CHAPTER 51

Configuring Network Admission Control

This chapter describes how to configure Network Admission Control (NAC) in Cisco IOS Software Release 12.2SX.

Note For complete syntax and usage information for the commands used in this chapter, see these publications:

- Cisco IOS Software Releases 12.2SX Command References, at this URL:
  http://www.cisco.com/en/US/docs/ios/mcl/122sx_mcl.html
- The *Network Admission Control* feature module at this URL:
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_8/gt_nac.htm
- The *Cisco IOS Security Command Reference*, Release 12.3 at this URL:
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/secur_r/

This chapter contains these sections:

Understanding NAC

These sections describe NAC:

NAC Overview

NAC is part of the Cisco Self-Defending Network Initiative that helps you identify, prevent, and adapt to security threats in your network. Because of the increased threat and impact of worms and viruses to networked businesses, NAC allows you to check and validate the antivirus status of endpoints or clients before granting network access.

Cisco IOS Software Release 12.2SX supports NAC Layer 2 IP validation and, with Release 12.2(33)SXH and later releases, NAC Layer 3 IP validation.

NAC Layer 2 IP (also known as LAN Port IP) operates on Layer 2 ports on edge switches. NAC Layer 2 IP validation has different methods for validation initiation, message exchange, and policy enforcement from the NAC Layer 2 IEEE 802.1x. LAN Port IP does not require IEEE 802.1x support on the host PCs. For additional information about IEEE 802.1x, see Chapter 52, "Configuring IEEE 802.1X Port-Based Authentication."

For a complete list of devices that support NAC, see the *Release Notes for Network Admission Control*, Release 2.1, at this URL:

http://www.cisco.com/en/US/docs/security/nac/2.1/release_notes/NAC21RN.html

NAC Layer 3 IP (also known as NAC Gateway IP) operates on Layer 3 interfaces on distribution layer switches. An advantage of NAC Layer 3 IP is that access layer switches do not require any changes to use the NAC feature.

Note The NAC feature applies access controls only to IPv4 traffic. NAC does not restrict Layer 2-bridged traffic.

NAC provides *posture validation* for routed traffic. Posture validation reduces the exposure of a virus to the network. This feature allows network access based on the antivirus credentials of the network device that is requesting network access. These credentials may be antivirus software, a virus definitions file, or a particular virus scan engine version. Based on the antivirus credentials of the host, the requesting device is allowed access to the network or is restricted from network access.

If the client host fails the credential validation, then partial access to the network can be allowed by using the *remediation* feature. The remediation process redirects HTTP traffic from the client host to a web page URL that provides access to the latest antivirus files. The URL used by the remediation process resolves to a remediation server address defined as a part of the network access policy. The remediation server is where the latest antivirus files are located. These antivirus files can be downloaded or upgraded from this location.

NAC Device Roles

The devices in the network have specific roles when you use NAC as shown in Figure 51-1.

Figure 51-1 Posture Validation Devices

The following devices that support NAC on the network perform these roles:

- Endpoint system or client—This is a device (host) on the network such as a PC, workstation, or server. The host, which is running the Cisco Trust Agent (CTA) software, requests access to the LAN and switch services and responds to requests from the switch. This endpoint system is a potential source of virus infections, and its antivirus status needs to be validated before the host is granted network access.
  - For NAC Layer 2 IP, the device is connected to an access port through a direct connection, an IP phone, or a wireless access point.
  - For NAC Layer 3 IP, the device is one or more Layer 3 hops away from the switch.

  The CTA software is also referred to as the *posture agent* or the *antivirus client*.
- Switch—This is a network access device, which provides validation services and policy enforcement.
  - Edge switch—This is the network access device that provides NAC Layer 2 IP validation services and policy enforcement at the network edge and controls the physical access to the network based on the access policy of the client.
  - Distribution switch—This is the NAC gateway, which provides validation services and policy enforcement at the Layer 3 network edge and controls access to the Layer 3 network based on the access policy of the client.

  The encapsulation information in the EAP messages can be based on the User Datagram Protocol (UDP). When using UDP, the switch uses EAP over UDP (EAPoUDP) frames, which are also referred to as EoU frames.

  The switch relays Extensible Authentication Protocol (EAP) messages between the endpoints and the authentication server.

- Authentication server—This device performs the actual validation of the client. The authentication server validates the antivirus status of the client, determines the access policy, and notifies the switch whether the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the EAP message exchange between the switch and authentication server is transparent to the switch.

  The switch supports the Cisco Secure Access Control Server (ACS) Version 4.0 or later with RADIUS, authentication, authorization, and accounting (AAA), and EAP extensions.

  The authentication server is also referred to as the *posture server*.

AAA Down Policy

The AAA down policy is a method of allowing a host to remain connected to the network if the AAA server is not available. Typical deployments of NAC use Cisco Secure ACS to validate the client posture and to pass policies back to the Network Access Device (NAD). If the AAA server cannot be reached 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 policy 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 again available, a user can be revalidated, and the user's 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.

When the AAA policy is applied, the session state is maintained as AAA DOWN.

NAC IP Validation

The following sections describe NAC IP validation:

NAC Layer 2 IP Validation

You can use NAC Layer 2 IP on the access port of an edge switch to which an endpoint system or client is connected. The device (host or client) can be a PC, a workstation, or a server that is connected to the access port through a direct connection, an IP phone, or a wireless access point, as shown in Figure 51-2.

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

Figure 51-2 Network Using NAC Layer 2 IP

NAC Layer 2 IP supports the posture validation of multiple hosts on the same Layer 2 port, as shown in Figure 51-2.

When you enable NAC Layer 2 IP validation on a Layer 2 port to which hosts are connected, the switch can use DHCP snooping and Address Resolution Protocol (ARP) snooping to identify connected hosts. The switch initiates posture validation after receiving an ARP packet or creating a DHCP snooping binding entry. When you enable NAC Layer 2 IP validation, ARP snooping is the default method to detect connected hosts. If you want the switch to detect hosts when a DHCP snooping binding entry is created, you must enable DHCP snooping.

NAC Layer 3 IP Validation

The gateway IP feature supports two types of posture validation (PV) triggers:

- Intercept ACLs
- ARP-based triggers (SVI interfaces only)

Intercept ACLs are configured to intercept inbound traffic from the clients and initiate PV if the traffic matches the ACL.

If the IP admission rule configured on an interface does not have an associated intercept ACL, the gateway uses ARP or DHCP events to trigger posture validation on the interface.

When the gateway learns a new client in its ARP cache, it initiates PV with the client. Using the ARP-based triggers reduces ACL TCAM usage, but it is only valid for clients that are one Layer 3 hop away from the gateway. Therefore, you can configure only SVIs (and not router ports) to have IP admission rules without an intercept ACL.

Posture Validation

If only dynamic ARP inspection is enabled on the access VLAN assigned to a Layer 2 port, posture validation is initiated when ARP packets pass the dynamic ARP inspection validation checks. However, if DHCP snooping and dynamic ARP inspection are enabled, when you create a DHCP snooping binding entry, posture validation is initiated through DHCP.

When posture validation is initiated, the switch creates an entry in the session table to track the posture validation status of the host and follows this process to determine the NAC policy:

1. If the host is in the exception list, the switch applies the user-configured NAC policy to the host.
2. If EoU bypass is enabled, 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. 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 to be 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.

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

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

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.

There are two types of policies that apply during posture validation:

- 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 method to redirect all HTTP or HTTPS traffic to a remediation server that allows a noncompliant host to perform the necessary upgrade actions to become compliant.

The operation of the URL-redirect deny ACEs (typically to bypass the redirection of the HTTP traffic destined to remediation servers) is that the traffic to these ACEs is forwarded in hardware without applying the default interface and the downloaded host policies.

If this traffic (that is, the traffic that matches the deny URL redirect ACEs) is required to be filtered, you need to define a VLAN ACL on the Layer 2 access VLAN.

The URL redirect policy consists of the following:

- A URL that points to the remediation server.
- An ACL on the switch that causes all HTTP or 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.

Cisco Secure ACS and AV Pairs

When NAC IP validation is enabled, the Cisco Secure ACS provides NAC AAA services by using RADIUS. Cisco Secure ACS gets information about the antivirus status of the endpoint system and validates the antivirus condition of the endpoint.

You can set these Attribute-Value (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*

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

  The Auth-Proxy posture code checks if 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 is complete, the source address is changed from any to the host source IP address. The ACEs are prepended to the downloadable 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.

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

  These AV pairs enable the switch to intercept an HTTP 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. The url-redirect-acl AV pair contains the name or number of an ACL that specifies the HTTP or HTTPS traffic to be redirected. The ACL must be defined on the switch. Traffic that matches a permit entry in the redirect ACL will be redirected.

  These AV pairs may be sent if the host's posture is not healthy.

Note You can redirect the URL for either HTTP or HTTPS traffic but not for both at the same time. This situation occurs because the Cisco IOS software HTTP server can either listen to the HTTP port or to the HTTPS port but cannot listen to both at the same time.

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

Audit Servers

End devices that do not run Cisco Trust Agent (CTA) will not be able to provide credentials when challenged by Network Access Devices. These devices are described as *agentless* or *nonresponsive*. The NAC architecture has been extended to incorporate audit servers. An audit server is a third-party server that can probe, scan, and determine security compliance of a host without the need for presence of Cisco trust agent on the host. The result of the audit server examination can influence the access servers to make host-specific network access policy decisions instead of enforcing a common restrictive policy for all nonresponsive hosts. You can build more robust host audit and examination functionality by integrating any third-party audit operations into the NAC architecture.

Figure 51-3 shows how audit servers fit into the typical topology.

Figure 51-3 NAC Device Roles

The architecture assumes that the audit server can be reached so that the host can communicate with it. When a host (endpoint device) makes network access through the NAD configured for posture validation, the network access device eventually requests the AAA server (Cisco Secure ACS) for an access policy to be enforced for the host. The AAA server can be configured to trigger a scan of the host with an external audit server. The audit server scan occurs asynchronously and can take several seconds to complete. During the time of the audit server scan, the AAA server conveys a minimal restrictive security policy to NAD for enforcement along with a short poll timer (session-timeout). The NAD polls the AAA server at the specified timer interval until the result is available from the audit server. After the AAA server receives the audit result, it computes an access policy based on the audit result and is sent down to NAD for enforcement on its next request.

ACLs

If you configure NAC IP validation on an interface, you must also configure a default security ACL on the same interface. The default ACL is applied to IP traffic for hosts that have not completed posture validation.

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 Layer 2 port. If the policy applies to the traffic, the switch forwards the traffic. If the policy does not apply, the switch applies the default ACL. If there is no default ACL configured, the traffic is permitted.

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 Layer 2 port. The redirect URL ACL policy also takes precedence over the policy already configured on the host. If the default port ACL is not configured on the switch, the switch can still apply the downloadable ACL from the Cisco Secure ACS.

NAC Timers

The switch supports these timers:

- Hold Timer, page 51-9
- Idle Timer, page 51-10
- Retransmission Timer, page 51-11
- Revalidation Timer, page 51-11
- Status-Query Timer, page 51-11

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 a Accept-Reject message to the switch.

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

An EAPoUDP session might not be validated because 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 trying to cause a denial-of-service attack.

Idle Timer

The idle timer controls how long the switch waits for an ARP packet from the postured host or 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 hosts that have initiated posture validation and the IP device tracking table.

The idle timer is reset when the 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.

The default value of the idle timer is calculated as the probe interval times the number of probe retries. By default, the idle timer default is 90 seconds which is the probe interval of 30 seconds times the number of probe retries of 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. The switch then resets the aging timers for the list and the idle timer. If the switch receives no response, the switch ends the session with the Cisco Secure ACS, and the host is no longer validated.

The switch uses the IP device tracking table to detect and manage hosts connected to the switch. The switch also uses ARP or DHCP snooping to detect hosts. By default, the IP device tracking feature is disabled on a switch.

You must enable the IP device tracking feature to use NAC IP validation.

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 or Layer 3 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 the table and you can also configure 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 active entries in the IP device tracking table but limits the number of inactive entries. When the table reaches the table size limit, the switch removes the inactive entries. If the table does not have inactive entries, the number of entries in the IP device tracking table increases. When a host becomes inactive, the switch ends the host session.

The table size limit is 2048.

After an interface link is restored, the switch sends ARP probes for the entry associated with the interface. The switch ages out entries for hosts that do not respond to ARP probes. The switch changes the state of hosts that respond to an active host 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 that a NAC policy is applied to a client that used EAPoUDP messages during posture validation. The timer starts after the initial posture validation is complete. 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 by using the **eou timeout revalidation** *seconds* global configuration command. You can also specify the revalidation timer value on an interface by using the **eou timeout revalidation** *seconds* interface configuration command.

Note The revalidation timer can be configured locally on the switch or it can be downloaded from the control server.

The revalidation timer operation 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 one of these values 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 reauthenticated. 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 and Switchover

When RPR mode redundancy is configured, a switchover causes the loss of all information about currently postured hosts. All sessions will be revalidated. Users will be unvalidated and may see service disruption.

With Release 12.2(33)SXH and later releases, if you are using SSO mode redundancy, you can enter the **ip admission ha** command to enable host session table synchronization to the standby supervisor engine. When the high availability feature is enabled, established postured hosts do not need to be revalidated when a switchover occurs, because they will not see any disruption from the switchover. Posture sessions that were not yet established prior to the SSO will need to be revalidated after the switchover.

Configuring NAC

The following sections describe how to configure NAC:

Default NAC Configuration

By default, NAC IP validation is disabled.

NAC IP Guidelines, Limitations, and Restrictions

- The NAC feature applies access controls only to IPv4 traffic. NAC does not restrict Layer 2 bridged traffic.
- IPv6 traffic does not trigger posture validation and NAC IP does not apply access policies to IPv6 traffic.
- Default ACLs must permit EAPoUDP traffic for NAC IP to function.
- DHCP traffic must be permitted in the interface default ACL and the host policy for DHCP snooping to function.
- If you want to forward HTTP and HTTPS requests from an endpoint device to a specific URL, you must enable the HTTP server feature. The url-redirect-acl AV pair should be defined as the URL ACL name. This ACL should contain a **deny tcp any** *remediation server address* **eq www** command followed by the permit ACEs for the HTTP traffic that is being redirected.

NAC Layer 2 IP Guidelines, Limitations, and Restrictions

When configuring NAC Layer 2 IP validation, follow these guidelines, limitations, and restrictions:

- You must configure Layer 3 routes from the switch to the host for the Layer 2 IP to operate correctly.
- Layer 2 IP is not allowed if the parent VLAN of the port has VACL capture or Cisco IOS firewall (CBAC) is configured.
- LAN Port IP (LPIP) ARP traffic redirected to the CPU cannot be spanned using the SPAN feature.
- NAC Layer 2 IP validation is not supported on trunk ports, tunnel ports, EtherChannel members, or routed ports. The Catalyst 6500 series switches support Layer 2 IP on EtherChannels.
- When NAC Layer 2 IP validation is enabled, you must configure an ACL on the Layer 2 port to which hosts are connected.
- NAC Layer 2 IP is not supported if the Layer 2 port is part of a private VLAN.
- NAC Layer 2 IP ARP traffic redirected to the CPU cannot be spanned using the SPAN feature.
- A denial-of-service attack might occur if the switch receives many ARP packets with different source IP addresses. To avoid this problem, you must configure the IP admission MLS rate-limiting feature using the **mls rate-limit layer2 ip-admission** command.
- If DAI is also enabled on the parent VLAN of the Layer 2 port, the IP admission rate limiting for ARP packets directed to the CPU is ineffective. In this situation, ARP inspection rate limiting is functional. ARP inspection rate limiting is performed in software and IP admission rate limiting is performed in hardware.
- 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. 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. DHCP packets are permitted in DHCP environments in both the default interface and the 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 Layer 2 port with ACEs permitting DNS packets.
- If NAC Layer 2 IP validation is configured on a Layer 2 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, the NAC Layer 2 IP configuration takes precedence over VLAN ACLs and router ACLs that are configured on ingress interfaces. For example, when a VLAN ACL and a router ACL are configured, the operation applies the policies serially in the order of the LPIP policy to VLAN ACL to router ACL. The next policy is applied only when the traffic passes through the previous policy check. Any policy in the serial order denying the traffic causes the traffic to be denied. The downloaded LPIP host policy 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.
- The traffic sent to the URL-redirect deny ACEs is forwarded in hardware without applying the default interface and the downloaded host policies. If this traffic (that is, the traffic matching the deny URL-redirect ACEs) requires filtering, you should define a VLAN ACL on the Layer 2 access VLAN. This configuration allows you to bypass the redirection of the HTTP traffic destined for the remediation servers.

NAC Layer 3 IP Guidelines, Limitations, and Restrictions

When configuring NAC Layer 3 IP validation, follow these guidelines, limitations, and restrictions:

- NAC Gateway feature is supported on Supervisor Engine 720 and Supervisor Engine 32-8GE.
- For ARP-based trigger, the GWIP detects host presence using the ARP probing mechanism.
- When you enable NAC Gateway IP validation on an interface, you must also configure a default Cisco IOS ACL on the interface.
- The traffic sent to the URL-redirect deny ACEs is forwarded in hardware without applying the default interface and the downloaded host policies. If this traffic (that is, the traffic matching the deny URL-redirect ACEs) requires filtering, you should define a Cisco IOS ACL on the interface. This configuration allows you to bypass the redirection of the HTTP traffic destined for the remediation servers.
- If IEEE 802.1x authentication in single-host mode and NAC Layer 2 IP validation are configured on a Layer 2 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.

Configuring NAC IP Validation

To configure NAC Layer 2 IP validation, beginning in privileged EXEC mode, perform this task:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# 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	`Router(config)# mls rate-limit layer 2 ip ip-admission` *pps* (*burst*) or `Router(config)# mls rate-limit unicast ip features` *pps* (*burst*)	For a Layer 2 port, enables the rate limiting of the IP admission traffic to the CPU. For a Layer 3 port, enables the rate limiting of the IP admission traffic to the CPU.

	Command	Purpose
Step 4	`Router(config)# access-list access_list_number {deny | permit} source [source_wildcard] [log]`	Defines an ACL by using a source address and wildcard. The *access_list_number* value 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* value is the source address of the network or host from which the packet is being sent specified as follows: • 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 5	`Router(config)# interface interface_id`	Enters interface configuration mode.
Step 6	`Router(config)# ip access-group {access_list_number | name} in`	Controls access to the specified interface.
Step 7	`Router(config)# 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 name** *rule-name* interface configuration command.
Step 8	`Router(config)# exit`	Returns to global configuration mode.
Step 9	`Router# aaa new-model`	Enables AAA.
Step 10	`Router(config)# 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 11	`Router(config)# ip device tracking`	Enables the IP device tracking table. To disable the IP device tracking table, use the **no device tracking** global configuration command.

	Command	Purpose
Step 12	`Router(config)# ip device tracking probe {count count | interval interval}`	(Optional) Configures these parameters for the IP device tracking table: • **count** *count*—Sets the number of times that the switch sends the ARP probe. The range is from 1 to 5. The default is 3. • **interval** *interval*—Sets 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	`Router(config)# radius-server host {hostname | ip_address} key string`	(Optional) Configures the RADIUS server parameters. For the *hostname* or *ip_address* value, specify the hostname or IP address of the remote RADIUS server. For the **key** *string* value, 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, reenter this command.
Step 14	`Router(config)# radius-server attribute 8 include-in-access-req`	If the switch is connected to nonresponsive hosts, configures the switch to send the Framed-IP-Address RADIUS attribute (Attribute[8]) in access-request or accounting-request packets.
Step 15	`Router(config)# radius-server vsa send authentication`	Configures the network access server to recognize and use vendor-specific attributes.
Step 16	`Router(config)# ip device tracking [probe {count count | interval interval}]`	(Optional) Configures these IP device tracking table parameters: • **probe count** *count*—Sets 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. The default is 3. • **probe interval** *interval*—Sets the number of seconds that the switch waits before resending the ARP probe. The range is from 30 to 300 seconds. The default is 30 seconds.
Step 17	`Router(config)# eou logging`	(Optional) Enables EAPoUDP system logging events.
Step 18	`end`	Returns to privileged EXEC mode.

	Command	Purpose
Step 19	`Router# show ip admission {[cache] [configuration] [eapoudp]}`	Displays the NAC configuration or network admission cache entries.
Step 20	`Router# 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	`Router# show ip access lists interface interface`	Displays the downloaded host policies in the Cisco IOS software configuration.
Step 22	`Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

When configuring NAC IP validation, note the following guidelines:

- To remove the IP NAC rule on the switch, use the **no ip admission name** *rule_name* **eapoudp** global configuration command. To remove the IP NAC rule that was applied to a specific interface, use the **no ip admission** *admission_name* interface configuration command.
- To remove the EAPoUDP authentication methods, use the **no aaa authentication eou default** global configuration command. To configure the auth-proxy posture code to not obtain security associations from the AAA server, use the **no aaa authorization auth-proxy default** global configuration command.
- To disable the IP device tracking table and return the parameters for the table to the default values, use the **no device tracking** and the **no device tracking probe** {**count** | **interval**} global configuration commands.
- 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.
- To disable the logging of EAPoUDP system events, use the **no eou logging** 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.
- If IEEE 802.1x authentication in single-host mode and NAC Layer 2 IP validation are configured on a Layer 2 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.

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

```
Router# configure terminal
Router(config)# ip admission name nac eapoudp
Router(config)# access-list 5 permit any any
Router(config)# interface gigabitethernet 2/0/1
Router(config-if)# ip access-group 5 in
Router(config-if)# ip admission nac
Router(config-if)# exit
Router(config)# aaa new-model
Router(config)# aaa authentication eou default group radius
Router(config)# radius-server host admin key rad123
Router(config)# radius-server vsa send authentication
Router(config)# ip device tracking probe count 2
Router(config)# eou logging
Router(config)# end
```

Configuring EAPoUDP

To configure the EAPoUDP, beginning in privileged EXEC mode, perform this task:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.

Step 2	`Router(config)# 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 **allow**, **default**, **logging**, **max-retry**, **port**, **rate-limit**, **revalidate**, and **timeout** keywords, see the command reference for this release and the *Network Admission Control* feature module.

Step 3	`Router(config)# interface interface_id`	Enters interface configuration mode.

Step 4	`Router(config)# 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 **default**, **max-retry**, **revalidate**, and **timeout** keywords, see the command reference for this release and the *Network Admission Control* feature module.

Step 5	`end`	Returns to privileged EXEC mode.
Step 6	`Router# 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	`Router# 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** interface configuration commands.

Configuring Identity Profiles and Policies

To configure the identity profile and policy beginning in privileged EXEC mode, perform this task:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# identity policy policy_name`	Creates an identity policy, and enters identity-policy configuration mode.
Step 3	`Router(config-identity-policy)# access-group access_group`	Defines network access attributes for the identity policy.
Step 4	`Router(config)# identity profile eapoudp`	Creates an identity profile, and enters identity-profile configuration mode.

	Command	Purpose
Step 5	`Router(config-identity-prof)# 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 applies the specified policy to the device.
Step 6	`Router(config)# exit`	Exits from identity-profile configuration mode, and returns to global configuration mode.
Step 7	`Router# end`	Returns to privileged EXEC mode.
Step 8	`Router# show running-config`	Verifies your entries.
Step 9	`Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

To remove the identity policy from the switch, use the **no identity-policy** *policy_name* global configuration command. To remove the identity profile, use the **no identity profile eapoudp** global configuration command. 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.

This example shows how to configure the identity profile and policy:

```
Router# configure terminal
Router(config)# identity policy policy1
Router(config-identity-policy)# access-group group1
Router(config)# identity profile eapoudp
Router(config-identity-prof)# device authorize ip address 10.10.142.25 policy policy1
Router(config-identity-prof)# exit
Router(config)# end
```

Configuring NAC High Availability

To configure IP admission high availability, perform this task:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# ip admission ha`	Enables IP admission high availability.
Step 3	`Router(config)# ip admission ha update update_interval`	Defines how often the active supervisor engine sends synchronization updates to the standby. The interval has a range of 30 to 60 seconds.
Step 4	`Router# show ip admission ha stats`	Displays the statistics related to session synchronization.
Step 5	`Router# clear ip admission ha stats`	(Optional) Clears the statistics related to session synchronization.

Note You cannot enable the IP admission high availability feature if there are active Webauth or Posture sessions.

To disable IP admission high availability from the switch, use the **no ip admission ha** configuration command.

This example shows how to configure IP admission high availability:

```
Router# configure terminal
Router(config)# ip admission ha
Router(config)# ip admission ha update 50
Router(config)# end
Router(config)# clear ip admission ha stats
Router(config-identity-prof)# show ip admission ha stats
```

Configuring a NAC AAA Down Policy

To configure NAC AAA down policy, perform this task:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# ip admission name` *rule-name* `eapoudp event timeout aaa policy identity` *identity_policy_name*	Creates a NAC rule and associates 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 identity** global configuration command.
Step 3	`Router(config)# 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 follows: • The 32-bit quantity in dotted-decimal format. • The keyword **any** as an abbreviation for *source* and *source-wildcard* value of 0.0.0.0 255.255.255.255. You do not need to enter a *source-wildcard* value. • The keyword **host** as an abbreviation for source and source-wildcard of *source* 0.0.0.0. (Optional) Applies the *source-wildcard* wildcard bits to the source. (Optional) Enters **log** to cause an informational logging message about the packet that matches the entry to be sent to the console.
Step 4	`Router(config-if)# interface` *interface-id*	Enters interface configuration mode.
Step 5	`Router(config-if)# ip access-group` {*access-list-number* | *name*} **in**	Controls access to the specified interface.
Step 6	`Router(config-if)# ip admission` *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	`Router(config)# exit`	Returns to global configuration mode.
Step 8	`Router(config)# aaa new-model`	Enables AAA.

	Command	Purpose
Step 9	`Router(config)# 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	`Router(config)# 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	`Router(config)# 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 12	`Router(config)# ip device tracking [probe {count` *count* `| interval` *interval*`}]`	(Optional) Configures these parameters for the IP device tracking table: • **count** *count*—Sets the number of times that the switch sends the ARP probe. The range is from 1 to 5. The default is 3. • **interval** *interval*—Sets 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	`Router(config)# radius-server host {`*hostname* `|` *ip-address*`} test username` *username* `idle-time 1 key` *string*	(Optional) Configures the RADIUS server parameters. For the *hostname* or *ip-address,* specify the hostname or IP address of the remote RADIUS server. For the **key** *string* value, 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. The **test username** value parameter is used for configuring the dummy username that tests whether the AAA server is active or not. The **idle-time** parameter is used to set how often the server should be tested to determine its operational status. If there is no traffic to the RADIUS server, the NAD sends dummy radius packets to the RADIUS server based on the idle-time. If you want to use multiple RADIUS servers, reenter this command.
Step 14	`Router(config)# radius-server attribute 8 include-in-access-req`	(Optional) Configures the switch to send the Framed-IP-Address RADIUS attribute (Attribute[8]) in access-request or accounting-request packets if the switch is connected to nonresponsive hosts. 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	`Router(config)# radius-server vsa send authentication`	Configures the network access server to recognize and use vendor-specific attributes.

	Command	Purpose
Step 16	`Router(config)# radius-server dead-criteria {tries | time} value`	Forces one or both of the criteria (used to mark a RADIUS server as dead) to be the indicated constant.
Step 17	`Router(config)# 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	`Router(config)# end`	Returns to privileged EXEC mode.
Step 19	`Router# show ip admission {[cache] [configuration] [eapoudp]}`	Displays the NAC configuration or network admission cache entries.
Step 20	`Router# 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	`Router(# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

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

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

Show running output
-------------------
aaa new-model
aaa authentication eou default group radius
aaa authorization network default local

ip admission name AAA_DOWN eapoudp event timeout aaa policy identity global_policy

identity policy global_policy
 access-group global_acl

interface FastEthernet2/13
 switchport
 switchport access vlan 222
 switchport mode access
 no ip address
 ip access-group 115 in
 ip admission AAA_DOWN
```

```
!
ip access-list extended global_acl
 permit ip any any

radius-server dead-criteria tries 3
radius-server attribute 8 include-in-access-req
radius-server host 40.0.0.4 auth-port 1645 acct-port 1646 test username administrator
idle-time 1 key cisco
radius-server vsa send authentication

Router# 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
Auth-proxy name AAA_DOWN
   eapoudp list not specified auth-cache-time 60 minutes
   Identity policy name global_policy for AAA fail policy
```

Monitoring and Maintaining NAC

You can perform the tasks in these sections to monitor and maintain NAC:

- Clearing Table Entries, page 51-23
- Displaying NAC Information, page 51-23

Clearing Table Entries

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 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.

Displaying NAC Information

To display NAC information, perform one of the following tasks:

Command	Purpose
Router# **show dot1x** [**all** | **interface** *interface_id* | **statistics interface** *interface_id*]	Displays IEEE 802.1x statistics, administrative status, and operational status.
Router# **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.
Router# **show ip admission** {[**cache**] [**configuration**] [**eapoudp**]}	Displays the NAC configuration or network admission cache entries.
Router# **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.