Network Admission Control Software Configuration Guide

This document describes how to configure Network Admission Control (NAC) on Catalyst series switches. NAC is part of the Cisco Self-Defending Network Initiative, which helps you identify, prevent, and adapt to security threats in your network. Because of the increased threat and impact of worms and viruses on networked businesses, NAC assesses the antivirus condition of endpoints or clients before granting network access.

Contents

This document contains the following sections:

Prerequisites for Configuring NAC

NAC support comprises two features: NAC Layer 2 IEEE 802.1X authentication and validation, and NAC Layer 2 IP validation. As shown in Table 1, support for these features is chassis-specific.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table 1 NAC Support Matrix

NAC Features	7600	6500	4500	3750 Metro	3750	3560	3550 (12.2S)	3550 (12.1S)	2970	2960	2955	2950 -LRE	2950	2940	Cisco Aironet
NAC Layer 2 IEEE 802.1X Authentication and Validation	X	X	X	—	X	X	X	X	X	X	X	—	X	X	X
NAC Layer 2 IP Validation	X	X	X	—	X	X	X	—	—	—	—	—	—	—	—

Note NAC is also implemented on Cisco IOS routers running Cisco IOS Release 12.3(8)T. The NAC implementation on all switches is not backward-compatible with the NAC implementation on the routers. The switches support default access control lists (ACLs) and downloadable ACLs from the Cisco Secure Access Control Server (ACS) but do not support intercept ACLs.

Note The Catalyst 6500 series switch running Cisco IOS Release 12.2(18)SXF does not support NAC Layer 2 IEEE 802.1X authentication and validation on edge switches.

Both NAC Layer 2 validation methods (IEEE 802.1X and IP) work on edge switches but have different validation initiation, message exchange, and policy enforcement methods. For a complete list of devices that support NAC, see the NAC release notes.

Note For complete syntax and usage information for the new or modified commands used in this document, see the "Command Reference" section on page 38, or the *Cisco IOS Security Command Reference, Release 12.3* at this location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/secur_r.

Note For the NAC 2.0 release notes, see this location:

http://www.cisco.com/en/US/netsol/ns617/networking_solutions_release_notes_list.html

Information About Network Admission Control

Virus infections cause serious network security breaches. Sources of virus infections are insecure endpoints, such as PCs and servers. The most likely security risk is from a device on which antivirus software is not installed or is disabled. If you enable the software, the devices might not have the latest virus definitions and scan engines. Although antivirus vendors are making it more difficult to disable antivirus software, the risk of outdated virus definitions and scan engines still exists.

NAC authenticates endpoint devices or clients and enforces access control policies to prevent infected devices from adversely affecting the network. It checks the antivirus condition or *posture* of endpoint systems or clients before granting the devices network access. NAC keeps insecure nodes from infecting the network by denying access to noncompliant devices, placing them in a quarantined network segment or giving them restricted access to computing resources.

These sections describe NAC:

NAC Device Roles

With NAC, the devices in the network have specific roles, as shown in Figure 1 and described below.

- *Endpoint Device/Client/Host*—This is a host that requests access to the protected LAN network and is the one whose posture is validated against the company corporate IT-Security policy. This host can be a desktop PC, server, laptop, or any other non-IOS device (printers or scanners). The endpoint device is configured with the Cisco Trust Agent (CTA), which is the interface between the authenticating server and the third party software on the endpoint device. Endpoint devices that are configured with CTA are called *CTA hosts*. Other endpoint devices like the Cisco IP Phone, non-IOS devices or PC/laptops, which are not configured with CTA, are referred to as *Non-Responsive Hosts* (NRHs). The authenticating server should provision policies for both the CTA Hosts as well as the NRHs. The CTA has the posture agent software that acts as an interface and also has the Posture Plugin DLL, which contains the actual information about the state of posture on the client.

Note Cisco Aironet access points running Cisco IOS Release 12.3(4)JA or later support NAC Layer 2 IEEE 802.1X authentication and validation by default; no configuration is required on the access points. The access points simply relay NAC communication between clients and switches.

The CTA software is also referred to as the *posture agent* or the *antivirus client*.

- *Network access device* (NAD)—This is the device on which NAC is implemented. It can be a Layer 2 or Layer 3 device at the network edge to which endpoint devices connect. The NAD initiates the posture validation process and then bridges the endpoint device and the authenticating server. The NAD initiates posture validation by relaying the Extensible Authentication Protocol (EAP) messages over the User Datagram Protocol (UDP). NAC uses this protocol referred to as EAP over User Datagram Protocol (EAPoUDP). (EAPoUDP is also termed *EoU*.)
  - For access points as well as Catalyst 2970, 2960, 2955, 2950, and 2940 series switches, the encapsulation information in the EAP messages is based on IEEE 802.1X port-based authentication. When using IEEE 802.1X for authentication, the switch uses EAP over LAN (EAPOL) frames.
  - For switches other than Catalyst 2970, 2960, 2955, 2950, and 2940 series switches, the encapsulation information in the EAP messages can be based on IEEE 802.1X port-based authentication or UDP. When using IEEE 802.1X for authentication, the switch uses EAPOL frames. When using UDP, the switch employs EoU frames.

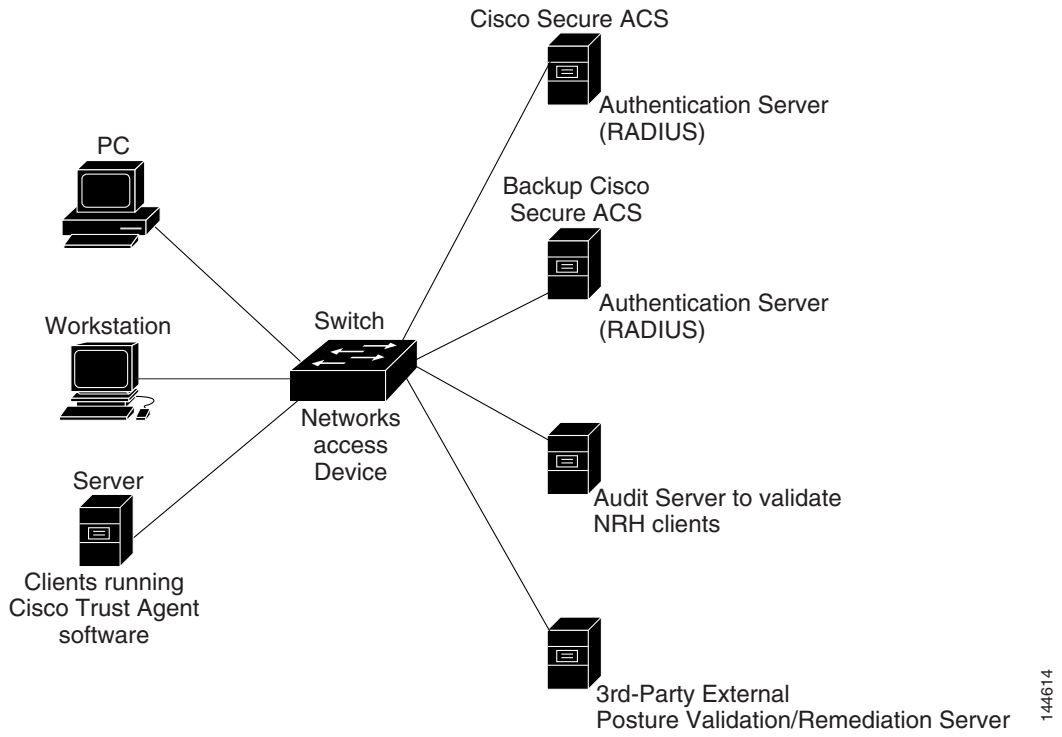
Note The devices that can act as intermediaries include the Catalyst 6500, 4500, 3750, 3560, 3550, 2960, 2970, 2955, 2950, and 2940 switches, the Catalyst 7600 series router, and the Cisco Gigabit Ethernet Switching Module (CGESM) switches. These devices must be running software that supports the RADIUS client and IEEE 802.1X.

- Authentication server (AS)—This is an instance of a Posture Validation Server (PVS) that first validates the posture credentials of an endpoint device, then downloads a Network Access Profile (NAP) for the respective endpoint device to the NAD. The NAP contains the access policies that must be applied for the endpoint device's session. This NAP is formed after the AS evaluates the endpoint device's posture credential state against the company's corporate IT-Security policies. After the NAD has initiated the EoU session between the endpoint device and the AS, it becomes transparent and only acts as a bridge between the two.

  AS can also function as a third party remediation or audit server for validating the client of the NRH.

Note Cisco Secure ACS 4.0 or later is an instance of RADIUS/TACACS (AS) for NAC. In NAC 2.0, the Catalyst switch supports Cisco Secure ACS 4.0 or later with RADIUS, authentication, authorization, and accounting (AAA), and EAP extensions.

Figure 1 NAC Device Roles



Posture Validation

NAC enables NADs to permit or deny network hosts access to the network based on the state of the software on the host. This process is called *posture validation*.

Posture validation consists of checking the antivirus condition or credentials of the client, evaluating the security posture credentials from the network client, and providing the appropriate network access policy to the NAD based on the system posture.

The Catalyst switch performs posture validation on switch ports as follows (Figure 1):

1. When an endpoint or client tries to connect to the network through a Cisco NAD, such as an edge switch, the switch challenges the endpoint's antivirus condition. The antivirus condition includes virus definitions and the version of the antivirus software and the scan engine.
2. The endpoint system, running the CTA software, collects antivirus information from the endpoint device (such as the type of antivirus software it uses), and sends the information to the switch.

   If an endpoint is not running the CTA software, the switch classifies the endpoint system as clientless and considers the endpoint system to be a *nonresponsive host* or a *NAC agentless host*.

   For more information about nonresponsive hosts, see the "Nonresponsive Hosts" section on page 7. For more information about clientless endpoint systems and nonresponsive hosts, see the "Posture Validation and Layer 2 IP Validation" section on page 10.

   For the *CTA Administrator Guide 2.0*, see this URL:

   http://www.cisco.com/en/US/products/ps5923/prod_maintenance_guides_list.html

   For the *Cisco Trust Agent 2.0 Release Notes*, see this URL:

   http://www.cisco.com/en/US/products/ps5923/prod_release_notes_list.html

   For the general listing of CTA documentation on the web, see this URL:

   http://www.cisco.com/en/US/products/ps5923/tsd_products_support_series_home.html
3. The switch sends the information to the Cisco Secure ACS to determine the NAC policy.

   The Cisco Secure ACS validates the antivirus condition of the endpoint, determines the NAC policy, and returns the access policy to the switch. The switch enforces the access policy against the endpoints.

   If the validation succeeds, the Cisco Secure ACS grants the client network access based on the access limitations.

   If the validation fails, the noncompliant device can be denied access, placed in a quarantined network segment, or given restricted access to computing resources. The validation might fail because either the client is infected with a worm or virus, the host is not running compliant software or the host is using an obsolete version of antivirus software.

   For information on Cisco Secure ACS for Windows, see this URL:

   http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html

   For information on the Cisco Secure ACS solution engine, see this URL:

   http://www.cisco.com/en/US/products/sw/secursw/ps5338/index.html

AAA Down Policy

Typical deployments of NAC use Cisco Secure ACS to validate the client posture and to pass policies back to the NAD. If the AAA server is not reachable when the posture validation occurs, instead of rejecting the user (that is, not providing the access to the network), an administrator can configure a default AAA down policy that can be applied to the host.

This system is advantageous for the following reasons:

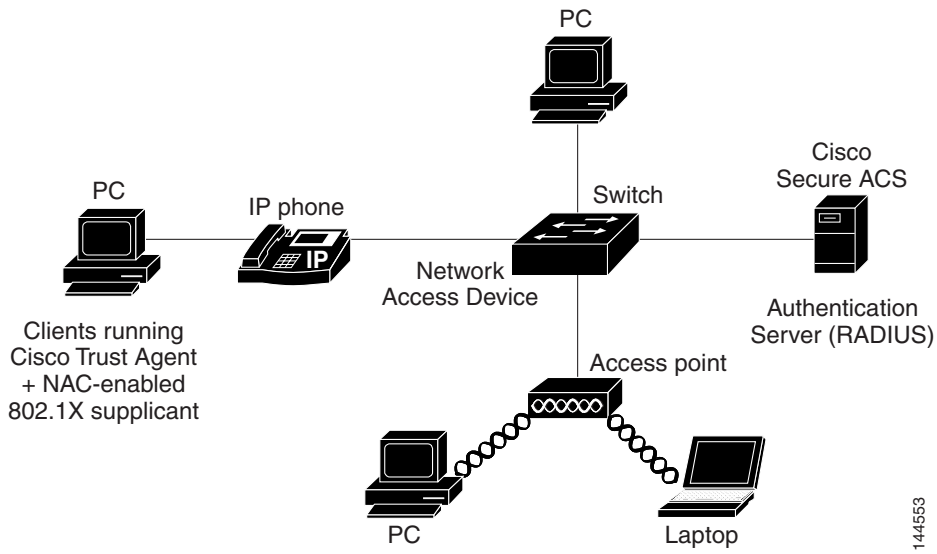
- While AAA is unavailable, the host will still have connectivity to the network, although it may be restricted.
- When the AAA server is once again reachable, users can be revalidated, and their policies can be downloaded from the ACS.

Note When the AAA server is down, the AAA down policy is applied only if there is no existing policy associated with the host. Typically, during revalidation when the AAA server goes down, the policies being used for the host are retained.

NAC Layer 2 IEEE 802.1X Authentication and Validation

You can use NAC Layer 2 IEEE 802.1X on the access port of an edge switch to which a device (an endpoint system or client) is connected. The device can be a PC, a workstation, a Cisco Aironet access point, or a server that is connected to the switch access port through a direct connection.

Figure 2 Network Using NAC Layer 2 IEEE 802.1X



Either the client or the switch can initiate posture validation. The switch relays EAPOL messages between the endpoints and the Cisco Secure ACS. After the Cisco Secure ACS returns the access control decision, the switch enforces the access limitations either by assigning an authenticated port to a specific VLAN, which provides segmentation and quarantine of poorly postured clients or by denying network access.

This section includes the following topics:

Nonresponsive Hosts

A nonresponsive host can either be a device running a legacy IEEE 802.1X-compliant supplicant without NAC support or a device without an IEEE 802.1X compliant supplicant. A host or client that does not respond to posture validation requests can be validated in one of these ways:

- 802.1X Guest VLAN (for devices that lack an IEEE 802.1X compliant supplicant)
- 802.1X identity + unknown posture

If a host with legacy IEEE 802.1X-compliant client software connects to the switch, the switch initiates a session with the Cisco Secure ACS and forwards the host information to the authentication server. The authentication server returns an access policy based on the host's known identity and unknown posture. The policy can be a VLAN assignment or a denial of network access. The switch applies this policy to the host.

The authentication server also sends the switch information that the *posture* Attribute-Value (AV) pair is set to *Unknown* because the host did not provide posture information. This information does not affect how the switch applies the access policy to the host.

Periodic Posture Revalidation

Posture changes can occur because of a change to the client or to the Cisco Secure ACS.

- If the host changes, the CTA on the host detects the change and initiates the revalidation by sending an EAPOL-Start message to the switch. For example, this may happen due to an operating system patch or an updated antivirus software package.
- If the authentication server changes, the switch does not revalidate the posture until the periodic re-authentication timer expires. For example, this may happen when a new antivirus.dat file is available.

You can configure the switch to periodically revalidate the posture of a responsive host by enabling periodic IEEE 802.1X client re-authentication and specifying its frequency. For devices running a legacy supplicant without CTA, nonresponsive hosts *can* be configured for periodic posture revalidation.

Note For devices that are not running a IEEE 802.1X compliant supplicant, nonresponsive hosts *cannot* be configured for periodic posture revalidation.

With NAC Layer 2 IEEE 802.1X, you can specify the number of seconds between re-authentication attempts by manually setting the number of seconds or by configuring the switch to use the value of the Session-Timeout RADIUS attribute in the Access-Accept message from the Cisco Secure ACS.

The switch also uses the Termination-Action RADIUS attribute for posture validation. Depending on the value of this attribute, the switch either automatically revalidates the client or ends the EAPOL-based session, then revalidates the client.

Switch Actions

Depending on the periodic re-authentication state, the re-authentication value, and the Session-Timeout RADIUS attribute, the switch takes one of the actions listed in Table 2.

- If you manually set the number of seconds, the switch re-authenticates the host when the timer expires.
- If the Access-Accept message does not include the Session-Timeout AV pair, the switch does not re-authenticate the host.
- If the Access-Accept message includes the Session-Timeout AV pair, the switch uses the re-authentication time from the Cisco Secure ACS.

Note The Access-Accept message is also referred to as an *Accept frame*.

- The switch re-authenticates the host depending on the value of the Termination-Action attribute in the RADIUS attribute:
  - If the Termination-Action AV pair is present and its value is *RADIUS-Request*, the switch authenticates the host.
  - If the Termination-Action AV pair is not present or its value is *Default*, the switch ends the session with the Cisco Secure ACS, and the host is unauthorized.

Table 2 Periodic Re-Authentication Results

Periodic Re-Authentication	Re-Authentication Time	Session-Timeout Attribute	Termination-Action Value	Switch Action
Disabled	—	—	—	No re-authentication occurs.
Enabled	Manually configured as the number of seconds	—	—	The switch re-authenticates and uses the manually specified number of seconds.
Enabled	Automatically configured to use the re-authentication time from the Cisco Secure ACS	Not included in the Access-Accept message	—	No re-authentication occurs.
Enabled	Automatically configured to use the re-authentication time from the Cisco Secure ACS	Included in the Access-Accept message	*Default* or no value	The session is terminated after the re-authentication time from the server expires.
Enabled	Automatically configured to use the re-authentication time from the Cisco Secure ACS	Included in the Access-Accept message	*RADIUS-Request*	The switch re-authenticates and uses the re-authentication time from the server.

AAA Down Policy for NAC Layer 2 IEEE 802.1X (Inaccessible Authentication Bypass)

Note This feature is available only on the Catalyst 3560 and Catalyst 3750 series switches.

To make use of Inaccessible Authentication Bypass, a port must be designated as a critical port. The process of handling critical ports is as follows:

1. A new IEEE 802.1X authentication session is detected.
2. Before authentication is triggered, and provided the AAA server is unreachable, the critical authentication policy is applied and port is transitioned to the Critical-Auth state. The *policy* that is applied is in the form of a VLAN assignment.
3. When the AAA server is once again available, a reauthentication will be re-triggered for the host.

Note When the AAA server is down, the AAA down policy is applied only if there is no existing policy associated with the host. Therefore, if the port was previously assigned to a VLAN due to a successful authentication, it will remain in that VLAN. However, if the port was unauthorized prior to moving to the Critical-Auth state, it will be assigned to the configured access VLAN.

For information on configuring the Inaccessible Authentication Bypass feature on the Catalyst 3750 and 3560 series switches, refer to the following locations:

http://www.cisco.com/en/US/products/hw/switches/ps5023/products_configuration_guide_chapter09186a00805555e8.html

http://www.cisco.com/en/US/products/hw/switches/ps5023/products_command_reference_book09186a00804fdc8c.html

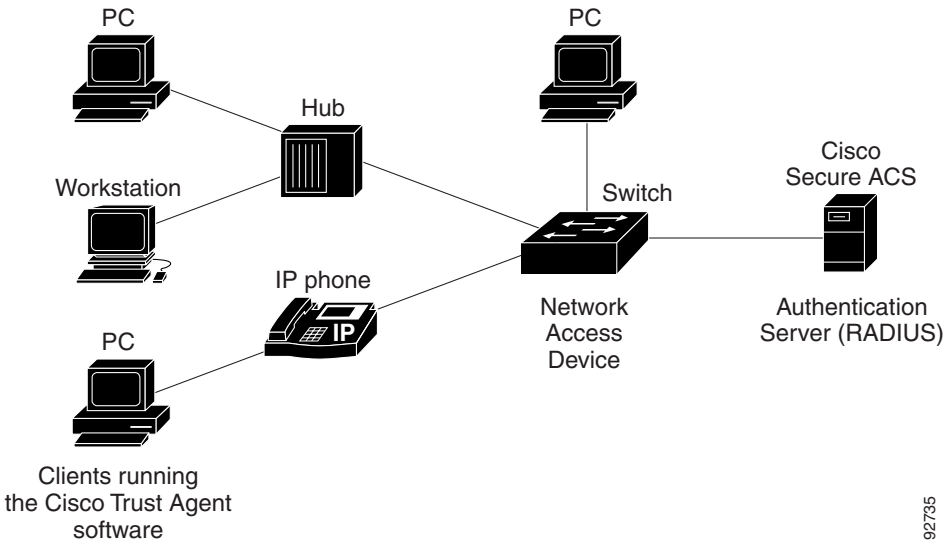
NAC Layer 2 IP Validation

You can use NAC Layer 2 IP on an access port of an edge switch to which a device (an endpoint system or client) is connected. The device can be a PC, a workstation, or a server that is connected to the switch access port through a direct connection, an IP phone, a hub, or a wireless access point, as shown in Figure 3.

Note Cisco Aironet access points *do not support* NAC Layer 2 IP validation.

When you enable NAC Layer 2 IP, EAPoUDP works only with IPv4 traffic. The switch checks the antivirus condition of the endpoint devices or clients and enforces access control policies.

Figure 3 Network Using NAC Layer 2 IP



This section discusses the following topics:

Posture Validation and Layer 2 IP Validation

NAC Layer 2 IP supports the posture validation of multiple hosts on the same switch port, as shown in Figure 3.

When you enable NAC Layer 2 IP validation on a switch port to which hosts are connected, the switch can use either DHCP snooping or Address Resolution Protocol (ARP) snooping to identify connected hosts. Posture validation initiated through DHCP snooping takes precedence over posture validation initiated through ARP snooping. The switch initiates posture validation after either receiving an ARP packet or creating a DHCP snooping binding entry.

Note ARP snooping is the default method to detect connected hosts. If you want the switch to detect hosts when a DHCP snooping binding entry exists, you must enable DHCP snooping.

If dynamic ARP inspection alone is enabled on an access VLAN that is assigned to a switch port, posture validation is initiated when ARP packets pass the dynamic ARP inspection validation checks. If DHCP snooping *and* dynamic ARP inspection are enabled, however, creating a DHCP snooping binding entry will initiate posture validation.

A malicious host could send spoofed ARP packets and try to bypass posture validation. To prevent unvalidated hosts from accessing the network, you can enable the IP Source Guard feature on the switch port.

Note The Catalyst 7600 series router and the Catalyst 6500 series switch *do not* support IP Source Guard.

When posture validation initiates, a switch creates an entry in the EAPoUDP session table to track the posture validation status of the host and observes the following decision tree to determine the NAC policy:

1. If the host is in the exception list (see the "Exception Lists" section on page 11), the switch applies the user-configured NAC policy to the host.
2. If EoU bypass is enabled (see the "EoU Bypass" section on page 11), the switch sends a nonresponsive-host request to the Cisco Secure ACS and applies the access policy from the server to the host. The switch inserts a RADIUS AV pair to the request to specify that the request is for a nonresponsive host.
3. If EoU bypass is disabled, the switch sends an EAPoUDP hello packet to the host, requesting the host antivirus condition (see the "EAPoUDP Sessions" section on page 11). If no response is received from the host after the specified number of attempts, the switch classifies the host as clientless, and the host is considered a nonresponsive host. The switch sends a nonresponsive-host request to the Cisco Secure ACS and applies the access policy from the server to the host.

Exception Lists

An exception list has local profile and policy configurations. Use the identity profile to statically authorize or validate devices based on the IP address, MAC address, or device type. An identity profile is associated with a local policy that specifies the access control attributes.

You can bypass posture validation of specific hosts by specifying those hosts in an exception list and applying a user-configured policy to the hosts. After the entry is added to the EAPoUDP session table, the switch compares the host information to the exception list. If the host is in the exception list, the switch applies the configured NAC policy to the host. The switch also updates the EAPoUDP session table with the validation status of the client as *POSTURE ESTAB*.

EoU Bypass

The switch can use the EoU bypass feature to speed up posture validation of hosts that are not using the CTA. If EoU bypass is enabled, the switch does not contact the host to request the antivirus condition. Instead, the switch sends a request to the Cisco Secure ACS that includes the IP address, MAC address, service type, and EAPoUDP session ID of the host. The Cisco Secure ACS makes the access control decision and sends the policy to the switch.

If EoU bypass is enabled and the host is nonresponsive, the switch sends a nonresponsive-host request to the Cisco Secure ACS and applies the access policy from the server to the host.

If EoU bypass is enabled and the host uses CTA, the switch also sends a nonresponsive-host request to the Cisco Secure ACS and applies the access policy from the server to the host.

EAPoUDP Sessions

EoU is enabled by default. If the EoU bypass is disabled, the switch sends an EAPoUDP packet to initiate posture validation. While posture validation occurs, the switch enforces the default access policy. After the switch sends an EAPoUDP message to the host and the host responds to the antivirus condition

request, the switch forwards the EAPoUDP response to the Cisco Secure ACS. If no response is received from the host after the specified number of attempts, the switch classifies the host as nonresponsive. After the ACS validates the credentials, the authentication server returns an Access-Accept message with the posture token and the policy attributes to the switch. The switch updates the EAPoUDP session table and enforces the access limitations, which provides segmentation and quarantine of poorly postured clients, or by denying network access.

Because of posture validation, two types of policies are applicable on ports:

- Host policy: The host policy consists of an ACL that enforces the access limitations as determined by the outcome of posture validation.
- URL redirect policy: The URL redirect policy provides a mechanism to redirect all HTTP/HTTPS traffic to a remediation server that allows a non-compliant host to perform the necessary upgrade actions to become compliant. The policy consists of:
  - A URL that points to the remediation server.
  - An ACL on the switch that causes all HTTP/HTTPS packets from the host other than those destined to the remediation server address to be captured and redirected to the switch software for the necessary HTTP redirection.

The ACL name for the host policy, the redirect URL, and the URL redirect ACL are conveyed using RADIUS Attribute-Value objects.

Note If a client's DHCP snooping binding entry is deleted, the switch removes the client entry in the EAPoUDP session table, and the client is no longer authenticated.

Cisco Secure ACS and Attribute-Value Pairs

When you enable NAC Layer 2 IP validation, the Cisco Secure ACS provides NAC authentication, authorization, and accounting (AAA) services by using RADIUS. Cisco Secure ACS gets information about the antivirus credentials of the endpoint system and validates the antivirus condition of the endpoint.

You can set these AV pairs on the Cisco Secure ACS by using the RADIUS *cisco-av-pair* vendor-specific attributes (VSAs):

- CiscoSecure-Defined-ACL—Specifies the names of the downloadable ACLs on the Cisco Secure ACS. The switch gets the ACL name through the CiscoSecure-Defined-ACL AV pair in this format:

  #ACL#-IP-*name-number*

  where *name* is the ACL name and *number* is the version number, such as 3f783768.

  The Auth-Proxy posture code checks whether the access control entries (ACEs) of the specified downloadable ACL were previously downloaded. If they were not, the Auth-Proxy posture code sends an AAA request with the downloadable ACL name as the username so that the ACEs are downloaded. The downloadable ACL is then created as a named ACL on the switch. This ACL has ACEs with a source address of **any** and does not have an implicit deny statement at the end. When the downloadable ACL is applied to an interface after posture validation completes, the source address is changed from **any** to the host source IP address. The ACEs are prepended to the default ACL applied to the switch interface to which the endpoint device is connected. If traffic matches the CiscoSecure-Defined-ACL ACEs, the appropriate NAC actions are taken.

  Following is an example of an interface ACL:

```
access-list 115 permit udp any any eq bootps (for bootps requests)
access-list 115 permit ip any 20.0.0.0 0.0.0.255 (NAC Ingress source N/W)
```

```
access-list 115 permit ip any host 40.0.0.5 (Audit Server)
```

- url-redirect and url-redirect-acl—Specifies the local URL policy on the switch. The switches uses the following cisco-av-pair VSAs:
  - url-redirect = <HTTP or HTTPS URL>
  - url-redirect-acl = switch ACL name or number

  These AV pairs enable the switch to intercept an HTTP and/or HTTPS request from the endpoint device and forward the client web browser to the specified redirect address from which the latest antivirus files can be downloaded. The url-redirect AV pair on the Cisco Secure ACS contains the URL to which the web browser will be redirected.

Note The url-redirect can be done for either HTTP or HTTPS but not both at the same time.

The url-redirect-acl AV pair contains the name or number of an ACL that specifies the HTTP and/or HTTPS traffic to be redirected. The ACL must be defined on the switch. Traffic that matches a permit entry in the redirect ACL is redirected. These AV pairs might be sent if the host's posture is unhealthy.

Following is an example of a *url-re-direct-acl*:

```
ip access-list extended url-redirect-acl
permit tcp any <protected-server-vlan-network>
```

For more information about AV pairs that are supported by Cisco IOS software, see the documentation about the software releases running on the AAA clients.

For information on ACS for the Windows Server, see this URL:
http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html

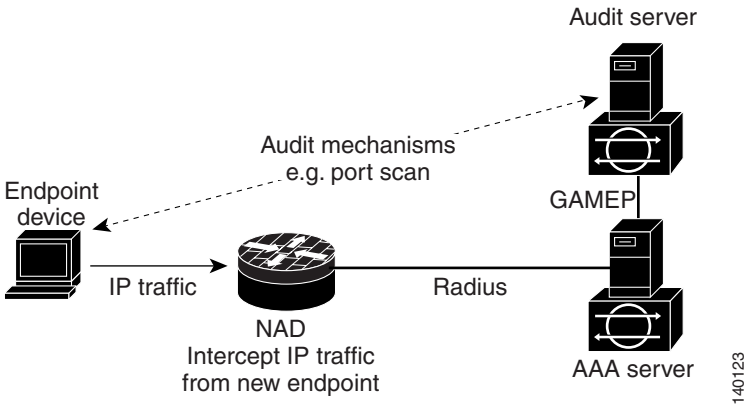
For information on the ACS Solution Engine, see this URL:
http://www.cisco.com/en/US/products/sw/secursw/ps5338/index.html

Audit Servers

End devices that do not run CTA will not be able to provide credentials when challenged by NADs. Such hosts are termed *Agentless* or *Non-Responsive*.

Figure 4 shows how audit servers fit into the typical topology.

Figure 4 NAC Device Roles



To enable you to perform more exhaustive examination of Agentless hosts, the NAC architecture has been extended to incorporate Audit Servers, which can probe and scan these hosts for security compliance, vulnerability and threats without the need for a CTA on the host. The result of the audit can influence Access Servers to make host specific network access policy decisions rather than to enforce a common restrictive policy for all non-responsive hosts. This enables you to build more robust host audit/examination functionality by integrating any 3rd party audit mechanisms into the NAC architecture.

NAC architecture assumes that the Audit Server is reachable so that the host can communicate with it. When a host accesses the network through a NAD configured for posture validation, the NAD requests the AAA server (Cisco Secure ACS) for an access policy to be enforced for the host. You can configure the AAA Server to trigger a scan of the host with an external Audit Sever. The audit scan happens asynchronously and can take several seconds to complete. During this time, the AAA Server would convey a minimal restrictive security policy to the NAD for enforcement along with a short poll timer (Session-Timeout). The NAD would poll the AAA sever at the specified timer interval until the result is available from the Audit Server. Once the AAA server receives the audit, it would compute an access policy based on the audit, which is sent down to the NAD for enforcement on its next request.

Default ACLs

Note The default ACL *must* permit EAPoUDP traffic for NAC Layer 2 IP validation to function.

If NAC Layer 2 IP validation is configured on a switch port, a default port ACL must also be configured on a switch port and will be applied to IP traffic.

If the default ACL is configured on the switch and the Cisco Secure ACS sends a host access policy to the switch, the switch applies the policy to traffic from the host connected to a switch port. After the Cisco Secure ACS downloads a per host policy, the incoming traffic is matched against that policy and if there is no match in that policy, the traffic will be matched against the default policy.

If the Cisco Secure ACS sends the switch a downloadable ACL that specifies a redirect URL as a policy-map action, this ACL takes precedence over the default ACL already configured on the switch port. The downloadable ACL *always takes precedence* over the default ACL. If the default port ACL is not configured on the switch, the downloadable ACLs are not programmed.

NAC Timers

The switch supports these timers:

Hold Timer

The hold timer prevents a new EAPoUDP session from immediately starting after the previous attempt to validate the session fails. This timer is used only when the Cisco Secure ACS sends an Accept-Reject message to the switch.

The default value for the hold timer is 180 seconds (3 minutes).

An EAPoUDP session might not be validated because either the posture validation of the host fails, a session timer expires, or the switch or Cisco Secure ACS receives invalid messages. If the switch or authentication server continuously receives invalid messages, a malicious user might be attempting a denial-of-service attack.

Idle Timer

The idle timer controls how long the switch waits either for an ARP packet from the postured host or for a refreshed entry in the IP device tracking table to verify that the host is still connected. The idle timer works with a list of known hosts to track those that have initiated posture validation and the IP device tracking table.

The idle timer is reset when a switch receives an ARP packet or when an entry in the IP device tracking table is refreshed. If the idle timer expires, the switch ends the EAPoUDP session on the host, and the host is no longer validated.

Note IP Device Tracking table is used to track new hosts as they appear on the network. The IP Device Tracking table detects hosts through IP ARP Inspection and IP DHCP Snooping (optional). IP ARP Inspection is enabled automatically when IP Device Tracking is enabled.

The default probe interval is 30 seconds. The timeout is actually probe interval times the number of probe entries. So, by default value of the idle timer is 90 seconds, because the probe interval is 30 seconds and the probe retries are 3.

The switch maintains a list of known hosts to track hosts that have initiated posture validation. When the switch receives an ARP packet, it resets the aging timers for the list and the idle timer. If the aging time of the list expires, the switch sends an ARP probe to verify that the host is present. If the host is present, it sends a response to the switch. The switch updates the entry in the list of known hosts. It then resets the aging timers for the list and the idle timer. If switch receives no response, the switch ends the session with the Cisco Secure ACS, and the host is no longer validated.

The switch also uses the IP device tracking table to detect and manage hosts connected to the switch. The switch uses ARP or DHCP snooping to detect of hosts. By default, the IP device tracking feature is disabled on a switch. When IP device tracking is enabled, and a host is detected, the switch adds an entry to the IP device tracking table that includes this information:

- IP and MAC address of the host
- Interface on which the switch detected the host
- Host state that is set to ACTIVE when the host is detected

If NAC Layer 2 IP validation is enabled on an interface, adding an entry to the IP device tracking table initiates posture validation.

For the IP device tracking table, you can configure the number of times that the switch sends ARP probes for an entry before removing an entry from table and the number of seconds that the switch waits before resending the ARP probe. If the switch uses the default settings of the IP device tracking table, the switch sends ARP probes every 30 seconds for all the entries. When the host responds to the probe, the host state is refreshed and remains *ACTIVE*. The switch can send up to three additional ARP probes at 30 second intervals if the switch does not get a response. After the maximum number of ARP probes are sent, the switch removes the host entry from the table. The switch ends the EAPoUDP session for the host if a session was set up.

Using the IP device tracking ensures that hosts are detected in a timely manner, despite the limitations of using DHCP. If a link goes down, the IP device tracking entries associated with the interface are not removed, and the state of entries is changed to *INACTIVE*. The switch does not limit the number of entries in the IP device tracking table but applies a limit to remove INACTIVE entries. All entries remain in the IP device tracking table until it reaches the limit. When the table reaches the limit, the switch removes the INACTIVE ones if the table has INACTIVE entries, and the switch adds new entries. If the table does not have INACTIVE entries, the number of entries in the IP device tracking table continues to increase. When a host becomes *INACTIVE*, the switch ends the host session.

- For Catalyst 3750, 3560, 3550, 2970, 2960, 2955, 2950, and 2940 switches and for Cisco EtherSwitch service modules, the limit to remove INACTIVE entries is 512.
- For Catalyst 4500 and 6500 series switches, and the Catalyst 7600 series router, the limit is 2048.

After an interface link is restored, the switch sends ARP probes for each entry associated with the interface. The switch ages out entries for hosts that do not respond to ARP probes. The switch also changes the state of hosts that respond to ACTIVE and initiates posture validation.

Retransmission Timer

The retransmission timer controls the amount of time that the switch waits for a response from the client before resending a request during posture validation. Setting the timer value too low might cause unnecessary transmissions, and setting the timer value too high might cause poor response times.

The default value of the retransmission timer is 3 seconds.

Revalidation Timer

The revalidation timer controls the amount of time a NAC policy is applicable to a client that used EAPoUDP messages during posture validation. The timer starts after the initial posture validation completes. The timer resets when the host is revalidated. The default value of the revalidation timer is 36000 seconds (10 hours).

You can specify the revalidation timer value on the switch and on an interface on that switch with the **eou timeout revalidation** global configuration command.

Note The revalidation timer can be configured locally on the switch or it can be downloaded from the Cisco Server ACS.

The revalidation timer behavior is based on Session-Timeout RADIUS attribute and the Termination-Action RADIUS attribute in the Access-Accept message from the Cisco Secure ACS running AAA. If the switch receives the Session-Timeout value, this value overrides the revalidation timer value on the switch.

If the revalidation timer expires, the switch action depends on the value of the Termination-Action attribute:

- If the value of the Termination-Action RADIUS attribute is the default, the session ends.
- If the switch gets a value for the Termination-Action attribute other than the default, the EAPoUDP session and the current access policy remain in effect during posture revalidation.
- If the value of the Termination-Action attribute is *RADIUS*, the switch revalidates the client.
- If the packet from the server does not include the Termination-Action attribute, the EAPoUDP session ends.

Status-Query Timer

The status-query timer controls the amount of time the switch waits before verifying that the previously validated client is present and that its posture has not changed. Only clients that were authenticated with EAPoUDP messages use this timer, which starts after the client is initially validated. The default value of the status-query timer is 300 seconds (5 minutes).

The timer resets when the host is re-authenticated. When the timer expires, the switch checks the host posture validation by sending a Status-Query message to the host. If the host sends a message to the switch that the posture has changed, the switch revalidates the posture of the host.

NAC Layer 2 IP Validation and Switch Stacks

Note This information applies to the Catalyst 3750 series switch and EtherSwitch service modules.

When the new stack master is elected, all the previously validated hosts connected to the switch stack must be revalidated if NAC Layer 2 IP is still enabled on interfaces to which the hosts are connected. If NAC Layer 2 IP is disabled on the interfaces, the previously validated hosts cannot be revalidated.

NAC Layer 2 IP Validation and Redundant Modular Switches

Note This information applies to the Catalyst 4500 and 6500 switches, and the Catalyst 7600 router.

When RPR mode redundancy is configured, a switchover will lose all information regarding currently postured hosts. When SSO mode redundancy is configured, a switchover will trigger a reposturing of all currently postured hosts.

AAA Down Policy for NAC Layer 2 IP Validation

Note This feature is not available on the Catalyst 4500 series switch.

For the AAA Down Policy, the system works as follows:

1. A new session is detected.
2. Before posture validation is triggered and provided the AAA server is unreachable, the AAA down policy is applied and session state is maintained as AAA DOWN.
3. When the AAA server is once again available, a revalidation will be re-triggered for the host.

Note When the AAA server is down, the AAA down policy is applied only if there is no existing policy associated with the host. Typically, during revalidation when the AAA server goes down, the policies being used for the host are retained.

NAC Configuration Guidelines and Restrictions

This section contains these configuration guidelines and restrictions:

- NAC Layer 2 IEEE 802.1x Guidelines, Limitations, and Restrictions, page 18
- NAC Layer 2 IP Guidelines, Limitations, and Restrictions, page 19

NAC Layer 2 IEEE 802.1x Guidelines, Limitations, and Restrictions

Note These guidelines apply to Catalyst 4900, 4500, 3750, 3560, 3550, 2970, 2960, 2955, 2950, and 2940 switches; Cisco Gigabit Ethernet Switching Module (CGESM), and Cisco EtherSwitch service modules.

The following items apply to the VLAN assigned to the port by the ACS server:

- The VLAN must be a valid VLAN on the switch.
- The switch port can be configured as a static-access port that is assigned to a nonprivate VLAN.
- The switch port can be configured as a private-VLAN port that belongs to a secondary private VLAN. All the hosts connected to the switch port are assigned to private VLANs, regardless whether or not the posture validation was successful.

  If the VLAN type in the Access-Accept message does not match the VLAN type of the switch port to which the client is assigned, the VLAN assignment fails.

  When assigning a port to a private VLAN, specify the secondary private VLAN. The switch determines the primary private VLAN by using the primary- and secondary-private-VLAN associations on the switch.

- For a list of ports on which NAC Layer 2 IEEE 802.1X cannot be configured, see the “IEEE 802.1X Configuration Guidelines” section in the “Understanding and Configuring 802.1X Port-Based Authentication” chapter of your software configuration guide.

- If you configure a guest VLAN to which nonresponsive hosts are assigned, the guest VLAN type must correspond to the appropriate port type. If the VLAN type does not correspond to the switch port type, nonresponsive hosts are denied network access.
- If the guest VLAN is configured on an access port, the VLAN type is a nonprivate VLAN. If the guest VLAN is configured on a private-VLAN port, the VLAN type is private VLAN.

  To support NAC, Access points must be configured for EAP authentication and VLANs.

  For instructions on configuring EAP authentication on access points, refer to the "Configuring Authentication Types" chapter in
  Cisco IOS Software Configuration Guide for Cisco Aironet Access Points:
  http://www.cisco.com/en/US/products/hw/wireless/ps430/products_configuration_guide_chapter09186a00804e7d09.html

  For instructions on configuring VLANs on access points, refer to the "Configuring VLANs" chapter in *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*:
  http://www.cisco.com/en/US/products/hw/wireless/ps430/products_configuration_guide_chapter09186a00804e7d4e.html
- NAC Layer 2 IEEE 802.1X interacts with other features in these ways:
  - If a host is assigned to a voice VLAN, the switch does not validate the posture of the host because you cannot configure a voice VLAN on a private-VLAN port.
  - By default, nonresponsive hosts are assigned to a guest VLAN. All other hosts, those with successful posture validation and those running legacy IEEE 802.1X-compliant client software without NAC, are granted network access based on the access control decision.
  - For more feature interactions, See the "IEEE 802.1X Configuration Guidelines" section in the "Configuring 802.1X Port-Based Authentication" chapter of your software configuration guide.
- NAC Layer 2 IEEE 802.1X AAA Down Policy is supported only on the Catalyst 3560 and Catalyst 3750 series switches.

NAC Layer 2 IP Guidelines, Limitations, and Restrictions

Note These guidelines apply to CGESM switches, the Cisco EtherSwitch service modules, the Catalyst 7600 router, and the Catalyst 6500, 4900, 4500, 3750, 3560, and 3550 switches.

Follow these guidelines, limitations, and restrictions when configuring NAC Layer 2 IP validation:

- To enable NAC Layer 2 IP, a Layer 3 route *must* be configured from the switch to the host.
- The default ACL *must* permit EAPoUDP traffic for LPIP to function.
- For all switches other than the Catalyst 6500 (and the Catalyst 7600 series router), NAC Layer 2 IP validation is not supported on trunk ports, tunnel ports, EtherChannels, EtherChannel members, or routed ports.
- When NAC Layer 2 IP validation is enabled, you must configure a default port ACL on the switch port to which hosts are connected.
- NAC Layer 2 IP does not validate the posture of IPv6 traffic and does not apply access policies to IPv6 traffic.
- A denial-of-service attack might occur if the switch receives many ARP packets with different source IP addresses.

For information on rate limiting ARP packets, see the discussion of the **ip arp inspection limit** in the *Cisco IOS command reference* at the URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/secur_r/sec_p1g.htm

- When NAC Layer 2 IP and NAC Layer 2 IEEE 802.1X are enabled on the same access port, IEEE 802.1X authentication takes precedence. (That is, if IEEE 802.1X authentication fails, NAC Layer 2 IP validation will not happen.) The posture of the host to which the port is connected might already have been validated, and the switch would have applied the access limitations based on IEEE 802.1X.
- DHCP Snooping must be enabled if the switch wants to use DHCP lease grants to identify connected hosts.
- For DHCP snooping functionality, the DHCP traffic should be permitted in the interface default ACL as well as the host policy.
- The DHCP packets should be permitted in a DHCP environment in the default interface as well as downloaded host policy.
- If you want the end stations to send DNS requests before posture validation occurs, you must configure the named downloadable ACL on the switch port with ACEs permitting DNS packets.
- If you want to forward the HTTP and HTTPS requests from an endpoint device to a specific URL, you must enable the HTTP server feature and define the url-redirect-acl should be defined as the URL ACL name. The URL ACL should be locally defined on the switch. This ACL should normally contain a “deny tcp any <remediation server address> eq www” and followed by the permit ACEs for the HTTP traffic that needs to be redirected.
- If NAC Layer 2 IP validation is configured on a switch port that belongs to a voice VLAN, the switch does not validate the posture of the IP phone. Make sure that the IP phone is on the exception list.
- If NAC Layer 2 IP validation is enabled, and VLAN ACL and Router ACLs are configured, the policies are serially applied in the order “NAC Layer 2 LP IP Policy>VLAN ACL>Router ACL.” The next policy is applied only when the traffic passes through the previous policy check. If any of the policy denied the traffic, the traffic will be denied.

Note The NAC Layer 2 IP host policy (downloaded from ACS) always overrides the default interface policy.

- If dynamic ARP inspection is enabled on the ingress VLAN, the switch initiates posture validation only after the ARP packets are validated.
- If IP Source Guard and NAC Layer 2 IP are enabled on the switch port, posture validation is not initiated by traffic that is blocked by IP Source Guard.
- If IEEE 802.1X authentication in single-host mode and NAC Layer 2 IP validation are configured on a switch port and IEEE 802.1X authentication of the connected hosts fails, the switch does not initiate posture validation when it receives DHCP or ARP packets from the host.

  If IEEE 802.1X authentication is configured on the port, the port cannot send or receive traffic other than EAPOL frames until the client is successfully authenticated.
- On the Catalyst 4500 series switch, the access-group mode command can be used to control whether NAC Layer 2 IP host policy ACLs override VLAN and router ACLs or are merged with them.
- On the Catalyst 6500 series switch and the Catalyst 7600 series router, the traffic that hits the URL-Redirect deny ACEs is forwarded in hardware without applying the default interface and downloaded host policies. If this traffic (that is, what matches the deny URL-Redirect ACEs) must be filtered, you should define a VLAN ACL on the switch port access VLAN.

- The Catalyst 6500 series switch and the Catalyst 7600 series router do not support NAC Layer 2 IP validation on trunk ports, tunnel ports, EtherChannel members, or routed ports. However, the Catalyst 6500 series switch and the Catalyst 7600 series router *support* Layer 2 IP on Etherchannels.
- The Catalyst 6500 series switch and the Catalyst 7600 series router do not allow NAC Layer 2 IP on the switchport if the parent VLAN of the port has VACL Capture and/or IOS Firewall (CBAC) configured.
- The Catalyst 6500 series switch and the Catalyst 7600 series router, do not support NAC Layer 2 IP if the switchport is part of a private VLAN.
- For the Catalyst 6500 series switch and the Catalyst 7600 series router, NAC Layer 2 LPIP ARP traffic redirected to the CPU cannot be spanned using the SPAN feature.

How to Configure NAC

This section contains the following topics:

Default NAC Configuration

For the default NAC Layer 2 IEEE 802.1X configuration, see the “Default IEEE 802.1X Configuration” section in the “Configuring 802.1X Port-Based Authentication” chapter of your software configuration guide.

By default, NAC Layer 2 IP validation is disabled.

Configuring NAC Layer 2 IEEE 802.1X

To configure NAC Layer 2 IEEE 802.1X on your Catalyst 4500 series switch, see the “Enabling 802.1X Authentication” and “Configuring Switch-to-Radius-Server Communication” sections in your software configuration guide.) All other tasks listed are optional.

http://www.cisco.com/en/US/products/hw/switches/ps4324/tsd_products_support_series_home.html

For all other switches, see the “Configuring IEEE 802.1X Authentication and Validation” and the “Configuring IEEE 802.1x Authentication Using a RADIUS Server” sections in your software configuration guide.

For the Catalyst 3750 series switch, refer to the URL:
http://www.cisco.com/en/US/products/hw/switches/ps5023/tsd_products_support_series_home.html

For the Catalyst 3560 series switch, refer to the URL:
http://www.cisco.com/en/US/products/hw/switches/ps5528/tsd_products_support_series_home.html

For the Catalyst 3550 series switch, refer to the URL:
http://www.cisco.com/en/US/products/hw/switches/ps646/tsd_products_support_series_home.html

For the Catalyst 2970 series switch, refer to the URL:
http://www.cisco.com/en/US/products/hw/switches/ps5206/tsd_products_support_series_home.html

For the Catalyst 2960 series switch, refer to the URL:
http://www.cisco.com/en/US/products/ps6406/tsd_products_support_series_home.html

For the Catalyst 2955 and 2950 series switches, refer to the URL:
http://www.cisco.com/en/US/products/hw/switches/ps628/tsd_products_support_series_home.html

For the Catalyst 2940 series switch, refer to the URL:
http://www.cisco.com/en/US/products/hw/switches/ps5213/tsd_products_support_series_home.html

Configuring NAC Layer 2 IP Validation

To configure NAC Layer 2 IP validation, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ip admission name** *rule-name* **eapoudp**	Creates and configures an IP NAC rule by specifying the rule name. To remove the IP NAC rule on the switch, use the **no ip admission name** *rule-name* **eapoudp** global configuration command.
Step 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]	Defines the default port ACL by using a source address and wildcard. The *access-list-number* is a decimal number from 1 to 99 or 1300 to 1999. Enter **deny** or **permit** to specify whether to deny or permit access if conditions are matched. The *source* is the source address of the network or host from which the packet is being sent specified as: • The 32-bit quantity in dotted-decimal format. • The keyword **any** as an abbreviation for *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. You do not need to enter a *source-wildcard*. • The keyword **host** as an abbreviation for source and source-wildcard of *source* 0.0.0.0. (Optional) The *source-wildcard* applies wildcard bits to the source. (Optional) Enter **log** to cause an informational logging message about the packet that matches the entry to be sent to the console.
Step 4	**interface** *interface-id*	Enters interface configuration mode.
Step 5	**ip access-group** {*access-list-number* | *name*} **in**	Controls access to the specified interface.

	Command	Purpose
Step 6	**ip admission name** *rule-name*	Applies the specified IP NAC rule to the interface. To remove the IP NAC rule that was applied to a specific interface, use the **no ip admission** *rule-name* interface configuration command.
Step 7	**exit**	Returns to global configuration mode.
Step 8	**aaa new-model**	Enables AAA.
Step 9	**aaa authentication eou default group radius**	Sets authentication methods for EAPoUDP. To remove the EAPoUDP authentication methods, use the **no aaa authentication eou default** global configuration command.
Step 10	**ip device tracking**	Enables the IP device tracking table. To disable the IP device tracking table, use the **no ip device tracking** global configuration commands.
Step 11	**ip device tracking [probe** {**count** *count* | **interval** *interval*}]	(Optional) Configures these parameters for the IP device tracking table: • **count** *count*—Set the number of times that the switch sends the ARP probe. The range is from 1 to 5. The default is 3. • **interval** *interval*—Set the number of seconds that the switch waits for a response before resending the ARP probe. The range is from 30 to 300 seconds. The default is 30 seconds.
Step 12	**radius-server host** {*hostname* | *ip-address*} **key** *string*	(Optional) Configures the RADIUS server parameters. For *hostname* | *ip-address,* specify the hostname or IP address of the remote RADIUS server. For **key** *string*, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server. **Note** Always configure the key as the last item in the **radius-server host** command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon. If you want to use multiple RADIUS servers, re-enter this command.
Step 13	**radius-server attribute 8 include-in-access-req**	(Optional) If the switch is connected to nonresponsive hosts, configure the switch to send the Framed-IP-Address RADIUS attribute (Attribute[8]) in access-request or accounting-request packets. To configure the switch to not send the Framed-IP-Address attribute, use the **no radius-server attribute 8 include-in-access-req** global configuration command.
Step 14	**radius-server vsa send authentication**	Configures the network access server to recognize and use vendor-specific attributes.
Step 15	**eou logging**	(Optional) Enables EAPoUDP system logging events. To disable the logging of EAPoUDP system events, use the **no eou logging** global configuration command.

	Command	Purpose
Step 16	**end**	Returns to privileged EXEC mode.
Step 17	**show ip admission** {[**cache**] [**configuration**] [**eapoudp**]}	Displays the NAC configuration or network admission cache entries.
Step 18	**show ip device tracking** {**all** | **interface** *interface-id* | **ip** *ip-address* | **mac** *mac-address*}	Displays information about the entries in the IP device tracking table.
Step 19	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To configure the auth-proxy posture code to not get security associations from the AAA server, use the **no aaa authorization auth-proxy default** global configuration command.

To clear all NAC client device entries on the switch or on the specified interface, use the **clear eou** privileged EXEC command. To clear entries in the IP device tracking table, use the **clear ip device tracking** privileged EXEC command.

This example shows how to configure NAC Layer 2 IP validation on a switch interface:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip admission name nac eapoudp
Switch(config)# access-list 5 permit any any
Switch(config)# interface gigabitethernet 2/0/1
Switch(config-if)# ip access-group 5 in
Switch(config-if)# ip admission name nac
Switch(config-if)# exit
Switch(config)# aaa new-model
Switch(config)# aaa authentication eou default group radius
Switch(config)# ip device tracking
Switch(config)# ip device tracking probe count 2
Switch(config)# radius-server host admin key rad123
Switch(config)# radius-server vsa send authentication
Switch(config)# eou logging
Switch(config)# end
Switch# show ip admission configuration

Authentication global cache time is 60 minutes Authentication global absolute time is 0
minutes Authentication global init state time is 2 minutes Authentication Proxy Watch-list
is disabled

Authentication Proxy Rule Configuration
 Auth-proxy name nac
    eapoudp list not specified auth-cache-time 60 minutes

Switch# show ip device tracking all
IP Device Tracking = Enabled
---------------------------------------------------------------
  IP Address     MAC Address       Interface          STATE
---------------------------------------------------------------
10.5.0.25       0060.b0f8.fbfb GigabitEthernet1/0/4   ACTIVE
```

Configuring EAPoUDP

EAPoUDP is the protocol that NAC Layer 2 IP uses to exchange posture information with the endpoint system. To fine tune the EAPoUDP state machine parameters, follow steps:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**eou allow** {**clientless** | **ip-station-id**} **eou default** **eou logging** **eou max-retry** *number* **eou port** *port-number* **eou ratelimit** *number* **eou timeout** {**aaa** *seconds* | **hold-period** *seconds* | **retransmit** *seconds* | **revalidation** *seconds* | **status-query** *seconds*} **eou revalidate**	Specifies EAPoUDP values. For more information about the keywords for the **allow**, **default**, **logging**, **max-retry**, **port**, **rate-limit**, **revalidate**, and **timeout** options, see the command reference portion of this document.
Step 3	**interface** *interface-id*	Enters interface configuration mode.
Step 4	**eou default** **eou max-retry** *number* **eou timeout** {**aaa** *seconds* | **hold-period** *seconds* | **retransmit** *seconds* | **revalidation** *seconds* | **status-query** *seconds*} **eou revalidate**	Enables and configures the EAPoUDP association for the specified interface. For more information about the keywords for the **default**, **max-retry**, **revalidate**, and **timeout** options, see the command reference portion of this document.
Step 5	**end**	Returns to privileged EXEC mode.
Step 6	**show eou** {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface** *interface-id* | **ip** *ip-address* | **mac** *mac-address* | **posturetoken** *name*}	Displays information about the EAPoUDP configuration or session cache entries.
Step 7	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To return to the global default EAPoUDP values, use the **no** forms of the **eou** global configuration commands. To disable the EAPoUDP associations, use the **no** forms of the **eou i**nterface configuration commands.

This example shows how to configure EAPoUDP on a switch interface:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# eou logging
Switch(config)# eou allow clientless
Switch(config)# eou timeout revalidation 2400
Switch(config)# eou revalidate
```

```
Switch(config)# interface gigabitEthernet 1/0/4
Switch(config-if)# eou timeout status-query 600
Switch(config-if)# end
Switch# show eou

Global EAPoUDP Configuration
----------------------------
EAPoUDP Version     = 1
EAPoUDP Port        = 0x5566
Clientless Hosts    = Enabled
IP Station ID       = Disabled
Revalidation        = Enabled
Revalidation Period = 2400 Seconds
ReTransmit Period   = 3 Seconds
StatusQuery Period  = 300 Seconds
Hold Period         = 180 Seconds
AAA Timeout         = 60 Seconds
Max Retries         = 3
EAP Rate Limit      = 20
EAPoUDP Logging     = Enabled

Interface Specific EAPoUDP Configurations
-----------------------------------------
Interface GigabitEthernet1/0/4
  StatusQuery Period  = 600 Seconds
```

Configuring Identity Profiles and Policies

To configure the identity profile and policy, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**identity policy** *policy-name*	Creates an identity policy, and enter identity-policy configuration mode. To remove the identity policy from the switch, use the **no identity-policy** *policy-name* global configuration command.
Step 3	**access-group** *access-group*	(Optional) Defines network access attributes for the identity policy.
Step 4	**identity profile eapoudp**	Creates an identity profile, and enter identity-profile configuration mode. To remove the identity profile, use the **no identity profile eapoudp** global configuration command.
Step 5	**device** {**authorize** | **not-authorize**} {**ip-address** *ip-address* | **mac-address** *mac-address* | **type cisco ip phone**} [**policy** *policy-name*]	Authorizes the specified IP device, and apply the specified policy to the device. To not authorize the specified IP device and remove the specified policy from the device, use the **no device** {**authorize** | **not-authorize**} {**ip-address** *ip-address* | **mac-address** *mac-address* | **type cisco ip phone**} [**policy** *policy-name*] interface configuration command.
Step 6	**exit**	Exits identity-profile configuration mode, and returns to global configuration mode.
Step 7	**end**	Returns to privileged EXEC mode.
Step 8	**show identity** [**policy**| **profile**]	Displays the configured identity policies and/or profiles.

	Command	Purpose
Step 9	**show running-config**	Verifies your entries.
Step 10	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

This example shows how to configure a profile that will authorize a host based on IP address, and associate a local policy with that host:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# identity policy policy1
Switch(config-identity-policy)# access-group group1
Switch(config)# identity profile eapoudp
Switch(config-identity-prof)# device authorize ip address 10.10.142.25 policy policy1
Switch(config-identity-prof)# exit
Switch(config)# end
Switch# show identity policy
Policy Name     ACL             Redirect ACL    Redirect URL
================================================================================
policy1         group1          NONE            NONE

Switch# show identity profile
No identity profile of type default is configured.

No identity profile of type dot1x is configured.

Service Type: eapoudp

Device / Address / Mask            Allowed         Policy
============================================================
10.5.0.99       / 0.0.0.0          Authorized      policy1
```

Configuring IP Device Tracking

Note You must perform this task to enable Layer 2 IP Validation.

NAC Layer 2 IP validation does not use an intercept ACL to define a subset of traffic that triggers posture validation. (This is different from Layer 3 implementations.) Instead, the IP Device Tracking table is used to track new hosts as they appear on the network. The IP Device Tracking table detects hosts through the following mechanisms:

- IP ARP Inspection
- IP DHCP Snooping (optional)

IP ARP Inspection is enabled automatically when IP Device Tracking is enabled. It detects the presence of new hosts by monitoring ARP packets. IP DHCP Snooping, if enabled, detects the presence or removal of new hosts when DHCP assigns or revokes their IP addresses.

Note If dynamic ARP inspection is enabled, only the ARP packets that it validates are used to detect new hosts for the Device Tracking table.

Once a device is added to the IP Device Tracking table, the device is monitored through periodic ARP probes. Hosts that fail to respond to these probes are removed from the Device Tracking table.

Note Optionally, you can configure the probe timeout and the maximum probe count. The probes are used to track the hosts after they are learned on the NAD.

To configure IP Device Tracking, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ip device tracking**	(Required) Enables IP Device Tracking. This enables the learning of the Layer 2 IP devices by snooping ARP packets on the ports where IP Admission is enabled.
Step 3	**ip device tracking probe count** *n*	(Optional) Changes the maximum no of times IP Device Tracker will probe the device. Default is 3.
Step 4	**ip device tracking probe interval** *interval_number*	(Optional) Changes the probe interval. Default is 30 seconds.
Step 5	**exit**	Exits identity-profile configuration mode, and returns to global configuration mode.
Step 6	**end**	Returns to privileged EXEC mode.
Step 7	**show ip device tracking** [**all**]	Displays the list of IP hosts that have been detected on the switch. These hosts are candidates for NAC Layer2 IP posture validation.
Step 8	**show running-config**	Verifies your entries.
Step 9	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

The following example shows how to configure IP Device Tracking:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# ip device tracking probe count 3
Switch(config)# ip device tracking probe interval 60
Switch(config)# end
Switch# show ip device tracking all
IP Device Tracking = Enabled
------------------------------------------------------------
IP Address     MAC Address       Interface          STATE
------------------------------------------------------------
8.0.0.1         0060.b0f8.fbfb GigabitEthernet1/0/4   ACTIVE
```

Note Along with IP Device Tracking, you *must* configure either IP DHCP snooping or IP ARP Inspection for NAC functionality.

Configuring IP DHCP Snooping for NAC (Optional)

If DHCP is required as a trigger/device learning mechanism for Layer 2 IP Validation, you must configure IP DHCP Snooping. The DHCP Snooping should be enabled on the both voice and data VLAN of the switchport where IP Admission is enabled.

To configure IP DHCP Snooping, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ip dhcp snooping**	Enables IP DHCP Snooping on the switch.
Step 3	**ip dhcp snooping vlan** *vlan_id*	Enables IP DHCP Snooping on the ingress VLAN of the switch.
Step 4	**ip dhcp snooping trust**	Enables the DHCP Snooping trust state for the interface. You should enable the DHCP Snooping trust state on the uplink ports where DHCP server is connected.
Step 5	**exit**	Exits identity-profile configuration mode, and returns to global configuration mode.
Step 6	**end**	Returns to privileged EXEC mode.
Step 7	**show ip dhcp snooping** [**binding**]	Displays the current DHCP snooping configuration. You can use the optional **binding** keyword to display the list of DHCP leases that have been detected by DHCP Snooping.
Step 8	**show running-config**	Verifies your entries.
Step 9	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

The following example shows how to configure IP DHCP Snooping for NAC:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 8
Switch(config)# end
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1,10,1001
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed Verification of hwaddr field is enabled
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------

Switch# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:60:B0:F8:FB:FB   8.0.0.1          79464       dhcp-snooping  8     GigabitEthernet1/0/4
Total number of bindings: 1
```

If you intend to use IP ARP Inspection alone, then one of the following preconditions should apply:

- A static ARP-filter ACL exists that will allow only those IPs that must be trusted (and should be allowed to form ARP entries on the NAD).
- The switch contains an IP DHCP snooping binding entry that allows the IP ARP Inspection feature to validate the IP ARP entries.

- The NAC ingress interface is made trusted for IP ARP Inspection. Generally, this is not feasible, because clients on the NAC ingress interface are the ones being monitored.

Configuring IP ARP Inspection with an ARP-filter List (Optional)

This task enables the learning of Layer 2 IP devices with static IP address assignments that are subject to dynamic ARP inspection validation checks.

To configure IP ARP Inspection with an ARP-filter list, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**arp access-list** *static-arp-list*	Configures the static IP ARP filter ACL on the NAD to allow the IPs N/W and MAC address to be trusted.
Step 3	**deny [ip [any | host** *sender-ip* [*sender-ip-mask*]]] **[mac any]**	Drops ARP packets based on some matching criteria.
Step 4	**permits [ip [any | host** *sender-ip* [*sender-ip-mask*]]] **[mac any]**	Forwards ARP packets based on some matching criteria.
Step 5	**exit**	Exits identity-profile configuration mode, and returns to global configuration mode.
Step 6	**ip arp inspection vlan***vlan_id*	Enables IP ARP inspection on the VLAN.
Step 7	**ip arp inspection filter** *static-arp-list* **vlan** *vlan_id*	Enables IP ARP inspection on the ingress VLAN on the switch. **Note** Perform this step provided IP DHCP Snooping entries are not formed on the device being tested
Step 8	**end**	Returns to privileged EXEC mode.
Step 9	**show ip arp inspection** [**statistics**] [**vlan** *vlan_id]*	Displays the current ARP Inspection configuration or statistics. You can use the optional **vlan** keyword to display information for a specific VLAN.
Step 10	**show running-config**	Verifies your entries.
Step 11	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

The following example shows how to configure IP ARP Inspection with an ARP-filter list:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# arp access-list arp-list
Switch(config-arp-nacl)# deny ip host 101.50.1.54 mac any
Switch(config-arp-nacl)# deny ip host 101.50.1.51 mac any
Switch(config-arp-nacl)# permit ip 101.50.1.0 0.0.0.255 mac any
Switch(config-arp-nacl)# exit
Switch(config)# ip arp inspection vlan 101
Switch(config)# ip arp inspection filter arp-acl vlan 101
Switch(config)# end
Switch# show ip arp inspection vlan 101

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
```

```
 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
  101     Enabled          Active      arp-acl            No

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
  101     Deny             Deny

Switch# show ip arp inspection statistics

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
 101              9              2              0              4

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
  101              9              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
  101                   0                        0                      0
```

Configuring IP ARP Inspection with IP DHCP Snooping (Optional)

This enables Layer 2 IP device learning to be subject to ARP Inspection feature validation checks. By default the ARP packets are validated using DHCP Snooping bindings.

Note To perform this task, you must first enable DHCP Snooping on the same VLANs where ARP Inspection is enabled.

To configure IP ARP Inspection with IP DHCP Snooping, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ip dhcp snooping**	Enables IP DHCP Snooping on the switch.
Step 3	**ip dhcp snooping vlan** *vlan_id*	Enables IP DHCP Snooping on the ingress VLAN of the switch.
Step 4	**ip dhcp snooping trust**	Enables the DHCP Snooping trust state for the interface.
Step 5	**ip arp inspection vlan** *vlan_id*	Enables IP ARP inspection on the VLAN. **Note** DHCP Snooping should be enabled on this VLAN, where IP ARP Inspection is enabled.
Step 6	**ip arp inspection vlan trust**	Enables the ARP Inspection trust state for the interface. You should enable ARP Inspection trust on the uplink ports where DHCP server is connected. This is required to allow ARP packets from the server without validation checks.
Step 7	**ip arp inspection filter** *static-arp-list* **vlan** *vlan_id*	Enables IP ARP inspection on the ingress VLAN on the switch. **Note** Perform this step provided IP DHCP Snooping entries are not formed on the device being tested.
Step 8	**end**	Returns to privileged EXEC mode.

	Command	Purpose
Step 9	**show ip arp inspection** [**statistics**] [**vlan** *vlan_id*]	Displays the current ARP Inspection configuration or statistics. You can use the optional **vlan** keyword to display information for a specific VLAN.
Step 10	**show running-config**	Verifies your entries.
Step 11	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Note For this configuration, you need not configure a static ARP filter list.

The following example shows how to configure IP ARP Inspection with IP DHCP Snooping:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip dhcp snooping vlan 8
Switch(config)# ip arp inspection vlan 8
Switch(config)# end
Switch# show ip arp inspection vlan 8

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    8     Enabled          Active

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
   8     Deny             Deny

Switch# show ip arp inspection statistics vlan 8

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
    8              4              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
   8              4              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
   8                   0                        0
```

Configuring a NAC AAA Down Policy (Optional)

Note NAC Layer 2 IP validation is not available on the Catalyst 4500 series switch.

To configure NAC AAA down policy, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ip admission name** *rule-name* **eapoudp event timeout aaa policy identity** *identity_policy_name*	Creates a NAC a rule and associate an identity policy to be applied to sessions, when the AAA server is unreachable. To remove the rule on the switch use the **no ip admission name** *rule-name* **eapoudp event timeout aaa policy** global configuration command.
Step 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]	Defines the default port ACL by using a source address and wildcard. The *access-list-number* is a decimal number from 1 to 99 or 1300 to 1999. Enter **deny** or **permit** to specify whether to deny or permit access if conditions are matched. The *source* is the source address of the network or host from which the packet is being sent specified as: • The 32-bit quantity in dotted-decimal format. • The keyword **any** as an abbreviation for *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. You do not need to enter a *source-wildcard*. • The keyword **host** as an abbreviation for source and source-wildcard of *source* 0.0.0.0. (Optional) The *source-wildcard* applies wildcard bits to the source. (Optional) Enter **log** to cause an informational logging message about the packet that matches the entry to be sent to the console.
Step 4	**interface** *interface-id*	Enters interface configuration mode.
Step 5	**ip access-group** {*access-list-number* | *name*} **in**	Controls access to the specified interface.
Step 6	**ip admission name** *rule-name*	Applies the specified IP NAC rule to the interface. To remove the IP NAC rule that was applied to a specific interface, use the **no ip admission** *rule-name* interface configuration command.
Step 7	**exit**	Returns to global configuration mode.
Step 8	**aaa new-model**	Enables AAA.
Step 9	**aaa authentication eou default group radius**	Sets authentication methods for EAPoUDP. To remove the EAPoUDP authentication methods, use the **no aaa authentication eou default** global configuration command.
Step 10	**aaa authorization network default local**	Sets the authorization method to local. To remove the authorization method, use **no aaa authorization network default local** command.
Step 11	**ip device tracking**	Enables the IP device tracking table. To disable the IP device tracking table, use the **no ip device tracking** global configuration commands.

	Command	Purpose
Step 12	**ip device tracking [probe** {**count** *count* **| interval** *interval*}]	Configures these parameters for the IP device tracking table: • **count** *count*—Set the number of times that the switch sends the ARP probe. The range is from 1 to 5. The default is 3. • **interval** *interval*—Set the number of seconds that the switch waits for a response before resending the ARP probe. The range is from 30 to 300 seconds. The default is 30 seconds.
Step 13	**radius-server host** {*hostname* | *ip-address*} **test username** *username* **idle-time 1 key string**	Configures the RADIUS server parameters. For *hostname* | *ip-address,* specify the hostname or IP address of the remote RADIUS server. For **key** *string*, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server. **Note** Always configure the key as the last item in the **radius-server host** command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon. **test username** is used for configuring the dummy username that tests whether the AAA server is active or not. **idle-time** parameter is used to set how often the SERVER should be tested for liveness. If there is no traffic to the RADIUS server, the NAD will send dummy radius packets to the RADIUS server based on the idle-time. If you want to use multiple RADIUS servers, re-enter this command.
Step 14	**radius-server attribute 8 include-in-access-req**	If the switch is connected to nonresponsive hosts, configure the switch to send the Framed-IP-Address RADIUS attribute (Attribute[8]) in access-request or accounting-request packets. To configure the switch to not send the Framed-IP-Address attribute, use the **no radius-server attribute 8 include-in-access-req** global configuration command.
Step 15	**radius-server vsa send authentication**	Configures the network access server to recognize and use vendor-specific attributes.
Step 16	**radius-server dead-criteria** {**tries** | **time**} *value*	(Optional) Forces one or both of the criteria—used to mark a RADIUS server as dead—to be the indicated constant.
Step 17	**eou logging**	(Optional) Enables EAPoUDP system logging events. To disable the logging of EAPoUDP system events, use the **no eou logging** global configuration command.
Step 18	**end**	Returns to privileged EXEC mode.
Step 19	**show ip admission** {[**cache**] [**configuration**] [**eapoudp**]}	Displays the NAC configuration or network admission cache entries.

	Command	Purpose
Step 20	**show ip device tracking** {**all** | **interface** *interface-id* | **ip** *ip-address* | **mac** *mac-address*}	Displays information about the entries in the IP device tracking table.
Step 21	**show aaa servers**	Displays the status of the AAA servers that have been configured on the switch.
Step 22	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The following example illustrates how to apply a AAA down policy:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip admission name AAA_DOWN eapoudp event timeout aaa policy identity
global_policy
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default local
Switch(config)# aaa authentication eou default group radius
Switch(config)# identity policy global_policy
Switch(config-identity-policy)# ac
Switch(config-identity-policy)# access-group global_acl
Switch(config)# ip access-list extended global_acl
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# radius-server host 40.0.0.4 test username administrator idle-time 1 key
cisco
Switch(config)# radius-server dead-criteria tries 3
Switch(config)# radius-server vsa send authentication
Switch(config)# radius-server attribute 8 include-in-access-req
Switch(config)# int fastEthernet 2/13
Switch(config-if)# ip admission AAA_DOWN
Switch(config-if)# exit
Switch# show ip admission configuration
Authentication global cache time is 60 minutes Authentication global absolute time is 0
minutes Authentication global init state time is 2 minutes Authentication Proxy Watch-list
is disabled

Authentication Proxy Rule Configuration
 Auth-proxy name AAA_DOWN
    eapoudp list not specified auth-cache-time 60 minutes
    Identity policy name global_policy for AAA fail policy

Switch# show aaa servers
RADIUS: id 1, priority 1, host 40.0.0.4, auth-port 1645, acct-port 1646
     State: current UP, duration 5122s, previous duration 9s
     Dead: total time 79s, count 3
     Authen: request 158, timeouts 14
             Response: unexpected 1, server error 0, incorrect 0, time 180ms
             Transaction: success 144, failure 1
     Author: request 0, timeouts 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
     Account: request 0, timeouts 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
     Elapsed time since counters last cleared: 2h13m

Switch#show aaa method-lists authentication authen queue=AAA_ML_AUTHEN_LOGIN authen
queue=AAA_ML_AUTHEN_ENABLE authen queue=AAA_ML_AUTHEN_PPP authen queue=AAA_ML_AUTHEN_SGBP
authen queue=AAA_ML_AUTHEN_ARAP authen queue=AAA_ML_AUTHEN_EAPOUDP
```

```
  name=default valid=1 id=0 state=ALIVE : SERVER_GROUP radius authen
queue=AAA_ML_AUTHEN_DOT1X
  name=default valid=1 id=0 state=ALIVE : SERVER_GROUP radius permanent lists
  name=Permanent Enable None valid=1 id=0 ALIVE : ENABLE  NONE
  name=Permanent Enable valid=1 id=0 ALIVE : ENABLE
  name=Permanent None valid=1 id=0 ALIVE : NONE
  name=Permanent Local valid=1 id=0 ALIVE : LOCAL
```

Displaying NAC Information

Note Access points *do not* support the following commands.

To display NAC information, use one of the following privileged EXEC commands:

Table 3 Commands for Displaying NAC Information

Command	Purpose
show dot1x [**all** | **interface** *interface-id* | **statistics interface** *interface-id*]	Display IEEE 802.1x statistics, administrative status, and operational status.
show eou {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface** *interface-id* | **ip** *ip-address* | **mac** *mac-address* | **posturetoken** *name*}	Display information about the EAPoUDP configuration or session cache entries.
show ip admission {[**cache**] [**configuration**] [**eapoudp**]}	Display the NAC configuration or network admission cache entries.
show ip device tracking {**all** | **interface** *interface-id* | **ip** *ip-address* | **mac** *mac-address*}	Display information about the entries in the IP device tracking table.

This example shows the sample output when a new host is detected:

```
00:45:15: %EOU-6-SESSION: IP=10.5.0.25| HOST=DETECTED| Interface=GigabitEthernet1/0/4
00:45:15: %EOU-6-CTA: IP=10.5.0.25| CiscoTrustAgent=DETECTED
00:45:16: %EOU-6-POLICY: IP=10.5.0.25| TOKEN=Healthy
00:45:16: %EOU-6-POLICY: IP=10.5.0.25| URL=http://10.5.0.43
00:45:16: %EOU-6-POLICY: IP=10.5.0.25| URL ACL=s-acl
00:45:16: %EOU-6-POLICY: IP=10.5.0.25| ACLNAME=#ACSACL#-IP-Healthy-42dbdd9d
00:45:16: %EOU-6-POLICY: IP=10.5.0.25| HOSTNAME=CMELTER-XP:dsbu
00:45:16: %EOU-6-POSTURE: IP=10.5.0.25| HOST=AUTHORIZED| Interface=GigabitEthernet1/0/4
00:45:16: %EOU-6-AUTHTYPE: IP=10.5.0.25| AuthType=EAP

Switch# show eou all
-------------------------------------------------------------------------
Address         Interface              AuthType   Posture-Token Age(min)
-------------------------------------------------------------------------
10.5.0.25       GigabitEthernet1/0/4   EAP        Healthy         0

Switch# show eou ip 10.5.0.25
Address             : 10.5.0.25
MAC Address         : 0060.b0f8.fbfb
Interface           : GigabitEthernet1/0/4
```

```
AuthType            : EAP
Audit Session ID    : 0000000000296E2E000000040A050019
PostureToken        : Healthy
Age(min)            : 0
URL Redirect        : http://10.5.0.43
URL Redirect ACL    : s-acl
ACL Name            : #ACSACL#-IP-Healthy-42dbdd9d
User Name           : HOST-XP:dsbu
Revalidation Period : 600 Seconds
Status Query Period : 600 Seconds
Current State       : AUTHENTICATED
```

Clearing EAPoUDP Session Table

To clear client entries in the EAPoUDP session table, use the **clear eou** privileged EXEC command. After the entries are removed, they are created only after the switch receives an ARP packet from the host or after it creates a DHCP snooping binding entry for the host. To clear entries in the IP device tracking table on the switch, use the **clear ip device tracking** privileged EXEC command.

Command Reference

Note Access points *do not* support the commands in this section of the document.

This section documents those NAC Layer 2 IP commands that are not generic to Cisco IOS. For documentation on the generic Cisco IOS commands, refer to the following URLs:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_8/gt_nac.htm

and

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/secur_r/sec_p1g.htm

aaa authentication eou

To set Extensible Authentication Protocol over UDP (EAPoUDP or EoU) authentication methods on the switch, use the **aaa authentication eou** global configuration command. Use the **no** form of this command to remove the authentication methods.

aaa authentication eou default group radius

no aaa authentication eou default

Syntax Description

This command has no arguments or keywords.

Defaults

No EAPoUDP authentication methods are configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

After configuring ACLs and defining the IP Network Admission Control (NAC) rule, you can configure EAPoUDP authentication methods on a switch. You can also set the authentication proxy methods by using the **aaa authorization auth-proxy default group radius** global configuration command.

Examples

This example shows how to set EAPoUDP authentication methods:

```
Switch(config)# aaa authentication eou default group radius
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
aaa authorization auth-proxy default	Enables and configures EAPoUDP authorization methods.
identity profile eapoudp	Creates an identity profile and enters EAPoUDP profile configuration mode. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
ip admission name eapoudp	Creates and configures IP NAC rules.

Command	Description
show ip admission	Displays information about NAC cached entries or the NAC configuration. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
show running-config	Displays the operating configuration. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

aaa authorization auth-proxy default

To enable the auth-proxy posture code to get security associations from the authentication, authorization, and accounting (AAA) server, use the **aaa authorization auth-proxy default** global configuration command. Use the **no** form of this command to disable this feature.

aaa authorization auth-proxy default group radius

no aaa authorization auth-proxy default

Note Though visible in the command-line help strings, the **cache**, *server-group-name*, and **tacacs+** keywords are not supported.

Syntax Description

This command has no arguments or keywords.

Defaults

The auth-proxy posture code does not get security associations from the AAA server.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

After configuring access control lists (ACLs) and defining the IP Network Admission Control (NAC) rule, set the authentication-proxy authentication methods. You can also set the Extensible Authentication Protocol over UDP (EAPoUDP) authentication methods on a switch by using the **aaa authentication eou default group radius** global configuration command.

Examples

This example shows how to get security associations from the AAA server:

```
Switch(config)# aaa authorization auth-proxy default group radius
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
aaa authentication eou	Sets EAPoUDP authentication methods on the switch.
identity profile eapoudp	Creates an identity profile and enters EAPoUDP profile configuration mode. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
ip admission name eapoudp	Creates and configures IP NAC rules.
show ip admission	Displays information about NAC cached entries or the NAC configuration. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
show running-config	Displays the operating configuration. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

clear ip admission

To clear IP admission entries on the switch, use the **clear ip admission** privileged EXEC command.

clear ip admission {{**cache** | **watch-list**} {***** | *ip-address*}}

Syntax Description

cache	Delete the IP admission cache entries.
watch-list	Delete the IP admission watch-list entries.
*****	Delete all the cache entries.
ip-address	Delete the cache entry for the specified IP address.

Defaults

There is no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Examples

This example shows how to clear all IP admission cache entries:

```
Switch# clear ip admission *
```

You can verify your settings by entering the **show eou** or **show ip admission** privileged EXEC command.

Related Commands

Command	Description
ip admission name eapoudp	Creates and configures Network Admission Control (NAC) rules.
show eou	Displays information about the Extensible Authentication Protocol over UDP (EAPoUDP) configuration or session cache entries.
show ip admission	Displays information about NAC cached entries or the NAC configuration. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.

clear ip device tracking

To clear entries in the IP device tracking table on the switch, use the **clear ip device tracking** privileged EXEC command.

clear ip device tracking {**all** | **interface** *interface-id* | **ip** *ip-address* | **mac** *mac-address*}

Syntax Description

all	Delete all IP device tracking entries.
interface *interface-id*	Delete all IP device tracking entries on the specified interface.
ip *ip-address*	Delete all IP device tracking entries for the specified IP address.
mac *mac-address*	Delete all IP device tracking entries for the specified MAC address.

Defaults

There is no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

After you use the **clear ip device tracking** privileged EXEC command to clear IP device tracking entries, the switch sends ARP probes to the hosts that were removed. If a host is present, it responds to the ARP probe, and the switch add an IP device tracking entry for the host.

Examples

This example shows how to clear all entries in the IP device tracking table:

```
Switch# clear ip device tracking all
```

You can verify your settings by entering the **show ip device tracking** privileged EXEC command.

Related Commands

Command	Description
ip device tracking	Enables the IP device tracking table and configures the parameters for the IP device tracking table.
show ip device tracking	Displays information about the entries in the IP device tracking table.

debug eou

To enable debugging of Extensible Authentication Protocol over UDP (EAPoUDP), use the **debug eou** privileged EXEC command. Use the **no** form of this command to disable debugging.

debug eou {**all** | **eap** | **errors** | **events** | **obj-create** | **obj-destroy** | **obj-link** | **obj-unlink** | **packets** | **ratelimit** | **sm**}

no debug eou {**all** | **eap** | **errors** | **events** | **obj-create** | **obj-destroy** | **obj-unlink** | **packets** | **ratelimit** | **sm**}

Syntax Description

all	Display all EAPoUDP information.
eap	Display EAPoUDP packets.
errors	Display information about EAPoUDP packet errors.
events	Display information about EAPoUDP packet events.
obj-create	Display information about EAPoUDP sessions that are created.
obj-destroy	Display information about EAPoUDP sessions that are deleted.
obj-link	Display information about EAPoUDP sessions that are added to the hash table.
obj-unlink	Display information about EAPoUDP sessions that are removed from the hash table.
packets	Display EAPoUDP packet information.
ratelimit	Display EAPoUDP posture-validation information.
sm	Display EAPoUDP state-machine transitions.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXF 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

The **undebug eou** command is the same as the **no debug eou** command.

On Catalyst 3750 switches and EtherSwitch service modules, when you enable debugging, it is enabled only on the stack master. To enable debugging on a stack member, you can start a session from the stack master by using the **session** *switch-number* privileged EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You can also use the **remote command** *stack-member-number LINE* privileged EXEC command on the stack master switch to enable debugging on a member switch without first starting a session.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2 > System Management > Troubleshooting and Fault Management**.
show eou	Displays information about the EAPoUDP global configuration or session cache entries.

debug ip admission

To enable debugging of IP admission events, use the **debug ip admission** privileged EXEC command. Use the **no** form of this command to disable debugging.

debug ip admission {**api** | **dos** | **eapoudp** | **function-trace** | **object-creation** | **object-deletion** | **timers**}

no debug ip admission {**api** | **dos** | **eapoudp** | **function-trace** | **object-creation** | **object-deletion** | **timers**}

Syntax Description

api	Display IP admission application program interface (API) events.
dos	Display authentication proxy denial-of-service prevention information.
eapoudp	Display information about Extensible Authentication Protocol over UDP (EAPoUDP) posture-validation events.
function-trace	Display information about the authentication-proxy function trace.
object-creation	Display information about authentication proxy objects that are created.
object-deletion	Display information about authentication proxy objects that are deleted.
timers	Display information about authentication-proxy timer events.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

The **undebug ip admission** command is the same as the **no debug ip admission** command.

On Catalyst 3750 switches and EtherSwitch service modules, when you enable debugging, it is enabled only on the stack master. To enable debugging on a stack member, you can start a session from the stack master by using the **session** *switch-number* privileged EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command** *stack-member-number LINE* privileged EXEC command on the stack master switch to enable debugging on a member switch without first starting a session.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2 > System Management > Troubleshooting and Fault Management**.
show eou	Displays information about the EAPoUDP global configuration or session cache entries.
show ip admission	Displays information about Network Admission Control (NAC) cached entries or the NAC configuration. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.

debug ip device tracking

To enable debugging of Network Admission Control (NAC) tracking on switch ports, use the **debug ip device tracking** privileged EXEC command. Use the **no** form of this command to disable debugging.

debug ip device tracking {**all** | **events** | **obj-create** | **obj-destroy** | **redundancy**}

no debug ip device tracking {**all** | **events** | **obj-create** | **obj-destroy** | **redundancy**}

Syntax Description

all	Display all Extensible Authentication Protocol over UDP (EAPoUDP) information.
events	Display information about EAPoUDP packet events.
obj-create	Display information about EAPoUDP sessions that are created.
obj-destroy	Display information about EAPoUDP sessions that are deleted.
redundancy	Display information about the SSO status of standby supervisor engines in EAPoUDP sessions. **Note** This keyword is limited to Catalyst 4500 series switches.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

The **undebug ip device tracking** command is the same as the **no debug ip device tracking** command.

On Catalyst 3750 switches and EtherSwitch service modules, when you enable debugging, it is enabled only on the stack master. To enable debugging on a stack member, you can start a session from the stack master by using the **session** *switch-number* privileged EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command** *stack-member-number LINE* privileged EXEC command on the stack master switch to enable debugging on a member switch without first starting a session.

debug sw-ip-admission

To enable debugging of switch-specific NAC Layer2 IP processing, such as ARP and DHCP binding events, use the **debug sw-ip-admission** privileged EXEC command. Use the **no** form of this command to disable debugging.

debug sw-ip-admission [packet]

no debug sw-ip-admission [packet]

Syntax Description

packet	(Optional) Enables debugging of packets used to track NAC Layer2 IP hosts.

Syntax Description

This command has no keywords or arguments.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

The **undebug sw-ip-admission** command is the same as the **no debug sw-ip-admission** command.

On Catalyst 3750 switches and EtherSwitch service modules, when you enable debugging, it is enabled only on the stack master. To enable debugging on a stack member, you can start a session from the stack master by using the **session** *switch-number* privileged EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command** *stack-member-number LINE* privileged EXEC command on the stack master switch to enable debugging on a member switch without first starting a session.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2 > System Management > Troubleshooting and Fault Management**.

Command	Description
show eou	Displays information about the Extensible Authentication Protocol over UDP (EAPoUDP) global configuration or session cache entries.
show ip admission	Displays information about Network Admission Control (NAC) cached entries or the NAC configuration. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages** > New Features in Rele**ase 12.3(8)T > Network Admission Control**.

description

To enter a description of the identity policy, use the **description** identity-policy configuration mode command. To clear the description, use the **no** form of this command without the description.

description *line-of-description* [*line-of-description*] [*line-of-description*] ...

no description *line-of-description* [*line-of-description*] [*line-of-description*] ...

Syntax Description

line-of-description	Describe the identity policy.

Defaults

No description is configured.

Command Modes

Identity-policy configuration

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

You can enter more than one line of text describing the identity policy.

Examples

This example shows how to enter a description of the identity policy called *policy100*:

```
Switch(config)# identity policy policy100
Switch(config-identity-policy)# description Admin policy for the engineering group
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
description (identity-profile configuration)	Enters a description of an identity policy. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
show running-config	Displays the operating configuration. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

device

To manually authorize or reject a device, use the **device** identity-profile configuration mode command. Use the **no** form of this command to return to the default setting.

device {**authorize** | **not-authorize**} {**ip-address** *ip-address* | **mac-address** *mac-address* | **type cisco ip phone**} [**policy** *policy-name*]

no device {**authorize** | **not-authorize**} {**ip-address** *ip-address* | **mac-address** *mac-address* | **type cisco ip phone**} [**policy** *policy-name*]

Syntax Description

authorize	Configure an authorized device.
not-authorize	Configure an unauthorized device.
ip-address *ip-address*	Specify the IP address of the device.
mac-address *mac-address*	Specify the MAC address of the device.
type cisco ip phone	Specify that the device is a Cisco IP Phone.
policy *policy-name*	Specify a policy to apply to the device.

Defaults

Devices are not manually authorized or rejected.

Command Modes

Identity-profile configuration

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

You must create an identity profile by using the **identity profile** {**default** | **dot1x** | **eapoudp**} global configuration command before using the **device** identity-profile configuration command.

Examples

This example shows how to statically authorize a device with a MAC address of 1234.abcd.5678 and a policy called *policy1*:

```
Switch(config)# identity profile eapoudp
Switch(config-identity-prof)# device authorize mac-address 1234.abcd.4578 policy policy1
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
access-group (identity policy)	Specifies an access group to be applied to an identity policy. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
identity profile eapoudp	Creates an identity profile and enters Extensible Authentication Protocol over UDP (EAPoUDP) profile configuration mode. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
show running-config	Displays the operating configuration. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

eou initialize

To manually reset Extensible Authentication Protocol over UDP (EAPoUDP) state machines, use the **eou initialize** privileged EXEC command.

eou initialize {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface** *interface-id* | **ip** *ip-address* | **mac** *mac-address* | **posturetoken** *name*}

Syntax Description

all	Revalidate all EAPoUDP clients.
authentication	Revalidate with one of these EAPoUDP authentication types: • **clientless**—The endpoint system is not running CTA software. • **eap**—The authentication type is EAP. • **static**—The authentication type is statically configured.
interface *interface-id*	Revalidate the EAPoUDP client on the specified interface.
ip *ip-address*	Revalidate the EAPoUDP client at the specified IP address.
mac *mac-address*	Revalidate the EAPoUDP client at the specified MAC address.
posturetoken *name*	Revalidate the EAPoUDP client with the specified posture token.

Defaults

There is no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

When you enter the **eou initialize** privileged EXEC command, configured EAPoUDP sessions are reset.

Examples

This example shows how to initiate the reset of all EAPoUDP associations:

```
Switch# eou initialize
```

You can verify your settings by entering the **show eou** privileged EXEC command.

Related Commands

Command	Description
eou revalidate (global and interface configuration)	Enables revalidation of the EAPoUDP associations on the switch or on a specific interface.
eou revalidate (privileged EXEC)	Manually initiates revalidation of EAPoUDP associations.
show eou	Displays information about the EAPoUDP configuration or session cache entries.

eou max-retry (global and interface configuration)

To specify the number of Extensible Authentication Protocol over UDP (EAPoUDP) revalidation attempts, use the **eou max-retry** global configuration and interface configuration commands. Use the **no** form of this command to return to the default setting.

eou max-retry *number*

no eou max-retry

Syntax Description

number	Number of times the switch tries to revalidate EAPoUDP associations.The range is from 1 to 3.

Defaults

The default number of revalidation attempts is 3.

Command Modes

Global configuration and interface configuration

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

You can configure the number of revalidation attempts by using the **eou max-retry** *number* global configuration command. You can also use the **eou max-retry** *number* interface configuration command to configure the among of revalidation attempts for a specific interface.

Examples

This example shows how to specify the number of revalidation attempts as 2 on a switch-wide basis:

```
Switch(config)# eou max-retry 2
```

This example shows how to specify the number of revalidation attempts as 1 on an interface:

```
Switch(config-if)# eou max-retry 1
```

You can verify your settings by entering the **show eou** privileged EXEC command.

Related Commands

Command	Description
show eou	Displays information about the EAPoUDP configuration or session cache entries.

eou ratelimit

To specify the number of simultaneous Extensible Authentication Protocol over UDP (EAPoUDP) posture validations, use the **eou ratelimit** global configuration command. Use the **no** form of this command to return to the default setting.

eou ratelimit *number*

no eou ratelimit

Syntax Description

number	Number of clients that can be simultaneously validated. The range is from 0 to 200.

Defaults

The default is 20 clients.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

If you enter the **eou rate-limit 0** command, the rate-limiting feature is disabled.

If the number of clients that can be simultaneously validated is 100 and the switch is connected to 101 clients, the posture validation of the last client (client 101) does not occur until another client ends an EAPoUDP session.

Use the **eou default** or the **no eou ratelimit** global configuration command to return to the default setting.

Examples

This example shows how to specify that the number of clients that can be simultaneously validated is 40:

```
Switch(config)# eou ratelimit 40
```

This example shows how to return to the default setting of 20 clients:

```
Switch(config-if)# eou default
```

You can verify your settings by entering the **show eou** privileged EXEC command.

Related Commands

Command	Description
eou default	Resets the global EAPoUDP parameters to the default settings. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
show eou	Displays information about the EAPoUDP configuration or session cache entries.

eou revalidate (global and interface configuration)

To enable revalidation of the Extensible Authentication Protocol over UDP (EAPoUDP) associations, use the **eou revalidate** global configuration and interface configuration commands.

eou revalidate

Syntax Description

This command has no keywords or arguments.

Defaults

There is no default setting.

Command Modes

Global configuration and interface configuration

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

You can enable revalidation of the EAPoUDP associations on the switch by using the **eou revalidate** global configuration command. You can also enable revalidation of the EAPoUDP associations on an interface by using the **eou revalidate** interface configuration command.

The revalidation timer value is based on Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute[29]) in the Access-Accept message from the Cisco Secure ACS running AAA. If the switch gets the Session-Timeout value, this value overrides the revalidation timer value on the switch.

If the revalidation timer expires, the switch action depends on the value of the Termination-Action attribute:

- If the value of the Termination-Action RADIUS attribute is the default, the session ends until the switch revalidates it.
- If the switch gets a value for the Termination-Action attribute other than the default, the EAPoUDP session and the current access policy remain in effect during posture revalidation.
- If the value of the Termination-Action attribute is *RADIUS*, the switch revalidates the client.
- If the packet from the server does not include the Termination-Action attribute, the EAPoUDP session ends, and the switch re-initiates posture validation.

Examples

This example shows how to globally initiate revalidation of the EAPoUDP associations:

```
Switch(config)# eou revalidate
```

This example shows how to initiate revalidation of the EAPoUDP associations on an interface:

```
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# eou revalidate
```

You can verify your settings by entering the **show eou** privileged EXEC command.

Related Commands

Command	Description
eou initialize	Manually resets EAPoUDP state machines.
eou allow (global configuration and interface configuration)	Allows additional EAPoUDP options. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
eou logging	Enables logging of EAPoUDP system events. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
eou port	Sets the UDP port for EAPoUDP. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
eou revalidate (privileged EXEC)	Manually initiates revalidation of EAPoUDP associations.
show eou	Displays information about the EAPoUDP configuration or session cache entries.

eou revalidate (privileged EXEC)

To manually initiate revalidation of Extensible Authentication Protocol over UDP (EAPoUDP) association, use the **eou revalidate** privileged EXEC command.

eou revalidate {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface** *interface-id* | **ip** *ip-address* | **mac** *mac-address* | **posturetoken** *name*}

Syntax Description

all	Revalidate all EAPoUDP clients.
authentication	Revalidate with one of these EAPoUDP authentication types: • **clientless**—The endpoint system is not running CTA software. • **eap**—The authentication type is EAP. • **static**—The authentication type is statically configured.
interface *interface-id*	Revalidate the EAPoUDP client on the specified interface.
ip *ip-address*	Revalidate the EAPoUDP client at the specified IP address.
mac *mac-address*	Revalidate the EAPoUDP client at the specified MAC address.
posturetoken *name*	Revalidate the EAPoUDP client with the specified posture token.

Defaults

There is no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

To manually initiate revalidation of the EAPoUDP associations on the switch, use the **eou revalidate** privileged EXEC command.

Examples

This example shows how to initiate the revalidation of all EAPoUDP clients:

```
Switch# eou revalidate all
```

This example shows how to initiate the revalidation of EAPoUDP clients on a specific interface

```
Switch# eou revalidate interface gigabitethernet 1/0/2
```

You can verify your settings by entering the **show eou** privileged EXEC command.

Related Commands

Command	Description
eou initialize	Manually resets EAPoUDP state machines.
eou revalidate (**global and interface configuration**)	Enables revalidation of the EAPoUDP associations on the switch or on a specific interface.
show eou	Displays information about the EAPoUDP configuration or session cache entries.

eou timeout (global and interface configuration)

To set the Extensible Authentication Protocol over UDP (EAPoUDP) timers, use the **eou timeout** global configuration and interface configuration commands. Use the **no** form of this command to set the default values.

eou timeout {**aaa** *seconds* | **hold-period** *seconds* | **retransmit** *seconds* | **revalidation** *seconds* | **status-query** *seconds*}

no eou timeout {**aaa** | **hold-period** | **retransmit** | **revalidation** | **status-query**}

Syntax Description

aaa *seconds*	Set the duration (in seconds) that the switch waits for retransmission of packets by the switch to the authentication, authorization, and accounting (AAA) server. The range is from 1 to 60.
hold-period *seconds*	Set the duration (in seconds) that the switch waits to re-authenticate the host after a failed authentication attempt. The range is from 60 to 86400 seconds.
retransmit *seconds*	Set the duration (in seconds) that the switch waits for a response from the client before resending a request for the antivirus condition. The range is from 1 to 60.
revalidation *seconds*	Set the duration (in seconds) that a Network Admission Control (NAC) policy is applicable to a client that used EAPoUDP messages during posture validation. The range is from 5 to 86400.
status-query *seconds*	Set the duration (in seconds) that the switch waits before verifying that the previously validated client is present and that its posture has not changed. The range is from 10 to 1800 seconds.

Defaults

The default AAA time is 60 seconds (1 minute).

The default hold time is 180 seconds (3 minutes).

The default retransmission time is 3 seconds.

The default revalidation time is 600 seconds (10 minutes).

The default status-query time is 300 seconds (5 minutes).

Command Modes

Global configuration and interface configuration

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

You can globally configure the EAPoUDP timers on a switch by entering the **eou timeout** global configuration command. You can also configure the EAPoUDP timers on a specific interface by entering the **eou timeout** interface configuration command.

For more information about the EAPoUDP timers, see the "NAC Timers" section on page 15.

Examples

This example shows how to set the retransmission timer to 45 seconds on a switch-wide basis:

```
Switch(config)# eou timeout retransmit 45
```

This example shows how to set the revalidation timer to 800 seconds on an interface:

```
Switch(config-if)# eou timeout revalidation 800
```

You can verify your settings by entering the **show eou** privileged EXEC command.

Related Commands

Command	Description
eou default	Resets the global EAPoUDP parameters to the default settings. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
eou allow (global configuration and interface configuration)	Allows additional EAPoUDP options. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
eou logging	Enables logging of EAPoUDP system events. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
eou port	Sets the UDP port for EAPoUDP. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
show eou	Displays information about the EAPoUDP configuration or session cache entries.

identity policy

To create an identity policy and enter Extensible Authentication Protocol over UDP (EAPoUDP) policy configuration mode, use the **identity policy** global configuration mode. Use the **no** form of this command to remove the policy.

identity policy *policy-name*

no identity policy *policy-name*

Syntax Description

policy-name	Specify the name of an EAPoUDP policy.

Defaults

No EAPoUDP policies are configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

After a device is manually authenticated based on the IP address, MAC address or based on the device type, you can define the policy to be applied to the device by using the **identity policy** *policy-name* global configuration mode. For more information, see the "Configuring Identity Profiles and Policies" section in the "Configuring Network Admission Control" chapter.

Examples

This example shows how to create an identity policy and enter EAPoUDP policy configuration mode:

```
Switch(config)# identity policy policy11
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
access-group (identity policy)	Specifies an access group to be applied to an identity policy. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
identity profile eapoudp	Creates an identity profile and enters EAPoUDP profile configuration mode. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
show running-config	Displays the operating configuration. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

ip admission name eapoudp

To create an IP Network Admission Control (NAC) rule, use the **ip admission name eapoudp** global configuration command. Use the **no** form of this command to remove the rule.

ip admission name *rule-name* **eapoudp**

no ip admission name *rule-name* **eapoudp**

Syntax Description

rule-name	Specify the name of the IP NAC rule.

Defaults

No IP NAC rules are configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

The IP NAC rule defines how you apply NAC.

To apply the IP NAC rule on an access port on an edge switch, use the **ip admission** *admission-name* interface configuration command.

Examples

This example shows how to create an IP NAC rule called *rule11*:

```
Switch(config)# ip admission name rule11 eapoudp
```

You can verify your settings by entering the **show ip admission** privileged EXEC command.

Related Commands

Command	Description
clear eou	Clears all NAC client device entries on the switch or on the specified interface. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
ip admission *admission-name* (interface configuration)	Creates a NAC rule to be applied to the specified interface. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.

Command	Description
show eou	Displays information about the Extensible Authentication Protocol over UDP (EAPoUDP) global configuration or session cache entries.
show ip admission	Displays information about Network Admission Control (NAC) cached entries or the NAC configuration. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.

ip admission name eapoudp bypass

To enable and configure the Extensible Authentication Protocol over UDP (EAPoUDP or EoU) bypass feature, use the **ip admission name eapoudp bypass** global configuration command. Use the **no** form of this command to remove the rule.

ip admission name *rule-name* **eapoudp bypass** {**auth-cache-list** *cache-time* [**list** {*acl-name* | *acl-number*}] | **list** {*access-list-name* | *access-list-number*}}

no ip admission name *rule-name* **eapoudp**

Syntax Description

rule-name	Specify the name of the IP Network Admission Control (NAC) rule.
auth-cache-list *cache-time*	Set the time until the authorization cache entries expire. The range is 1 to 135791 minutes. The default is TBD.
list {*acl-name* | *acl-number*}	Specify the name or number of a standard or extended access control list (ACL) that is applied to the authentication proxy. These keywords are optional if they are entered after the **auth-cache-time cache-time** keywords. **Note** This option is not supported on the Catalyst 6500 series switch and the Catalyst 7600 series router.

Defaults

EoU bypass is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

When EoU bypass is enabled, the switch does not contact the host to request the antivirus condition. Instead, the switch sends a request to the Cisco Secure Access Control Server (ACS) that includes the IP address, MAC address, service type, and EAPoUDP session ID of the host. The authentication server makes the access control decision and sends the policy to the switch.

You can associate the specified rule with an ACL to control which hosts are authenticated with NAC. If you do not configure a standard ACL, the switch uses the NAC rule to intercept IP traffic from all hosts connected to NAC-enabled ports.

You can use the **auth-cache-time** *cache-time* keywords to specify the time at which cache entries expire and the host must be revalidated.

You can use the **list** {*acl-name* | *acl-number*} keywords to specify a named or numbered ACL that is applied to the NAC rule. If IP connections are initiated by hosts in the ACL, the initial connection requests are intercepted by the NAC feature.

Examples

This example shows how to enable EoU bypass and associate it with a numbered ACL. The switch uses NAC to validate the antivirus state of IP traffic that matches the ACL instead of permitting packets that match the ACL.

```
Switch(config)# ip admission name rule11 eapoudp bypass list 101
```

This example shows how to enable EoU bypass and specify the cache entry timer:

```
Switch(config)# ip admission name rule11 eapoudp bypass auth-cache-time 30
```

This example shows how to disable EoU bypass:

```
Switch(config)# ip admission name rule11 eapoudp bypass
```

You can verify your settings by entering the **show ip admission** privileged EXEC command.

Related Commands

Command	Description
clear eou	Clears all NAC client device entries on the switch or on the specified interface. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
show eou	Displays information about the EAPoUDP global configuration or session cache entries.
show ip admission	Displays information about NAC cached entries or the NAC configuration. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.

ip device tracking

To enable the IP device tracking feature and to configure the IP device tracking table parameters, use the **ip device tracking** global configuration command. Use the **no** form of this command to disable the feature and to return to the default settings.

ip device tracking [**probe** {**count** *count* | **interval** *interval*}]

no ip device tracking [**probe** {**count** | **interval**}]

Syntax Description

probe	(Optional) Configure the parameters for the IP device tracking table.
count *count*	Set the number of times that the switch sends the ARP probe for an entry before removing an entry from the IP device tracking table. The range is from 1 to 5.
interval *interval*	Set the number of seconds that the switch waits before resending the ARP probe. The range is from 30 to 300 seconds.

Defaults

IP device tracking is disabled.

The default number of times that the switch sends the ARP probe for an entry is 3.

The default number of seconds that the switch waits before resending the ARP probe is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

For information about the IP device tracking feature and the IP device tracking table, see the "NAC Timers" section on page 15.

This example shows how to enable the IP device tracking:

```
Switch(config)# ip device tracking
```

This example shows how to set the number of times that the switch sends ARP probes to 4:

```
Switch(config)# ip device tracking probe count 4
```

You can verify your settings by entering the **show ip device tracking** privileged EXEC command.

Related Commands

Command	Description
clear ip device tracking	Clears entries in the IP device tracking table on the switch.
show ip device tracking	Displays information about the entries in the IP device tracking table.

mls rate-limit layer2 ip-admission

Note This command is specific to the Catalyst 6500 series switch and the Catalyst 7600 series router.

To rate limit the IP admission Layer 2 traffic (redirected to the CPU) with the hardware rate limiter, use the **mls rate-limit layer2 ip ip-admission** global configuration command. Use the **no** form of this command to disable the feature.

mls rate-limit layer2 ip ip-admission *pps* [*burst*]

no mls rate-limit layer2 ip ip-admission

Syntax Description

pps	Sets the rate limiting packets per second. The range is from 10 to 1000000.
burst	(Optional) Sets the maximum allowed packets in a burst. The range is from 1 to 255. If this keyword is not set, the burst value is set to 10.

Defaults

Rate limiting is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

The NAC rate limiter is off by default; all the packets matching the scenario are sent to the RP.

Examples

This example shows how to set the packet rate to 1000 packets per second and the burst rate to a maximum of 100 packets:

```
Switch(config)# mls rate-limit layer2 ip-admission 1000 100
```

radius-server attribute 8

To configure the switch to send Framed-IP-Address RADIUS attribute (Attribute[8]) in access-request or accounting-request packets, use the **radius-server attribute 8** global configuration mode. Use the **no** form of this command to configure the switch to not send the RADIUS attribute (Attribute[8]).

radius-server attribute 8 include-in-access-req

no radius-server attribute 8 include-in-access-req

Syntax Description

This command has no keywords or arguments.

Defaults

The switch does not send the Framed-IP-Address RADIUS attribute (Attribute[8]) in RADIUS access-request or accounting-request packets.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

When the switch validates the posture of nonresponsive hosts, also referred to as Network Admission Control (NAC) agentless hosts, you must use the **radius-server attribute 8 include-in-access-req** global configuration command.

When you enter the **radius-server attribute 8 include-in-access-req** global configuration command, the switch sends the Framed-IP-Address attribute in RADIUS access-request or accounting-request packets.

Examples

This example shows how to configure the switch to send the RADIUS attribute (Attribute[8]) in access-request or accounting-request packets:

```
Switch(config)# radius-server attribute 8 include-in-access-req
```

You can verify your settings by entering the **show eou** privileged EXEC command.

Related Commands

Command	Description
show eou	Displays information about the Extensible Authentication Protocol over UDP (EAPoUDP) configuration or session cache entries.

redirect

To specify the URL to which the switch redirects clients, use the **redirect** configuration mode. Use the **no** form of this command to remove the URL.

redirect url *url* [**match** *acl-name*]

no redirect url *url* [**match**]

Note This command is *not* supported on Catalyst 3750, 3560, 2970, 2960 switches and on Cisco EtherSwitch service modules.

Syntax Description

url	Specify the URL to which clients are redirected.
match *acl-name*	Specify that traffic matching the specified access control list (ACL) is redirected to the URL.

Defaults

No URLs or ACLs are configured.

Command Modes

Identity-policy configuration

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

When you specify a redirect URL, an identity policy must be associated with an Extensible Authentication protocol over UDP (EAPoUDP) identity profile.

Examples

This example shows how to create an identity policy called *policy100* and enter EAPoUDP policy configuration mode:

```
Switch(config)# identity policy policy100
Switch(config-identity-policy)# redirect tftp:172.20.10.30/nac_authen.tar match
authen_policy
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
identity profile eapoudp	Creates an identity profile and enters EAPoUDP profile configuration mode. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
show running-config	Displays the operating configuration. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

show eou

To display information about the Extensible Authentication Protocol over UDP (EAPoUDP) configuration or session cache entries, use the **show eou** privileged EXEC command.

show eou {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface** *interface-id* | **ip** *ip-address* | **mac** *mac-address* | **posturetoken** *name*} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

all	Display EAPoUDP information about all clients.
authentication	Display information about one of these EAPoUDP authentication types: • **clientless**—The endpoint system is not running CTA software. • **eap**—The authentication type is EAP. • **static**—The authentication type is statically configured.
interface *interface-id*	Display EAPoUDP information for the specified interface.
ip *ip-address*	Display EAPoUDP information for the specified IP address.
mac *mac-address*	Display EAPoUDP information for the specified MAC address.
posturetoken *name*	Display EAPoUDP information for the specified posture token.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

If you do not specify a port, global parameters and a summary appear. If you specify a port, details for that port appear.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show eou** privileged EXEC command:

```
Switch# show eou
Global EAPoUDP Configuration
----------------------------
EAPoUDP Version     = 1
EAPoUDP Port        = 0x5566
Clientless Hosts    = Disabled
```

```
IP Station ID       = Disabled
Revalidation        = Enabled
Revalidation Period = 36000 Seconds
ReTransmit Period   = 3 Seconds
StatusQuery Period  = 300 Seconds
Hold Period         = 180 Seconds
AAA Timeout         = 60 Seconds
Max Retries         = 3
EAP Rate Limit      = 20
EAPoUDP Logging     = Disabled

Interface Specific EAPoUDP Configurations
-----------------------------------------
Interface GigabitEthernet1/0/1
  No interface specific configuration
```

Table 4 describes the fields in the display:

Table 4 show eou Field Descriptions

Field	Description
EAPoUDP Version	Displays the EAPoUDP protocol version.
EAPoUDP Port	Displays the EAPoUDP port number.
Clientless Hosts	Displays the status of the clientless hosts (enabled or disabled).
IP Station ID	Displays whether the IP address is allowed in the AAA[1] station-id field. By default, this field is disabled.
Revalidation	Displays the revalidation status.
Revalidation Period	Displays the host revalidation interval.
ReTransmit Period	Displays the EAPoUDP packet retransmission interval.
StatusQuery Period	Displays the EAPoUDP status query interval for validated hosts.
Hold Period	Displays the time that the switch waits after NAC authentication fails.
AAA Timeout	Displays the AAA timeout period.
Max Retries	Displays the allowed number of transmissions.
EAPoUDP Logging	Displays the logging status.

1. AAA = authentication, authorization, and accounting

Related Commands

Command	Description
eou default	Resets the global EAPoUDP parameters to the default settings. For syntax information, select **Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control**.
eou max-retry (global and interface configuration)	Specifies the number of EAPoUDP revalidation attempts.
eou ratelimit	Specifies the number of simultaneous EAPoUDP posture validations.
eou timeout	Sets the EAPoUDP timers.

show ip access-lists interface

To display the LP IP host policies, use the **show ip access-lists** privileged EXEC command.

show ip access-lists interface *interface*

Syntax Description

interface	Specify the interface to display.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Examples

This is an example of output from the **show ip device tracking all** privileged EXEC command:

```
Switch# show ip access-lists GigabitEthernet3/4
IP Admission access control entires (Inbound)
     permit ip host 102.50.1.54 any
```

show ip device tracking

To display information about the entries in the IP device tracking table, use the **show ip device tracking** privileged EXEC command.

show ip device tracking {**all** | **interface** *interface-id* | **ip** *ip-address* | **mac** *mac-address*} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

all	Display all IP device tracking table entries.
interface *interface-id*	Display IP device tracking table entries for the specified interface.
ip *ip-address*	Display IP device tracking table entries for the specified IP address.
mac *mac-address*	Display IP device tracking table entries for the specified MAC address.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show ip device tracking all** privileged EXEC command:

```
Switch# show ip device tracking all
-----------------------------------------------------------------
  IP Address    MAC Address     Interface              STATE
-----------------------------------------------------------------
  1.1.1.1       cf2a.220a.12f4  GigabitEthernet1/0/1   ACTIVE
  1.2.1.1       df4a.1235.ef1a  GigabitEthernet1/0/2   INACTIVE
```

Related Commands

Command	Description
ip device tracking	Enables the IP device tracking table and to configure the IP device tracking table parameters.

Message and Recovery Procedures

This section contains the following topics:

AP Messages

This section contains the Authentication Proxy messages for Network Admission Control (NAC) Layer 2 IP validation.

- The Catalyst 6500 and 4500 series switches and the Catalyst 7600 series router support all messages in this section.
- The Catalyst 3750, 3560, 3550, 2970, 2960, 2955, 2950, and 2940 switches support only the `AP-4-POLICY_URL_REDIRECT` and the `AP-6-POSTURE_POLICY` messages.

Error Message `AP-4-AUTH_PROXY_NOMEM: Sufficient memory was not available to [chars].`

Explanation This message means that the system memory is not sufficient to perform the specified operation. [chars] is the operation.

Recommended Action Reduce other system activity to ease memory demands. You can also allocate more memory resources.

Error Message `AP-4-POLICY_URL_REDIRECT: Failed to locate match access control list [chars] for host [inet].`

Explanation This message means that the switch could not redirect the HTTP or HTTPS traffic from the host to the redirect URL. The url-redirect Attribute-Value (AV) pair consists of the redirect URL and an access control list (ACL) called *match-all t*hat specifies the HTTP and HTTPS traffic to be redirected. If the ACL is not configured or does not specify the traffic to be redirected, the switch does not redirect requests from the hosts. [inet] is the host IP address.

Recommended Action Configure and apply an ACL on the switch interface to which the host is connected, and ensure that the url-redirect AV pair consists of the redirect URL and the ACL.

Error Message `AP-4-POSTURE_EXCEED_MAX_INIT: Exceeded maximum limit [dec] on entries in authentication proxy.`

Explanation This message means that the number of entries in the authentication proxy posture cache which are in *INIT* state exceeds the limit. This happens when the switch has an authentication proxy configured for posture validation and the switch receives requests from a large number of unique hosts with source IP addresses. This could be a denial-of-service attack. When the number of entries in the posture cache count is below the maximum, new cache entries can be created. [dec] is the number of entries allowed in the authentication proxy cache.

Recommended Action No action required. When the number of entries in the posture cache count is below the maximum, new cache entries can be created.

Error Message `AP-6-POSTURE_DOWNLOAD_ACL: Send AAA request to download [chars] named access control list.`

Explanation This message means that the switch sent a request to the authentication, authorization, and accounting (AAA) server to get the specified ACL. [chars] is the name or number of the ACL.

Recommended Action No action is required.

Error Message `AP-6-POSTURE_POLICY: [chars] [chars] [chars] policy for host [inet].`

Explanation This message means that the specified policy is enforced or removed for the specified host. The policy is either an access control list (ACL) or a redirect URL. The first and second [chars] are the actions that the switch takes to enforce or remove the policy, and the third [chars] is the ACL or redirect URL.

Recommended Action No action is required.

Error Message `AP-6-POSTURE_START_VALIDATION: IP=[inet] | Interface=[chars].`

Explanation This message means that the switch created an entry for the host in the authentication proxy posture cache and initiated the posture validation process. [inet] is the host IP address, and [chars] is the switch interface to which the host is connected.

Recommended Action No action is required.

Error Message `AP-6-POSTURE_STATE_CHANGE: IP=[inet]|STATE=[chars].`

Explanation This message means that the posture validation state of the specified host in the authentication proxy posture validation cache changed. [inet] is the host IP address. [chars] is the posture validation state.

Recommended Action No action is required.

EOU Messages

These are the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP or EoU) messages for Network Admission Control (NAC) Layer 2 IP validation.

Note The Catalyst 6500, 4500, 3750, 3560, 3550, 2970, 2960, 2955, 2950, and 2940 switches, as well as the Catalyst 7600 router, support all the messages in this section.

Error Message `EOU-2-PROCESS_ERR: Router could not create a EAPoUDP process.`

Explanation This message means the switch could not create an EAPoUDP session.

Recommended Action Reload the device.

Error Message `EOU-4-BAD_PKT: IP=[inet]| Bad Packet=[chars].`

Explanation This message means that the router received an invalid EAPoUDP packet from the specified host. [inet] is the host IP address, and [chars] is the information about the bad packet.

Recommended Action Check the NAC Layer 2 IP configuration on the host.

Error Message `EOU-4-MSG_ERR:` Unknown message event received.

Explanation This message means that the EAPoUDP validation process received an unknown message event.

Recommended Action If this message recurs, reload the device.

Error Message `EOU-4-PROCESS_STOP: PROCESS=[chars]| ACTION=[chars].`

Explanation This message means that the specified process stopped. The first [chars] is the process, and the second [chars] is the action taken on the process.

Recommended Action Reload the device.

Error Message `EOU-4-SOCKET: EAPoUDP socket binding fails for PORT=[hex]. Check if the interface has valid IP address.`

Explanation This message means that the switch could not bind the port to a valid IP address. [hex] is the port MAC address.

Recommended Action Configure a valid IP address on the switch port.

Error Message `EOU-4-UNKN_EVENT_ERR: UNKNOWN Event for HOST=%i| Event=%d.`

Explanation This message means that the switch received an unknown EAPoUDP event.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `EOU-4-UNKN_PROCESS_ERR: An unknown operational error occurred.`

Explanation This message means that the EAPoUDP process cannot operate due to an internal system error.

Recommended Action Reload the device.

Error Message `EOU-4-UNKN_TIMER_ERR: An unknown Timer operational error occurred.`

Explanation This message means that the EAPoUDP validation process cannot operate due to an internal system error.

Recommended Action Reload the device.

Error Message `EOU-4-VALIDATION: Unable to initiate validation for HOST=[inet]| INTERFACE=[chars].`

Explanation This message means that the switch could not start posture validation for the specified host.

Recommended Action This is not an action: This is probably due to a failure in binding the EAPoUDP port.

Error Message `EOU-4-VERSION_MISMATCH: HOST=[inet] | Version=[dec].`

Explanation This message means the EAPoUDP versions of the specified host and switch are incompatible. [inet] is the host IP address, and [dec] is the EAPoUDP version of the host.

Recommended Action Check EAPoUDP versions on the devices.

Error Message `EOU-5-RESPONSE_FAILS: Received an EAP failure response from AAA for host=[inet].`

Explanation This message means that the switch received an EAP-failure response from the authentication, authorization, and accounting (AAA) server that the host antivirus condition could not be validated.

Recommended Action No action required.

Error Message `EOU-6-AUTHSTATUS: [chars]|[inet].`

Explanation This message means that the authentication status for the specified host is Success or Failure. [chars] is the status, and [inet] is the host IP address.

Recommended Action No action is required.

Error Message `EOU-6-AUTHTYPE: IP=[inet]| AuthType=[chars].`

Explanation This message means that the authentication type for the specified host is [chars]. [inet] is the host IP address.

Recommended Action No action is required.

Error Message `EOU-6-CTA: IP=[inet]| CiscoTrustAgent=[chars].`

Explanation This message means that the CTA was detected for the specified host. [inet] is the host IP address, and [chars] is the CTA name.

Recommended Action If the CTA was not detected, install it on the host.

Error Message `EOU-6-IDENTITY_MATCH: IP=[inet]| PROFILE=EAPoUDP| POLICYNAME=[chars].`

Explanation This message means that the switch found the specified host with an EAPoUDP identity profile. If the specified policy is enforced, the posture of switch is not validated. [inet] is the host IP address, and [chars] is the policy name.

Recommended Action If you want the posture host to be validated, remove the host entry from the EAPoUDP identity profile.

Error Message `EOU-6-POLICY: IP=[inet]| [chars]=[chars].`

Explanation This message means that the switch received an access policy from the AAA server to enforce against the specified host.

Recommended Action No action is required.

Error Message `EOU-6-POSTURE: IP=[inet]| HOST=[chars]| Interface=[chars].`

Explanation This message means the posture validation status for the specified host changed. [inet] is the host IP address, the first [chars] is the hostname, and the second [chars] is the interface.

Recommended Action No action is required.

Error Message `EOU-6-SESSION: IP=[inet]| HOST=[chars]| Interface=[chars].`

Explanation This message means that an entry was created or deleted for the host on the specified interface. [inet] is the host IP address, the first [chars] is an action, such as *DETECTED* or *REMOVED*, and the second [chars] is the interface.

Recommended Action No action is required.

Error Message `EOU-6-SQ: IP=[inet]| STATUSQUERY|[chars].`

Explanation This message means that the result of the status query for the specified host failed or is invalid. [inet] is the host IP address, and [chars] is the result of the status query (failure, invalid, or no response).

Recommended Action No action is required.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Network Admission Control Software Configuration Guide