example shows how to enable the RADIUS keepalive timer:

```
Console> (enable) set radius keepalive enable
Radius Keepalive enabled.
```

This example shows how to disable the RADIUS keepalive timer:

```
Console> (enable) set radius keepalive disable
Radius Keepalive disabled.
```

## Setting the RADIUS Auto-Initialize Feature

To enable or disable the RADIUS auto-initialize feature, perform this task in enable mode:

| Task                                    | Command                                            |
|-----------------------------------------|----------------------------------------------------|
| Set the RADIUS auto-initialize feature. | <b>set radius auto-initialize [enable/disable]</b> |

This example shows how to enable the RADIUS auto-initialize feature:

```
Console> (enable) set radius auto-initialize enable
Radius Auto-initialize enabled.
```

This example shows how to disable the RADIUS auto-initialize feature:

```
Console> (enable) set radius auto-initialize disable
Radius Auto-initialize disabled.
```

## Displaying the Critical Status of Features on a Port

To display the critical status of features on a port, perform this task in enable mode:

| Task                                               | Command                                   |
|----------------------------------------------------|-------------------------------------------|
| Display the critical status of features on a port. | <b>show port critical <i>mod/port</i></b> |

This example shows how to display the critical status of features on a port:

```
Console> (enable) show port critical 5/1
Port Critical State Features in Critical State

5/1 enabled dot1x, eou
```

## Displaying the AAA Fail Policy on a Port

To display the AAA fail policy for EOU on a port, perform this task in enable mode:

| Task                                           | Command                                              |
|------------------------------------------------|------------------------------------------------------|
| Display the AAA fail policy for EOU on a port. | <b>show port eou <i>mod/port</i> aaa-fail-policy</b> |

This example shows how to display AAA fail policy on a port:

```
Console> (enable) show port eou 5/1 aaa-fail-policy
Port AAA-Fail-Policy

5/1
```

To display the AAA fail policy for web-auth on a port, perform this task in enable mode:

| Task                                                | Command                                                   |
|-----------------------------------------------------|-----------------------------------------------------------|
| Display the AAA fail policy for web-auth on a port. | <b>show port web-auth <i>mod/port</i> aaa-fail-policy</b> |

This example shows how to display AAA fail policy on a port:

```
Console> (enable) show port web-auth 5/1 aaa-fail-policy
Port AAA-Fail-Policy

5/1
```

## Displaying RADIUS Server Information

To display RADIUS server information, perform this task in enable mode:

| Task                               | Command            |
|------------------------------------|--------------------|
| Display RADIUS server information. | <b>show radius</b> |

This example shows how to display RADIUS server information:

```

Console> (enable) show radius
Active RADIUS Server : 0.0.0.0
RADIUS Deadtime : 0 minutes
RADIUS Key :
RADIUS Retransmit : 2
RADIUS Timeout : 5 seconds
Framed-IP Address Transmit : Disabled
RADIUS Framed MTU : 1000 bytes
RADIUS Keepalive : Enabled
RADIUS Keepalive Timer : 0 minutes
RADIUS Autoinitialize Critical: Disabled

RADIUS-Server Status Auth-port Acct-port Resolved IP Address

```

## Displaying the MAC Authorization Bypass Settings on a Port

To display the MAC authorization bypass settings on a port, perform this task in enable mode:

| Task                                                     | Command                                          |
|----------------------------------------------------------|--------------------------------------------------|
| Display the MAC authorization bypass settings on a port. | <b>show port mac-auth-bypass <i>mod/port</i></b> |

This example shows how to display the MAC authorization bypass settings on a port:

```

Console> (enable) show port mac-auth-bypass 5/1
Port Mac-Auth-Bypass State MAC Address Auth-State Vlan

5/1 Disabled - - 1

Port Termination action Session Timeout Shutdown/Time-Left

5/1 - 3600 NO -

Port PolicyGroups

5/1 -

Port Critical Critical-Status

5/1 Disabled -
Console> (enable)

```

## Displaying the Web Authorization Settings on a Port

To display web authorization settings on a port, perform this task in enable mode:

| Task                                              | Command                                   |
|---------------------------------------------------|-------------------------------------------|
| Display the web authorization settings on a port. | <b>show port web-auth <i>mod/port</i></b> |

This example shows how to display the web authorization settings on a port:

```

Console> (enable) show port web-auth 5/1

```

```

Port IP-Address Vlan Enabled Web-Auth-State Critical-Status

5/1 - 1 enabled - -

Port IP-Address Session-Timeout Session-Timeleft Radius-Rcvd-Timeout

5/1 - - - No

Port IP-Address Policy-Groups

5/1 - -

```

## Displaying the EOU Settings on a Port

To display the EOU settings on a port, perform this task in enable mode:

| Task                                | Command                              |
|-------------------------------------|--------------------------------------|
| Display the EOU settings on a port. | <b>show port eou</b> <i>mod/port</i> |

This example shows how to display the EOU settings on a port:

```

Console> (enable) show port eou 5/1
Port EOU-State IP Address MAC Address Critical-Status

5/1 disabled - - -

Port FSM State Auth Type SQ-Timeout Session Timeout

5/1 - - - -

Port Posture URL Redirect

5/1 - -

Port Termination action Session id

5/1 - -

Port PolicyGroups

5/1 -

Port Critical

5/1 enabled

```

## Clearing Policy Mapping on a Port

To clear the policy mapping on a port, perform this task in enable mode:

| Task                                    | Command                                                      |
|-----------------------------------------|--------------------------------------------------------------|
| Clear the EOU policy mapping on a port. | <b>clear port eou</b> <i>mod/port</i> <b>aaa-fail-policy</b> |

This example shows how to clear the EOU policy mapping on a port:

```

Console> (enable) clear port eou 5/1 aaa-fail-policy

```

```
aaa-fail-policy cleared successfully on port 5/1
```

To clear the web-based proxy authentication mapping on a port, perform this task in enable mode:

| Task                                        | Command                                                   |
|---------------------------------------------|-----------------------------------------------------------|
| Clear the webauth policy mapping on a port. | <b>clear port webauth <i>mod/port</i> aaa-fail-policy</b> |

This example shows how to clear the webauth policy mapping on a port:

```
Console> (enable) clear port webauth 5/1 aaa-fail-policy
aaa-fail-policy cleared successfully on port 5/1
```

## LAN Port IP Configuration Example

Use this configuration example when configuring LAN port IP:

- Port 8/14 connects to the RADIUS server
- Port 8/13 connects to the host with CTA
- Port 8/24 connects to the host without CTA

```
begin
!
***** NON-DEFAULT CONFIGURATION *****
!
!
#time: Fri Mar 4 2005, 17:11:20
!
#version 8.5(0.44)JAC
!
!
#Nac
set eou enable
set eou allow clientless enable
set policy name exception_policy group exception_hosts
set eou authorize ip 77.0.0.90 policy exception_policy
!
#radius
set radius server 10.76.39.93 auth-port 1812 primary
set radius key cisco
!
#vtp
set vtp mode transparent vlan
set vlan 12 name RADIUS_CONNECTIVIY type ethernet mtu 1500 said 100012 state active
set vlan 77 name ALL_HOSTS type ethernet mtu 1500 said 100077 state active
set vlan 1,3
!
#ip
set interface sc0 12 9.6.3.3/255.255.255.0 9.6.3.255
set interface s10 down
set interface sc1 77 77.0.0.2/255.255.255.0 77.0.0.255
set ip route 10.0.0.0/255.0.0.0 9.6.3.1
!
!
#security ACLs
clear security acl all
#NACACL
set security acl ip NACACL permit arp
set security acl ip NACACL permit arp-inspection any any
```

```

set security acl ip NACACL permit dhcp-snooping
set security acl ip NACACL permit udp any eq 21862 host 9.6.3.3 eq 53000
set security acl ip NACACL permit ip group Healthy_hosts any
set security acl ip NACACL deny ip group infected_hosts any
set security acl ip NACACL permit ip group exception_hosts any
set security acl ip NACACL permit ip group clientless_hosts host 10.76.39.100
#
commit security acl all #
map the ACL to VLAN 77
set security acl map NACACL 77
!
#module 8 : 48-port 10/100BaseTX Ethernet
set vlan 12 8/14
set vlan 77 8/13,8/24
set port name 8/13 HOSTS
set port name 8/14 RADIUS
set port name 8/24 HOSTS
set port eou 8/13 enable
set port eou 8/24 bypass
set port dhcp-snooping 8/14 trust enable
!
#module 9 empty
!
#module 15 : 1-port Multilayer Switch Feature Card
!
#module 16 empty
!
#switch port analyzer
set span permit-list disable
set span permit-list include
end
sup2> (enable)

```

The configuration on the MSFC (default router) is as follows:

```

Router# show run
Building configuration...
Current configuration : 509 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
!
ip subnet-zero
!
!
!
ip multicast-routing
ip dhcp-server 10.76.39.93
redundancy
 high-availability
 single-router-mode
!
!
!
interface Vlan12
 ip address 9.6.3.6 255.255.255.0
!
interface Vlan77
 ip address 77.0.0.76 255.255.255.0

```

```

ip helper-address 10.76.39.93
!
ip classless
ip route 10.76.0.0 255.255.0.0 Vlan12
no ip http server
!
!
!
line con 0
line vty 0 4
 login
!
!
end

```

## LAN Port IP Enhancements in Software Release 8.6(1) and Later Releases

These sections describe the enhancements for configuring NAC with LAN port IP in software release 8.6(1) and later releases:

- [Configuring URL Redirect Support for LAN Port IP Exception Hosts, page 44-32](#)
- [Configuring LAN Port IP on Private VLAN Ports, page 44-34](#)

### Configuring URL Redirect Support for LAN Port IP Exception Hosts

Exception hosts (such as printers and IP phones) cannot validate posture. The IP/MAC addresses of the exception hosts are added to an exception list. When a host in the exception list is detected on an interface, a preconfigured policy is installed.

For normal, nonexception hosts, URL redirection is accomplished through information that is received from the RADIUS server after a successful posture validation. Because the RADIUS server is not contacted, exception hosts must find a way to access a server, or you must provide a URL through which the hosts can download software components (such as antivirus updates).

#### Configuration Guidelines and Restrictions

Follow these configuration guidelines and restrictions when configuring URL redirect for LAN port IP exception hosts:

- URL redirection is not supported on multiple-host and multiple-authentication ports.
- URL redirection works only if there is a VACL with ARP inspection and DHCP snooping mapped on the VLAN of the port.
- Because Supervisor Engine 1 does not support ARP inspection, URL redirection is not supported on Supervisor Engine 1.

#### Specifying the Policy Name and URL Redirect String

The **set policy name** *policy-name* **url-redirect** *url-redirect-string* command maps a URL redirect string to a policy name. URL strings of up to 255 characters are allowed. If the URL string exceeds 255 characters, the command fails.

To specify the policy name and URL redirect string, perform this task in privileged mode:

| Task                                             | Command                                                                                  |
|--------------------------------------------------|------------------------------------------------------------------------------------------|
| Specify the policy name and URL redirect string. | <b>set policy name</b> <i>policy-name</i> <b>url-redirect</b> <i>url-redirect-string</i> |

This example shows how to specify the policy name and URL redirect string:

```
Console> (enable) set policy name exception_policy url-redirect http://cisco.com
Url Redirect http://cisco.com mapped to policy name exception_policy
Console> (enable)
```

### Displaying the Policy Name and URL Redirect String Mapping

To display the policy name and URL redirect string mapping, perform this task in normal mode:

| Task                                                     | Command                                                     |
|----------------------------------------------------------|-------------------------------------------------------------|
| Display the policy name and URL redirect string mapping. | <b>show policy name</b> [ <b>all</b>   <i>policy-name</i> ] |

This example shows how to display the policy name and URL redirect string mapping for the specified policy:

```
Console> (enable) show policy name exception_policy
Policy Name : exception_policy

URL-Redirect : http://cisco.com
Console> (enable)
```

This example shows how to display the policy names and URL redirect string mappings for all policies:

```
Console> (enable) show policy name all
Policy Name : TEST

Associated IP Address/Mask Information:
0.0.0.18/255.255.255.224
Policy Name : poll

Associated IP Address/Mask Information:
0.0.0.19/255.255.255.224
Policy Name : BLDG_F

Policy Name : exception_policy

URL-Redirect : http://cisco.com
Console> (enable)
```

### Clearing the URL Redirect String Associated with the Policy Name

To clear the URL redirect string associated with the policy name, perform this task in privileged mode:

| Task                                                           | Command                                                         |
|----------------------------------------------------------------|-----------------------------------------------------------------|
| Clear the URL redirect string associated with the policy name. | <b>clear policy name</b> <i>policy-name</i> <b>url-redirect</b> |

This example shows how to clear the URL redirect string associated with the policy name:

```
Console> (enable) clear policy name exception_policy url-redirect
Cleared url-redirect for the policy exception_policy
Console> (enable)
```

## Configuring LAN Port IP on Private VLAN Ports



### Note

For detailed information on private VLANs, see the [“Configuring Private VLANs on the Switch” section on page 11-19](#).

A private VLAN port is associated with two VLANs, the primary VLAN and the secondary VLAN. Traffic coming from the host (ingress traffic) is tagged with the secondary VLAN and traffic coming from the router port is tagged with the primary VLAN. To trigger EOU on a port, an ARP inspection or DHCP snooping ACL must be mapped to the port VLAN. To trigger EOU on a port in a private VLAN, you must map an ARP inspection or DHCP snooping ACL explicitly to the secondary VLAN as it is the VLAN that is associated with the ingress traffic.

Different PBACLs can be mapped to the primary and secondary VLANs. After a successful posture validation, if the PBACL that is mapped to the primary and secondary VLAN have groups where the host is a member, they are expanded to accommodate the IP address of the host.

## Configuring Network Admission Control with LAN Port 802.1X

These sections describe how to configure NAC with LAN port 802.1X:

- [Understanding How Network Admission Control with LAN Port 802.1X Works, page 44-34](#)
- [LAN Port 802.1X Enhancements in Software Release 8.6\(1\) and Later Releases, page 44-36](#)

## Understanding How Network Admission Control with LAN Port 802.1X Works



### Note

There are no LAN port 802.1X-specific CLI commands. Posture validation and authentication occur seamlessly inside a single EAP tunnel through standard 802.1X authentication. For information on configuring IEEE 802.1X authentication, see [Chapter 40, “Configuring 802.1X Authentication.”](#)



### Note

The restrictions that apply to LAN port IP also apply to LAN port 802.1X. For LAN port IP restrictions, see the [“LAN Port IP Configuration Guidelines and Restrictions” section on page 44-6](#).

LAN port 802.1X combined with standard 802.1X authentication provides a unified authentication and posture validation mechanism at the Layer 2 network edge. LAN port 802.1X acts at the same point in the network as LAN port IP but uses different mechanisms to initiate posture validation, to carry the communication between host and authentication server, and to enforce the resulting access limitations.

Posture validation in LAN port 802.1X is triggered by the standard 802.1X mechanisms (either the supplicant sends an EAPOL-Start message to the NAD, or the NAD probes the supplicant with an EAP-Request/Identity message); the posture information may be sent with the user identity credentials

for validation by the back-end server. The authentication exchange between the supplicant and the NAD is over EAPOL. Policy enforcement is done by assigning the authenticated port to a specified VLAN to provide segmentation and quarantine of poorly postured hosts at Layer 2.

**Note**

LAN port 802.1X restricts non-IPv4 traffic from nonpostured hosts. LAN port 802.1X is preferred for deployments where such a restriction is a requirement.

The LAN port 802.1X policy enforcements include the following (which are already supported with standard 802.1X authentication):

- VLAN assignment—Normal native VLAN assignment (private VLAN assignment is not supported with LAN port 802.1X).
- Security ACL assignment—A PBACL name comes from the RADIUS server, it is assigned to the port interface, and it could be a PACL or VACL.
- Policy groups—PBACL policy groups can be sent down from the ACS server.

For LAN port 802.1X, the policy enforcement uses a VLAN/PBACL combination where LAN port IP uses only PBACLs.

Reauthentication works the same way as in standard 802.1X authentication which makes use of the RADIUS server-sent session timeout and termination action attributes or the local CLI-configured attributes. These attributes are not received as part of the Access-Accept message from the RADIUS server.

With LAN port 802.1X, hosts are classified into one of the following categories:

- Enhanced CTA—This CTA can send both authentication and posture TLVs in a single EAP tunnel and the policy enforcement that comes from the RADIUS server has both the VLAN assignment and the PBACL groups.
- Legacy supplicants and legacy CTA—These hosts do not have the enhanced CTA; they have the standard 802.1X supplicant that cannot connect to CTA and they also have the legacy CTA that can do posture validation using EAPoUDP. With these hosts, after LAN port 802.1X completes, the switch checks for posture validation results. If the posture results are not received, it is assumed that the host does not have enhanced CTA. If LAN port IP is configured on the port, it is triggered to do the posture validation. This category is a combination of LAN port IP and 802.1X authentication.
- Legacy supplicant and no CTA—These 802.1X-capable hosts do not have CTA. After 802.1X authentication completes, the switch realizes that posture validation has not occurred and if LAN port IP is enabled on the port, the switch directs LAN port IP to carry out the posture validation. When LAN port IP runs, it realizes that the host is not responding to its EoU packets and downloads the clientless posture policy for the host. In contrast, 802.1X authentication would have an enforced policy based on the authentication result.
- No supplicant and legacy CTA—When the host does not have an 802.1X-capable supplicant, 802.1X times out and moves the port into the guest VLAN or if MAC authentication bypass is configured, MAC authentication bypass is requested to authenticate the host's MAC address. After authorizing the port (through MAC authentication bypass or the guest VLAN), if LAN port IP is configured, LAN port IP does the posture validation and retrieves the posture policy.
- No supplicant and no CTA—When a dumb host is connected to a switch port that is not 802.1X-capable or does not have a CTA installed, the switch initially tries EAPOL exchanges. When it fails to get a response, the switch moves the port into the guest VLAN state or requests that MAC address bypass (if configured) authenticate the MAC address. Once the port is authorized by one of

these features, the switch requests that the LAN port IP (if configured) does the posture validation. LAN port IP realizes that its Hello messages are not getting any response and does a clientless authentication to retrieve the posture policy for nonresponsive hosts.

## LAN Port 802.1X Enhancements in Software Release 8.6(1) and Later Releases

These sections describe the enhancements for configuring NAC with LAN port 802.1X in software release 8.6(1) and later releases:

- [URL Redirection Support for LAN Port 802.1X, page 44-36](#)
- [Enabling and Disabling the Session Timeout Override for LAN Port 802.1X, page 44-37](#)

### URL Redirection Support for LAN Port 802.1X

After a successful LAN port 802.1X authentication, you can redirect HTTP traffic to the supervisor engine using URL redirection. URL redirection requires that you configure an ACL with an ACE that will redirect all ingress traffic with destination TCP port 80 to the supervisor engine. Enter the **set security acl ip *acl-name* permit url-redirect** command to create the ACE. Any ACL that is mapped to a port/VLAN with this ACE redirects all HTTP traffic to the supervisor engine.

URL redirection requires that the IP address of an authenticated host appears in a URL redirect list. The IP address of the host can be obtained in three ways:

- Framed IP address sent from the RADIUS server
- DHCP snooping
- ARP inspection

DHCP snooping is given the highest precedence, followed by ARP inspection, and then framed IP. If the IP address is received through a higher precedence mechanism than the current one and the previous IP address differs from the current one, the installed policies are removed and updated with the latest IP address. Also, the host IP address added to the URL redirect list is updated with the preferred IP address.

As a result of URL redirection, the NAD intercepts all HTTP traffic from the host that matches the URL redirect match ACL (configured locally or downloaded from the ACS). The intercepted HTTP TCP session is terminated at the NAD. The URL redirect feature then invokes the feature-specific handler that posts an HTTP 302 redirect status code to the host over the terminated TCP session in the following format:

```
HTTP/1.1 302 Page Moved
Location: <REDIRECT URL-ADDRESS>
Pragma: no-cache
Cache-Control: no-cache
```

The redirect URL address is sent from the RADIUS server. When the host browser receives the 302 status code, it initiates a new HTTP request to the provided redirected URL address and the redirection occurs.

The redirect URL that is sent from the RADIUS server needs to be configured on the RADIUS server. A typical URL redirect VSA would be as follows:

```
Url-redirect=<url-address>
```

To prevent all the HTTP packets from being redirected to software by the ACL on the interface, you must ensure that packets destined to the redirected URL are not redirected to the software for URL redirection. The ACL must have an ACE installed so that it occurs before the URL redirection ACE that permits traffic to the redirected host. Installing the ACE in this position ensures that the redirected request will encounter the prepositioned ACE and will not be intercepted by the supervisor engine.

A host can be added to URL redirection through the LAN port IP, web-based proxy authentication, and LAN port 802.1X. Web-based proxy authentication is given the highest precedence, followed by LAN port IP, and then LAN port 802.1X. The host port is opened only after a successful 802.1X authentication. When the host tries to access the web, it has to be authenticated through web-based proxy authentication, followed by posture validation by LAN port IP. The host is permitted to access the URL that is received from the RADIUS server after a successful 802.1X authentication.

For URL redirection to work with LAN port 802.1X, there must be an ACL mapped to the VLAN of the port that has DHCP snooping, ARP inspection, and the URL redirect ACE.

## Enabling and Disabling the Session Timeout Override for LAN Port 802.1X

After a successful 802.1X authentication, and if reauthentication is enabled on a port, 802.1X authentication will reauthenticate the port when the reauthentication timer expires. The reauthentication timer value can be configured through the CLI or can be sent from the RADIUS server. The `set port dot1x mod/port re-authperiod server {disable | enable}` command allows you to specify whether the reauthentication timer value from the RADIUS server will be used or whether the CLI-configured value will be used. By default, the session timeout value that is received from the RADIUS server takes precedence over the CLI-configured timeout value. See [Table 44-1](#) for suggested session timeout override mapping values.

**Table 44-1** Session Timeout Override Mapping Values

| Reauthorization Enabled | Reauthorization Period from Server Enabled | Session Timeout Received | Termination Action   | NAS Action                        |
|-------------------------|--------------------------------------------|--------------------------|----------------------|-----------------------------------|
| No                      | Optional                                   | n/a                      | n/a                  | No reauthorization                |
| Yes                     | No                                         | n/a                      | n/a                  | Reauthorization with local timer  |
| Yes                     | Yes                                        | No                       | n/a                  | No reauthorization                |
| Yes                     | Yes                                        | Yes                      | Default or no action | Termination with RADIUS timer     |
| Yes                     | Yes                                        | Yes                      | RADIUS request       | Reauthorization with RADIUS timer |



### Note

If you enable 802.1X IAB on a port that is already authenticated, if the RADIUS server is not reachable during reauthentication, then the port remains in the authenticated state.

To enable or disable the session timeout override for LAN port 802.1X, perform this task in privileged mode:

| Task                                                                | Command                                                                |
|---------------------------------------------------------------------|------------------------------------------------------------------------|
| Enable or disable the session timeout override for LAN port 802.1X. | <b>set port dot1x mod/port re-authperiod server {disable   enable}</b> |

This example shows how to enable the session timeout override for LAN port 802.1X:

```
Console> (enable) set port dot1x 5/8 re-authperiod server enable
Port 5/8 session-timeout-override option is enabled
Console> (enable)
```

This example shows how to display the session timeout override setting for LAN port 802.1X:

```
Console> (enable) show port dot1x 5/8
Port Auth-State BEnd-State Port-Control Port-Status

 5/8 - - force-authorized -

Port Port-Mode Re-authentication Shutdown-timeout Control-Mode

 5/8 SingleAuth disabled disabled admin oper

Port Posture-Token Critical-Status Termination action Session-timeout

 5/8 - - - -

Port Session-Timeout-Override Url-Redirect

 5/8 enabled -

Port Critical

 5/8 disabled
Console> (enable)
```