Network Admission Control Configuration Guide Cisco IOS Release 15MT

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

CONTENTS

Network Admission Control

The Network Admission Control feature addresses the increased threat and impact of worms and viruses have on business networks. This feature is part of the Cisco Self-Defending Network Initiative that helps customers identify, prevent, and adapt to security threats.

In its initial phase, the Cisco Network Admission Control (NAC) functionality enables Cisco routers to enforce access privileges when an endpoint attempts to connect to a network. This access decision can be on the basis of information about the endpoint device, such as its current antivirus state. The antivirus state includes information such as version of antivirus software, virus definitions, and version of scan engine.

Network admission control systems allow noncompliant devices to be denied access, placed in a quarantined area, or given restricted access to computing resources, thus keeping insecure nodes from infecting the network.

The key component of the Cisco Network Admission Control program is the Cisco Trust Agent, which resides on an endpoint system and communicates with Cisco routers on the network. The Cisco Trust Agent collects security state information, such as what antivirus software is being used, and communicates this information to Cisco routers. The information is then relayed to a Cisco Secure Access Control Server (ACS) where access control decisions are made. The ACS directs the Cisco router to perform enforcement against the endpoint.

Prerequisites for Network Admission Control

- The Cisco IOS router must be running Cisco IOS software Release 12.3(8)T or later.
- The Cisco Trust Agent must be installed on the endpoint devices (for example, on PCs and laptops).
- A Cisco Secure ACS is required for authentication, authorization, and accounting (AAA).
- A proficiency with configuring access control lists (ACLs) and AAA is necessary.

Restrictions for Network Admission Control

- This feature is available only on Cisco IOS firewall feature sets.

Information About Network Admission Control

Before configuring the Network Admission Control feature, the following concepts need to be understood:

Virus Infections and Their Effect on Networks

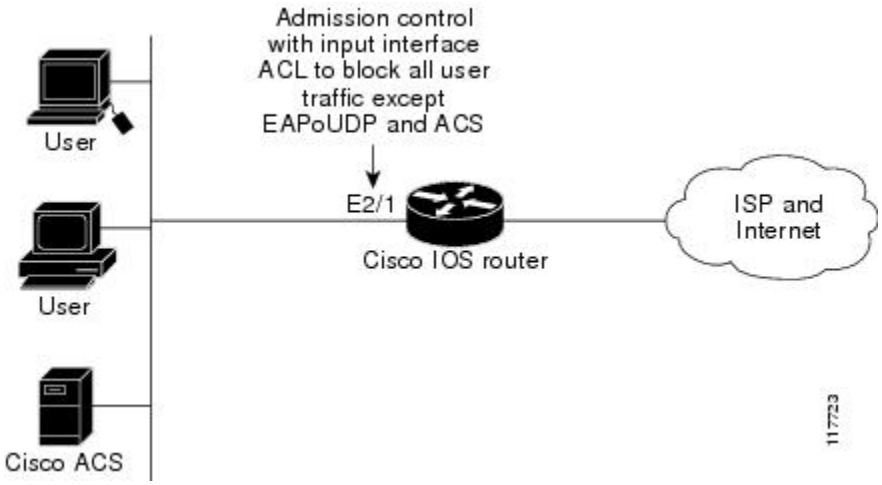
Virus infections are the single largest cause of serious security breaches for networks and often result in huge financial losses. Sources of virus infections are insecure endpoints (for example, PCs, laptops, and servers). Although the endpoints may have antivirus software installed, the software is often disabled. Even if the software is enabled, the endpoints may not have the latest virus definitions and scan engines. A larger security risk is from devices that do not have any antivirus software installed. Although antivirus vendors today are making it more difficult to disable the antivirus software, they are not addressing the risk of outdated virus definitions and scan engines.

How Network Admission Control Works

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

The figure below illustrates how Cisco Network Admission Control works.

Figure 1 Cisco IOS Network Admission Control System



The figure above shows that IP admission control is applied at the LAN interface. All network devices must be validated for their antivirus states upon their initial IP connections through the router. Until then, all traffic from endpoint systems (except for EAPoUDP and Cisco Secure ACS traffic) is blocked at the interface.

The endpoint system is then challenged for its antivirus state over an EAPoUDP association. The endpoint system gains access to the network if it complies with the network admission control policy as evaluated by the Cisco Secure ACS. If the endpoint system does not comply, the device is either denied access or quarantined.

Network Access Device

A network access device (NAD) is typically a Cisco IOS router (a Layer 3 Extensible Authentication Protocol over User Datagram Protocol [EAPoUDP] access point) that provides connectivity to external networks, such as the Internet or remote enterprise networks. Cisco Network Admission Control functionality may have an Intercept ACL, which determines connections that are intercepted for network admission. Connections from endpoints that match the access list are intercepted by Network Admission Control and are challenged for their antivirus states over a Layer 3 association before they are granted network access.

Cisco Trust Agent

Cisco Trust Agent is a specialized software that runs on endpoint systems. Cisco Trust Agent responds to challenges from the router about the antivirus state of an endpoint system. If an endpoint system is not running the Cisco Trust Agent, the network access device (router) classifies the endpoint system as “clientless.” The network access device uses the EOU clientless username and EOU clientless password that are configured on the network access device as the credentials of the endpoint system for validation with Cisco Secure ACS. The policy attributes that are associated with this username are enforced against the endpoint system.

Cisco Secure ACS

Cisco Secure ACS provides authentication, authorization, and accounting services for network admission control using industry-standard RADIUS authentication protocol. Cisco Secure ACS returns access control decisions to the network access device on the basis of the antivirus credentials of the endpoint system.

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

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

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

- posture-token--Enables Cisco Secure ACS to send a text version of a system posture token (SPT) that is derived by posture validation. The SPT is always sent in numeric format, and using the posture-token AV pair makes it easier to view the result of a posture validation request on the AAA client. (See the following example.)

```
posture-token=Healthy
```

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

- ◦ Healthy
  ◦ Checkup
  ◦ Quarantine
  ◦ Infected
  ◦ Unknown
- status-query-timeout--Overrides the status-query default value of the AAA client with the user specified value, in seconds. (See the following example.)

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

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

Remediation

Network Admission Control supports HTTP redirection that redirects any HTTP request from the endpoint device to a specified redirect address. This support mechanism redirects all HTTP requests from a source to a specified web page (URL) to which the latest antivirus files can be downloaded. For the HTTP redirection to work, the value must be set for the “url-redirect” VSA on the ACS and, correspondingly, associate an access control entry in the downloadable ACL that permits the access of the endpoint system to the redirect URL address. After the value of the url-redirect VSA has been set and the access control entry has been associated, any HTTP request that matches the IP admission Intercept ACL are redirected to the specified redirect URL address.

Network Admission Control and Authentication Proxy

It is possible that network admission control and authentication proxy can be configured for the same set of hosts on a given interface. In each case, the Intercept ACL should be the same for IP admission EAPoUDP and authentication proxy. IP admission proxy with proxy authentication should be configured first, followed by IP admission control.

NAC MIB

The NAC MIB feature adds Simple Network Management Protocol (SNMP) support for the NAC subsystem. Using SNMP commands (get and set operations), an administrator can monitor and control NAC sessions on the network access device (NAD).

For more information about SNMP get and set operations, see the subsection "NAC MIB, page 5" in the section "Additional References, page 25."

Correlation Between SNMP Get and Set Operations and the Cisco CLI

Most of the objects in the object tables in the NAC MIB (CISCO-NAC-NAD-MIB.my) describe various EAPoUDP and session parameters that are applicable to the setup of a NAD. These properties can be viewed and modified by performing various SNMP get and set operations. Many of the values of the table objects can also be viewed or modified by configuring corresponding command-line interface (CLI) commands on a router. For example, an SNMP get operation can be performed on the cnnEOUGlobalObjectsGroup table or the **show eou** command can be configured on a router. The parameter information obtained from the SNMP get operation is the same as the output from the **show eou** command. Similarly, performing an SNMP get operation on the table cnnEouIfConfigTable provides interface-specific parameters that can also be viewed in output from the **show eou** command.

SNMP set operations are allowed for table objects that have corresponding CLI commands, which can be used to modify table object values. For example, to change the value range for the cnnEouHostValidateAction object in the cnnEouHostValidateAction MIB table to 2, you can either perform the SNMP set operation or configure the **eou initialize all** command on a router.

For examples of NAC MIB output, see the subsection NAC MIB Output Examples in the section Configuration Examples for Network Admission Control.

Initializing and Revalidating Sessions

NAC allows administrators to initialize and revalidate sessions using the following CLI commands:

- **eou initialize all**
- **eou initialize authentication clientless**
- **eou initialize authentication eap**
- **eou initialize authentication static**
- **eou initialize ip** {*ip-address* }
- **eou initialize mac** {*mac-address* }

- **eou initialize posturetoken** {*string*}
- **eou revalidate all**
- **eou revalidate authentication clientless**
- **eou revalidate authentication eap**
- **eou revalidate authentication static**
- **eou revalidate ip** {*ip-address*}
- **eou revalidate mac** {*mac-address* }
- **eou revalidate posturetoken** {*string*}

The initialization and revalidation actions can also be accomplished by performing SNMP set operations on the objects of the cnnEouHostValidateAction table. For more information about initializing and revalidating sessions, see the section Commands That Correlate to cnnEouHostValidateAction Table Objects.

For examples of CLI commands that correlate to changes that can be made to cnnEouHostValidateAction table objects, see the subsection NAC MIB Output Examples in the section Configuration Examples for Network Admission Control.

Session-Specific Information

The NAC MIB provides a way to view session-specific details using the cnnEouHostQueryTable and cnnEouHostResultTable. The cnnEouHostQueryTable is used to build the query. The query is the same format as the **show eou ip** {*ip-address*} command (that is, the IP address would be shown as in the **show eou ip** command--for example, 10.1.1.1).Administrators must use the SNMP set operation on the objects of the cnnEouHostQueryTable to create the query. The results of the query are stored as a row in the cnnEouHostResultTable. For more information about viewing session-specific details, see the section Viewing MIB Query Results.

Using show Commands to View MIB Object Information

The CLI commands **show eou**, **show eou all**, **show eou authentication**, **show eou initialize**, **show eou ip**, **show eou mac**, **show eou posturetoken, show eou revalidate**, and **show ip device tracking all**provide the same output information as that in the CISCO-NAC-NAD-MIB tables using SNMP get operations.

For examples of **show** command output information that can also be viewed in MIB object tables, see the subsection NAC MIB Output Examples in the section Configuration Examples for Network Admission Control

How to Configure Network Admission Control

Configuring the ACL and Admission Control

Network admission control is applied in the inbound direction at any interface. Applying network admission control inbound at an interface causes network admission control to intercept the initial IP connections of the intercept end system through the router.

Use the steps in this section to configure an intercept ACL.

Note In this configuration, an intercept ACL is defined as "101," and the Intercept ACL is associated with the IP admission control rule "greentree." Any IP traffic that is destined to the 192.50.0.0 network are subjected to validation. In addition, beginning with Step 5, an intercept ACL is applied inbound to the interface that is associated with network admission control. This ACL typically blocks access to endpoint systems until they are validated. This ACL is referred to as the default access list.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **{ permit | deny }** *protocol source destination*
4. **ip admission name** *admission-name* [**eapoudp | proxy { ftp | http | telnet }] [list** {*acl* | *acl-name*}]
5. **interface** *type slot / port*
6. **ip address** *ip-address mask*
7. **ip admission** *admission-name*
8. **exit**
9. Do one of the following:
   - **access-list** *access-list-number* **{ permit | deny }** *protocol source destination*
10. **ip access-group** {*access-list-number* |*access-list-name*} **in**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**access-list** *access-list-number* **{ permit | deny }** *protocol source destination* **Example:** `Router (config)# access-list 101 permit ip any 192.50.0.0 0.0.0.255`	Defines a numbered access list.
Step 4	**ip admission name** *admission-name* [**eapoudp | proxy { ftp | http | telnet }] [list** {*acl* | *acl-name*}] **Example:** `Router (config)# ip admission name greentree eapoudp list 101`	Creates IP network admission control rules. The rules define how you apply admission control. The rules are as follows: • **eapoudp** --Specifies IP network admission control using EAPoUDP. • **proxy ftp** --Specifies FTP to trigger authentication proxy. • **proxy http** --Specifies HTTP to trigger authentication proxy. • **proxy telnet** --Specifies Telnet to trigger authentication proxy. You can associate the named rule with an ACL, providing control over which hosts use the admission control feature. If no standard access list is defined, the named admission rule intercepts IP traffic from all hosts whose connection-initiating packets are received at the configured interface. The list option allows you to apply a standard, extended (1 through 199) or named access list to a named admission control rule. IP connections that are initiated by hosts in the access list are intercepted by the admission control feature.
Step 5	**interface** *type slot / port* **Example:** `Router (config)# interface ethernet 2/1`	Defines an interface and enters interface configuration mode.
Step 6	**ip address** *ip-address mask* **Example:** `Router (config-if)# ip address 192.0.0.1 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 7	**ip admission** *admission-name* **Example:** `Router (config-if)# ip admission greentree`	Applies the named admission control rule at the interface.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Router (config-if)# exit`	Exits interface configuration mode.

Step 9	Do one of the following:
	• **access-list** *access-list-number* **{ permit | deny }** *protocol source destination*
	
	Example:
	`Router (config)# access-list 105 permit udp any any`
	
	Example:
	`Router (config)# access-list 105 permit ip host 192.168.0.2 any`
	
	Example:
	`Router (config)# access-list 105 deny ip any any`
	
	Example:
		Defines a numbered access list.
		Note In the first two examples (under "Command or Action"), ACL "105" denies all IP traffic except UDP and access to 192.168.0.2 (Cisco Secure ACS).
		Note In the third example (under "Command or Action," ACL "105" is applied on the interface that is configured for network admission control, and access to endpoint systems (except for EAPoUDP traffic and access to Cisco Secure ACS [192.168.0.2 in the example] is blocked until their antivirus states are validated. This ACL ("105") is referred to as "Interface ACL."

Step 10	**ip access-group** {*access-list-number* |*access-list-name*} **in** **Example:** `Router (config)# ip access-group 105 in`	Controls access to an interface.

Configuring Global EAPoUDP Values

To configure global EAPoUDP values, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **eou** { allow | **clientless** | default | initialize | **logging** | **max-retry** | **port** | **rate-limit** | **revalidate** | **timeout**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**eou** { allow | **clientless** | default | initialize | **logging** | **max-retry** | **port** | **rate-limit** | **revalidate** | **timeout**} **Example:** `Router (config)# eou initialize`	Specifies EAPoUDP values. • For a breakout of available keywords and arguments for the **eou** command, see the following commands: ◦ **eou allow** ◦ **eou clientless** ◦ **eou default** ◦ **eou initialize** ◦ **eou logging** ◦ **eou max-retry** ◦ **eou port** ◦ **eou rate-limit** ◦ **eou revalidate** ◦ **eou timeout**

Configuring an Interface-Specific EAPoUDP Association

To configure an EAPoUDP association that can be changed or customized for a specific interface that is associated with network admission control, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot / port*
4. **eou** [**default** | **max-retry** | **revalidate** | **timeout**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot / port* **Example:** `Router (config)# interface ethernet 2/1`	Defines an interface and enters interface configuration mode.
Step 4	**eou** [**default** | **max-retry** | **revalidate** | **timeout**] **Example:** `Router (config-if)# eou revalidate`	Enables an EAPoUDP association for a specific interface. • For a breakout of available keywords and arguments for the **eou** command, see the following commands: ◦ **eou default** ◦ **eou max-retry** ◦ **eou revalidate** ◦ **eou timeout**

Configuring AAA for EAPoUDP

To set up AAA for EAPoUDP, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication eou default enable group radius**
5. **aaa authorization network default group radius**
6. **radius-server host** {*hostname* | *ip-address*}
7. **radius-server key** {**0** *string* | **7** *string* | *string*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router (config)# aaa new-model`	Enables the AAA access control model.
Step 4	**aaa authentication eou default enable group radius** **Example:** `Router (config)# aaa authentication eou default enable group radius`	Sets authentication lists for an EAPoUDP association.
Step 5	**aaa authorization network default group radius** **Example:** `Router (config)# aaa authorization network default group radius`	Uses the list of all RADIUS servers for authentication.
Step 6	**radius-server host** {*hostname* | *ip-address*} **Example:** `Router (config)# radius-server host 192.0.0.40`	Specifies a RADIUS server host.
Step 7	**radius-server key** {**0** *string* | **7** *string* | *string*} **Example:** `Router (config)# radius-server key cisco`	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

Configuring the Identity Profile and Policy

Identity is a common infrastructure that is used to specify local profile and policy configurations. The identity profile allows you to statically authorize or validate individual devices on the basis of IP address, MAC address, or device type. Each statically authenticated device can be associated with a local policy that specifies the network access control attributes. Hosts are added to this "exception list" using the **identity profile** command, and corresponding policies are associated with these hosts using the **identity policy** command.

If the client is part of the identity (that is, the client is on the exception list), the status of the client is set on the basis of the identity configuration. The client does not have to go through the posture validation process, and the associated identity policy is applied for the client.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **identity profile eapoudp**
4. **device** {**authorize** {**ip address** *ip-address* {**policy** *policy-name}* | **mac-address***mac-address* | **type** *{***cisco** | **ip** | **phone***}}* | **not-authorize***}*
5. **exit**
6. **identity policy** *policy-name* [**access-group** *group-name* | **description** *line-of-description* | **redirect** *url* | **template** [**virtual-template** *interface-name*]]
7. **access-group** *group-name*
8. **exit**
9. **exit**
10. **ip access-list extended** *access-list-name*
11. {**permit** | **deny**} *source source-wildcarddestination destination-wildcard*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**identity profile eapoudp** **Example:** `Router (config)# identity profile eapoudp`	Creates an identity profile and enters identity profile configuration mode.
Step 4	**device** {**authorize** {**ip address** *ip-address* {**policy** *policy-name}* | **mac-address***mac-address* | **type** *{***cisco** | **ip** | **phone***}}* | **not-authorize***}* **Example:** `Router (config-identity-prof)# device authorize ip address 10.10.142.25 policy policyname1`	Statically authorizes an IP device and applies an associated policy to the device.
Step 5	**exit** **Example:** `Router (config-identity-prof)# exit`	Exits identity profile configuration mode.
Step 6	**identity policy** *policy-name* [**access-group** *group-name* | **description** *line-of-description* | **redirect** *url* | **template** [**virtual-template** *interface-name*]] **Example:** `Router (config-identity-prof)# identity policy policyname1`	Creates an identity policy and enters identity policy configuration mode.
Step 7	**access-group** *group-name* **Example:** `Router (config-identity-policy)# access-group exempt-acl`	Defines network access attributes for the identity policy.
Step 8	**exit** **Example:** `Router (config-identity-policy)# exit`	Exits identity policy configuration mode.
Step 9	**exit** **Example:** `Router (config-identity-prof)# exit`	Exits identity profile configuration mode.

	Command or Action	Purpose
Step 10	**ip access-list extended** *access-list-name* **Example:** `Router (config)# ip access-list extended exempt-acl`	Defines access control for statically authenticated devices (and enters network access control configuration mode).
Step 11	{**permit** | **deny**} *source source-wildcarddestination destination-wildcard* **Example:** `Router (config-ext-nacl)# permit ip any 192.50.0.0. 0.0.0.255`	Set conditions to allow a packet to pass a named IP access list.

Clearing EAPoUDP Sessions That Are Associated with an Interface

To clear EAPoUDP sessions that are associated with a particular interface or that are on the NAD, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **clear eou all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear eou all** **Example:** `Router# clear eou all`	Clears all EAPoUDP sessions on the NAD.

Verifying Network Admission Control

To verify EAP and EAPoUDP messages or sessions, perform the following steps. The **show** commands may be used in any order or independent of the other **show** command.

SUMMARY STEPS

1. **enable**
2. **show eou all**
3. **show ip admission eapoudp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show eou all** **Example:** `Router# show eou all`	Displays information about EAPoUDP sessions on the network access device.
Step 3	**show ip admission eapoudp** **Example:** `Router# show ip admission eapoudp`	Displays the network admission control configuration or network admission cache entries.

Troubleshooting Network Admission Control

The following commands may be used to display information about EAP and EAPoUDP messages or sessions. The **debug** commands may be used in any order or independent of the other **debug** commands.

SUMMARY STEPS

1. **enable**
2. **debug eap** {**all** | **errors** | **packets** | **sm**}
3. **debug eou** {**all** | **eap** | **errors** | **packets** | **sm**}
4. **debug ip admission eapoudp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug eap** {**all** | **errors** | **packets** | **sm**} **Example:** `Router# debug eap all`	Displays information about EAP messages.
Step 3	**debug eou** {**all** | **eap** | **errors** | **packets** | **sm**} **Example:** `Router# debug eou all`	Displays information about EAPoUDP messages.
Step 4	**debug ip admission eapoudp** **Example:** `Router# debug ip admission eapoudp`	Displays information about IP admission events.

Monitoring and Controlling NAC with the CISCO-NAC-NAD-MIB

CLI Commands That Correlate to cnnEouGlobalObjectsGroup Table Objects

An SNMP get or set operation can be performed to obtain or change information about value ranges for objects in the cnnEouGlobalObjectsGroup table. The same information can be viewed in output from the **show eou**command. The table below displays examples of some global configuration objects and the SNMP get and set operations required to obtain or change their values.

For an example of **show eou** command output, see the show eou section of the NAC MIB Output Examples section.

Table 1 Obtaining and Changing Global Configuration Values Using SNMP Get and Set Operations

Global Configuration Objects	SNMP Operation
EAPoUDP version	Performs a get operation on the cnnEouVersion object. (The object value is “1.”)
EAPoUDP port	Performs a get operation on the cnnEouPort object.
Enabling logging (enable EOU logging)	Sets the cnnEouLoggingEnable object. (The object value is “true.”)

CLI Commands That Correlate to cnnEoulfConfigTable Objects

An SNMP get operation is performed to obtain information about value ranges for objects in the cnnEouIfConfigTable. The same information can be viewed in output from the **show eou**command. The table below displays examples of some interface-specific configuration objects and the SNMP get operations required to obtain their values.

Table 2 Obtaining Interface-Specific Configuration Values Using SNMP Get Operations

Interface-Specific Object	SNMP Operation
AAA timeout	Performs a get operation on the cnnEouIfTimeoutAAA object. • Format: GET cnnEouIfTimeoutAAA.IfIndex • You must specify the corresponding index number of the specific interface.
Maximum retries	Performs a get operation on the cnnEouIfMaxRetry object. • Format: GET cnnEouIfMaxRetry.IfIndex

CLI Commands That Correlate to cnnEouHostValidateAction Table Objects

EOU sessions can be initialized or revalidated by the CLI or by using the SNMP set operation on the table cnnEouHostValidateAction.

Following are some examples (listed by CLI command) that correlate to MIB objects.

eou initialize all

EOU initialization can be accomplished for all sessions by using the **eou initialize all** command or by using an SNMP set operation on the object cnnEouHostValidateAction. This object must be set to the numeric value 2.

eou initialize authentication clientless

EOU initialization can be accomplished for sessions having an authentication type “clientless” using the **eou initialize authentication clientless** command or an SNMP set operation on the object cnnEouHostValidateAction. This object must be set to the numeric value 3.

eou initialize ip

EOU initialization can be accomplished for a particular session using the **eou initialize ip** {*ip-address* } command.

To achieve the same result using an SNMP operation, three objects have to be set in the cnnEouHostValidateAction MIB table:

- cnnEouHostValidateAction--The value range must be set.
- cnnEouHostValidateIpAddrType--The IP address type must be set. This value must be set to IPv4 because IPv4 is currently the only address type supported by NAC. (This value is the type of address being set for the cnnEouHostValidateIPAddr object.)
- cnnEouHostValidateIPAddr--The IP address must be set.

Note The three MIB objects should be set in a single SNMP set operation.

eou initialize posturetoken

All sessions having a particular posturetoken can be initialized using the **eou initialize posturetoken** {*string* } command. The default value range for this command is 8.

To achieve the same result using an SNMP set operation, you must set the following objects:

- cnnEouHostValidateAction--Set this value to 8.
- cnnEouHostValidatePostureTokenStr--Set the string value.

Note The two MIB objects should be set in a single SNMP set operation.

Creating MIB Query Tables

The MIB table cnnEouHostQueryTable is used to create, or build, MIB queries.

MIB Query Correlating to the CLI show eou all Command

To build a query that provides the same results as using the **show eou all**command, perform the following SNMP get operation.

The object cnnEouHostQueryMask in the table cnnEouHostQueryTable indicates the kind of query. The corresponding value of the cnnEouHostQueryMask object in output from the **show eou all** command is 8 (the integer value).

SUMMARY STEPS

1. Set the cnnEouHostQueryStatus object to createandgo.
2. Set the cnnEouHostQueryMask object to 8.
3. Set the cnnEouHostQueryStatus object to active.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Set the cnnEouHostQueryStatus object to createandgo.	Creates a query row.
Step 2	Set the cnnEouHostQueryMask object to 8.	Corresponds in value to the **show eou all** command.
Step 3	Set the cnnEouHostQueryStatus object to active.	Indicates that you have finished building the query.

Note Examples are not shown in the previous table because the format differs depending on the software you are using.

- What to Do Next, page 20

What to Do Next

View the results. See the section Viewing MIB Query Results Correlating to the show eou all Command.

Viewing MIB Query Results Correlating to the show eou all Command

After the MIB query has been built and you have indicated that you are finished (with the “active” status), the results can be viewed. A query in the cnnEouHostQueryTable is represented by a row. The row number is the Query Index. Similarly, the cnnEouHostResultTable is composed of result rows. Each row in the cnnEouHostResultTable is uniquely identified by a combination of Query Index and Result Index. The results of the cnnEouHostQueryTable index and the cnnEouHostResultTable have to be matched. Match one row in the Query table to one of the rows in the Result table. For example, if a query that corresponds to a **show** command results in ten sessions, the Result table has ten rows, each row corresponding to a particular session. The first row in the Result table is R1.1. The second row is R1.2, and so on to R1.10. If another query is created in the Query table, and it results in five sessions, five rows are created in the Result table (R2.1, R2.2, R2.3, R2.4, and R2.5).

The table below illustrates how the Query table sessions are mapped to Result table rows.

Table 3 Query Table-to-Result Table Mapping

Query Table	Result Table Rows
Q1 (10 sessions)	R1.1, R1.2, R1.3, R1.4, R1.5, R1.6, R1.7, R1.8, R1.9, R1.10
Q2 (5 sessions)	R2.1, R2.2, R2.3, R2.4, R2.5

To create an SNMP query that provides the same information as output from the **show eou ip {***ip-address***} command**, perform the following steps.

SUMMARY STEPS

1. Set cnnEouHostQueryStatus to createandgo.
2. Set cnnEouHostQueryIpAddrType to IPv4 and the IP address (for example, 10.2.3.4).
3. Set cnnEouHostQueryStatus to active.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Set cnnEouHostQueryStatus to createandgo.	Creates a query row.
Step 2	Set cnnEouHostQueryIpAddrType to IPv4 and the IP address (for example, 10.2.3.4).	Sets the address type. • The only address type currently supported by NAC is IPv4.
Step 3	Set cnnEouHostQueryStatus to active.	Indicates you have finished building the query.

Note Examples are not shown in the previous table because the format differs depending on the software you are using.

Viewing the Results in the cnnEouHostResultTable

To view the results in the cnnEouHostResultTable, perform the following steps.

SUMMARY STEPS

1. Perform a get operation on cnnEouHostQueryRows.
2. Perform a get operation on the cnnEouHostResultTable objects in the format resultTableObjectName.QueryIndex.ResultIndex.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Perform a get operation on cnnEouHostQueryRows.	Finds how many rows are created in a Result table for a particular query. • If a query row is a negative number, the query is still being processed.
Step 2	Perform a get operation on the cnnEouHostResultTable objects in the format resultTableObjectName.QueryIndex.ResultIndex.	Finds the value of a particular object in a Result table that matches a particular query. • For multiple rows in the Result table for a single query, the ResultIndex ranges from 1 to the value of cnnEouHostQueryRows.

Note Examples are not shown in the above table because the format differs depending on the software you are using.

MIB Query Correlating to the show eou ip Command

To build a MIB query that provides the same results as the **show eou ip** {*ip-address*}command, perform the following SNMP get operation.

SUMMARY STEPS

1. Set the cnnEouHostQueryStatus object to createandgo.
2. Set the cnnEouHostQueryIpAddrType object to “IPv4”.
3. Set the cnnEouHostQueryIpAddr object to IP address (for example, 10.2.3.4).
4. Set the cnnEouHostQueryStatus object to active.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Set the cnnEouHostQueryStatus object to createandgo.	Sets the query status.
Step 2	Set the cnnEouHostQueryIpAddrType object to “IPv4”.	Sets the address type. **Note** The only address type currently supported by NAC is IPv4.
Step 3	Set the cnnEouHostQueryIpAddr object to IP address (for example, 10.2.3.4).	Sets the IP address.
Step 4	Set the cnnEouHostQueryStatus object to active.	Indicates that you have finished building the query.

Note Examples are not shown in the previous table because the format differs depending on the software you are using.

Viewing MIB Query Results

After the MIB query has been built, the results can be viewed in cnnEouHostResultTable. For information about how to review the results, see the subsection Viewing MIB Query Results Correlating to the show eou all Command for more information.

If you are doing a MIB query that correlates to the **show eou all**command, there could possibly be as many as 2,000 rows of output. To ensure that you can view all the information in a MIB query, you can split the query into subqueries. For example, for a query having 2,000 rows of output, you could split the query into four subqueries to view the results in a page-by-page format. The first subquery would include rows 1 through 500 (the first 500 sessions); the second subquery would include rows 501 through 1,000; the third subquery would include rows 1,001 through 1,500; and the fourth subquery would include rows 1,501 through 2,000.

Note The cnnEouHostQueryTotalHosts object provides the total number of hosts (number of rows) that match a query criterion. By looking at this number, you can determine how many subqueries are necessary. However, you cannot get the cnnEouHostQueryTotalHosts object number until you have built your first query.

Build your query by performing the following steps.

SUMMARY STEPS

1. Set the cnnEouHostQueryStatus object to createandgo.
2. Set the cnnEouHostQueryMask object to 8.
3. Set cnnEouHostQueryRows to 500.
4. Set cnnEouHostQuerySkipNHosts to 0.
5. Set the cnnEouHostQueryStatus object to active.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Set the cnnEouHostQueryStatus object to createandgo.	Sets the query status.
Step 2	Set the cnnEouHostQueryMask object to 8.	Correlates to the default of the **show eou all** command.
Step 3	Set cnnEouHostQueryRows to 500.	Identifies the maximum number of rows to be built in the result table for this query.
Step 4	Set cnnEouHostQuerySkipNHosts to 0.	Corresponds to the result rows to be created.
Step 5	Set the cnnEouHostQueryStatus object to active.	Indicates that you have finished building the query.

Note Examples are not shown in the previous table because the format differs depending on the software you are using. The table is on the basis of a query having 2,000 sessions (rows).

- What to Do Next, page 23

What to Do Next

After the above task is performed, information for the first 500 hosts (rows) is queried. To view query information for the next 500 hosts (rows), perform the same five steps, with the exception of changing the cnnEouHostQuerySkipNHosts object value to 500 in Step 4. This task results in query information for rows 501 through 1000. In the same way, to obtain query information for the remaining hosts (through 2000), perform the same five steps again, with the exception of changing the cnnEouHostQuerySkipNHosts object values in Step 4 to 1000 and 1500, respectively.

Configuration Examples for Network Admission Control

Network Admission Control Example

The following output example shows that IP admission control has been configured on a Cisco IOS router:

```
Router# show running-config
Building configuration...

Current configuration: 1240 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
aaa new-model
!
!
aaa authentication eou default group radius
aaa session-id common
ip subnet-zero
ip cef
!
! The following line creates a network admission rule. A list is not specified; therefore,
! the rule intercepts all traffic on the applied interface.
ip admission name avrule eapoudp
!
eou logging
!
!
interface FastEthernet0/0
 ip address 10.13.11.106 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.255.255.0
 ip access-group 102 in
! The following line configures an IP admission control interface.
 ip admission avrule
 duplex auto
 speed auto
!
ip http server
no ip http secure-server
ip classless
!
!
! The following lines configure an interface access list that allows EAPoUDP traffic
! and blocks the rest of the traffic until it is validated.
access-list 102 permit udp any any eq 21862
access-list 102 deny   ip any any
!
!
! The following line configures RADIUS.
radius-server host 10.13.11.105 auth-port 1645 acct-port 1646 key cisco
!
control-plane
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
```

```
line vty 0 4
!
!
end
```

NAC MIB Output Examples

The following are examples of **show** command output displaying MIB object information.

show eou

The **show eou** command provides output for information that can also be viewed in various CISCO-NAC-NAD-MIB tables. The information that follows the **show eou** command can also be found in the cnnEouGlobalObjectsGroup table and the information that follows the **show eou all** command can be found in the cnnEouIfConfigTable.

```
Router# show eou
Global EAPoUDP Configuration
----------------------------
EAPoUDP Version     = 1
EAPoUDP Port        = 0x5566
Clientless Hosts    = Enabled
IP Station ID       = Disabled
Revalidation        = Enabled
Revalidation Period = 36000 Seconds
ReTransmit Period   = 3 Seconds
StatusQuery Period  = 300 Seconds
Hold Period         = 30 Seconds
AAA Timeout         = 60 Seconds
Max Retries         = 3
EAP Rate Limit      = 20
EAPoUDP Logging     = Enabled
Clientless Host Username = clientless
Clientless Host Password = clientless
Router# show eou all
Interface Specific EAPoUDP Configurations
-----------------------------------------
Interface Vlan333
AAA Timeout         = 60 Seconds
Max Retries         = 3
eou initialize interface {interface-name}
eou revalidate interface {interface-name}
```

show ip device tracking all

The **show ip device tracking all** command provides output for information that can also be found in the cnnIpDeviceTrackingObjectsGroup MIB table. The following is an example of such **show** command output:

```
Router# show ip device tracking all
IP Device Tracking = Enabled
Probe Count: 2
Probe Interval: 10
```

Additional References

Related Documents

Related Topic	Document Title
Configuring ACLs	IP Access List Overview feature module.
Authentication, authorization, and accounting	Authentication, Authorization, and Accounting section of *Cisco IOS Security Configuration Guide: Securing User Services*, Release 12.4T.
Interfaces, configuring	*Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.4T.
SNMP and SNMP get and set operations	

MIBs

MIBs	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Network Admission Control

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4 Feature Information for Network Admission Control

Feature Name	Releases	Feature Information
Network Admission Control	12.3(8)T	The Network Admission Control feature addresses the increased threat and impact of worms and viruses to networked businesses. This feature is part of the Cisco Self-Defending Network Initiative that helps customers identify, prevent, and adapt to security threats. In its initial phase, the Cisco Network Admission Control functionality enables Cisco routers to enforce access privileges when an endpoint attempts to connect to a network. The following commands were introduced or modified by this feature: **aaa authentication eou default enable group radius, access-group (identity policy), auth-type, clear eou, clear ip admission cache, debug eap, debug eou, debug ip admission eapoudp, description (identity policy), description (identity profile), device (identity profile), eou allow, eou clientless, eou default, eou initialize, eou logging, eou max-retry, eou port, eou rate-limit, eou revalidate, eou timeout, identity policy, identity profile eapoudp, ip admission, ip admission name, redirect (identity policy), show eou, show ip admission, template (identity policy).**
NAC MIB	12.4(15)T	Support was added for the CISCO-NAC-NAD-MIB. This MIB module is used to monitor and configure the NAD on the Cisco NAC system. The following commands were introduced or modified by this feature: **show ip device tracking**.

Feature Name	Releases	Feature Information
	12.2(33)SXI	This feature was integrated into Cisco IOS Release 12.2(33)SXI.

Glossary

default access policy-- Set of ACLs that are applied to a client device until its credentials are validated by the AAA server.

EAPoUDP-- Extensible Authentication Protocol over User Datagram Protocol. EAP is a framework that supports multiple, optional authentication mechanisms for PPP, including clear-text passwords, challenge-response, and arbitrary dialogue sequences. UDP is a connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, and it requires that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

ip admission rule --Named rule that defines how IP admission control is applied. The IP admission rule is associated with an Intercept ACL and provides control over which hosts can use the IP admission feature. To create an IP admission control rule, use the ip admission name command.

posture token --Status that is used to convey the result of the evaluation of posture credentials. The AAA server maps the posture token (its status can be Healthy, Checkup, Quarantine, Infected, or Unknown) to a network access policy (ACL, URL, redirect, or status query timer) for the peer that the client wants to reach.

NAC-Auth Fail Open

In network admission control (NAC) deployments, authentication, authorization, and accounting (AAA) servers validate the antivirus status of clients before granting network access. This process is called posture validation. If the AAA server is unreachable, clients do not have access to the network. The NAC--Auth Fail Open feature enables the administrator to apply a policy that allows users to have network access when the AAA server is unreachable. The administrator can configure a global policy that applies to a device, or a rule-based policy that applies to a specific interface.

When the AAA server returns to a reachable status, the posture validation process resumes for clients that are using the NAC--Auth Fail Open policy.

Prerequisites for NAC-Auth Fail Open

You can configure this feature in networks using NAC and an AAA server for security. NAC is implemented on Cisco IOS routers running Cisco IOS Release 12.3(8)T or a later release.

Restrictions for NAC-Auth Fail Open

To apply local policies to a device or an interface when the AAA server is unreachable, you must configure the **aaa authorization network default local** command.

Information About Network Admission Control

Controlling Admission to a Network

NAC protects networks from endpoint devices or clients (such as PCs or servers) that are infected with viruses by enforcing access control policies that prevent infected devices from adversely affecting the network. It checks the antivirus condition (called *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.

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

Posture validation consists of the following actions:

- Checking the antivirus condition or credentials of the client.
- Evaluating the security posture credentials from the network client.
- Providing the appropriate network access policy to the NAD based on the system posture.

Network Admission Control When the AAA Server Is Unreachable

Typical deployments of NAC use a AAA server to validate the client posture and to pass policies to the NAD. If the AAA server is not reachable when the posture validation occurs, the typical response is to deny network access. Using NAC--Auth Fail Open, an administrator can configure a default policy that allows the host at least limited network access while the AAA server is unreachable.

This policy offers these two advantages:

- While AAA is unavailable, the host continues to have connectivity to the network, although it may be restricted.
- When the AAA server is once again reachable, users can be validated again, and their policies can be downloaded from the access control server (ACS).

Note When the AAA server is unreachable, the NAC--Auth Fail Open policy is applied only when there is no existing policy associated with the host. Typically, when the AAA server becomes unreachable during revalidation, the policies already in effect for the host are retained.

How to Configure NAC-Auth Fail Open

You can configure NAC--Auth Fail Open policies per interface, or globally for a device. Configuring NAC--Auth Fail Open is optional, and includes the following tasks:

- Enabling EOU Logging, page 39

Configuring a NAC Rule-Associated Policy Globally for a Device

This task creates a NAC rule and associates a policy to be applied while the AAA server is unreachable. You can apply a policy globally to all interfaces on a network access device, if you want to provide the same level of network access to all users who access that device.

An AAA server must be configured and NAC must be implemented on the NAD.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission name** *admission-name* [**eapoudp** [**bypass**] | **proxy** {**ftp** | **http** | **telnet**} | **service-policy type tag** {*service-policy-name* }] [**list** {*acl* | *acl-name* }] [**event**] [**timeout aaa**] [**policy identity** {*identity-policy-name* }]
4. **ip admission** *admission-name [* **event timeout aaa policy identity** *identity-policy-name]*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip admission name** *admission-name* [**eapoudp** [**bypass**]	**proxy** {**ftp**	**http**	**telnet**}	**service-policy type tag** {*service-policy-name* }] [**list** {*acl*	*acl-name* }] [**event**] [**timeout aaa**] [**policy identity** {*identity-policy-name* }] **Example:** `Router (config)# ip admission name greentree event timeout aaa policy identity aaa-down`	(Optional) Configures a rule-specific policy globally for the device. If a rule is configured, then it is applied instead of any other global event timeout policy configured on the device. To remove a rule that was applied globally to the device, use the **no** form of thecommand.

	Command or Action	Purpose
Step 4	**ip admission** *admission-name [* **event timeout aaa policy identity** *identity-policy-name]* **Example:** `Router (config)# ip admission event timeout aaa policy identity AAA_DOWN`	(Optional) Configures the specified IP NAC policy globally for the device. To remove IP NAC policy that was applied to the device, use the **no** form of thecommand. **Note** This policy applies only if no rule-specific policy is configured.
Step 5	**end** **Example:** `Router (config)# end`	Exits the global configuration mode.

Applying a NAC Policy to a Specific Interface

An IP admission rule with NAC--Auth Fail Open policies can be attached to an interface. This task attaches a NAC--Auth Fail Open policy to a rule, and applies the rule to a specified interface on a device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip access-group** {*access-list-number* | *name*} **in**
5. **ip admission** *admission-name*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *interface-id* **Example:** `Router (config)# interface fastEthernet 2/1`	Enters interface configuration mode.
Step 4	**ip access-group** {*access-list-number* | *name*} **in** **Example:** `Router (config-if)# ip access-group ACL15 in`	Controls access to the specified interface.
Step 5	**ip admission** *admission-name* **Example:** `Router (config-if)# ip admission AAA_DOWN`	Attaches the globally configured IP admission rule to the specified interface(s). To remove the rule on the interface, use the **no** form of the command.
Step 6	**exit** **Example:** `Router (config)# exit`	Returns to global configuration mode.

Configuring Authentication and Authorization Methods

This task configures the authentication and authorization methods for the device. The access granted using these methods remain in effect for users who attempt reauthorization while the AAA server is unavailable. These methods must be configured before you configure any policy to be applied to users who try to access the network when the AAA server is unreachable.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication eou default group radius**
5. **aaa authorization network default local**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router (config)# aaa new-model`	Enables AAA.
Step 4	**aaa authentication eou default group radius** **Example:** `Router (config)# aaa authentication eou default group radius`	Sets authentication methods for Extensible Authorization Protocol over User Datagram Protocol (EAPoUDP). To remove the EAPoUDP authentication methods, use the use the **no** form of the command.
Step 5	**aaa authorization network default local** **Example:** `Router (config)# aaa authorization network default local`	Sets the authorization method to local. To remove the authorization method, use the **no** form of the command.

Configuring RADIUS Server Parameters

Identifying the RADIUS Server

A RADIUS server can be identified by:

- hostname
- IP address
- hostname and a specific UDP port number

- IP address and a specific UDP port number

The combination of the RADIUS server IP address and a specific UDP port number creates a unique identifier, which enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service--for example, authentication--the second host entry configured acts as the backup to the first one. The RADIUS host entries are tried in the order that they were configured.

Determining When the RADIUS Server Is Unavailable

Because the NAC--Auth Fail Open feature applies a local policy when the RADIUS server is unavailable, you should configure “dead criteria” that identify when the RADIUS server is unavailable. There are two configurable dead criteria:

- time--the interval (in seconds) without a response to a request for AAA service
- tries--the number of consecutive AAA service requests without a response

If you do not configure the dead criteria, they are calculated dynamically, based on the server configuration and the number of requests being sent to the server.

You can also configure the number of minutes to wait before attempting to resume communication with a RADIUS server after it has been defined as unavailable.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server dead-criteria [time** *seconds]* **[tries** *number-of- tries]*
4. **radius-server deadtime** *minutes*
5. **radius-server host** *ip-address* **[acct-port** *udp-port*] [**auth-port***udp-port*] [**key***string*] [**test username***name* [**idle-time***time*]
6. **radius-server attribute 8 include-in-access-req**
7. **radius-server vsa send authentication**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**radius-server dead-criteria [time** *seconds]* **[tries** *number-of- tries]* **Example:** `Router (config)# radius-server dead-criteria time 30 tries 20` **Example:**	(Optional) Sets the conditions that are used to decide when a RADIUS server is considered unavailable or *dead* . • The range for *seconds* is from 1 to 120 seconds. The default is that the NAD dynamically determines the *seconds* value within a range from 10 to 60 seconds. • The range for *number-of-tries* is from 1 to 100. The default is that the NAD dynamically determines the *number-of-tries* parameter within a range from 10 to 100.
Step 4	**radius-server deadtime** *minutes* **Example:** `Router (config)# radius-server deadtime 60`	(Optional) Sets the number of minutes that a RADIUS server is not sent requests after it is found to be dead. The range is from 0 to 1440 minutes (24 hours). The default is 0 minutes.

	Command or Action	Purpose
Step 5	**radius-server host** *ip-address* **[acct-port** *udp-port*] [**auth-port***udp-port*] [**key***string*] [**test username***name* [**idle-time***time*] **Example:** `Router (config)# radius-server host 10.0.0.2 acct-port 1550 auth-port 1560 test username user1 idle-time 30 key abc1234` **Example:**	(Optional) Configures the RADIUS server parameters by using these keywords: • **acct-port** *udp-port*-- Specifies the UDP port for the RADIUS accounting server. The range for the UDP port number is from 0 to 65536. The default is 1646. If the port number is set to 0, the host is not used for accounting. • **auth-port** *udp-port*-- Specifies the UDP port for the RADIUS authentication server. The range for the UDP port number is from 0 to 65536. The default is 1645. If the port number is set to 0, the host is not used for authentication. **Note** You should configure the UDP port for the RADIUS accounting server and the UDP port for the RADIUS authentication server to nondefault values. • **key** *string*-- Specifies the authentication and encryption key for all RADIUS communication between the NAD and the RADIUS daemon. **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** *name* -- Enables automated testing of the RADIUS server status, and specify the username to be used. • **idle-time** *time*-- Sets the interval of time in minutes after which the NAD sends test packets to the server. The range is from 1 to 35791 minutes. The default is 60 minutes (1 hour). To configure multiple RADIUS servers, reenter this command.
Step 6	**radius-server attribute 8 include-in-access-req** **Example:** `Router (config)# radius-server attribute 8 include-in-access-req`	If the device is connected to nonresponsive hosts, configures the device to send the Framed-IP-Address RADIUS attribute (attribute[8]) in access-request or accounting-request packets. To configure the device to not send the Framed-IP-Address attribute, use the **no radius-server attribute 8 include-in-access-req** global configuration command.
Step 7	**radius-server vsa send authentication** **Example:** `Router (config)# radius-server vsa send authentication`	Configures the network access server to recognize and use vendor-specific attributes (VSAs).

	Command or Action	Purpose
Step 8	**end** **Example:** `Router (config)# end`	Returns to privileged EXEC mode.

Displaying the Status of Configured AAA Servers

This task displays the status of the AAA servers you have configured for the device.

SUMMARY STEPS

1. **enable**
2. **show aaa servers**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show aaa servers** **Example:** `Router# show aaa servers`	Displays the status of the AAA servers configured for the device.

Displaying the NAC Configuration

This task displays the current NAC configuration for the device.

SUMMARY STEPS

1. **enable**
2. **show ip admission configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip admission configuration** **Example:** `Router#` **show ip admission configuration**	Displays all the IP admission control rules configured for the device.

Displaying the EAPoUDP Configuration

This task displays information about the current EAPoUDP configuration for the device, including any NAC--Auth Fail Open policies in effect.

SUMMARY STEPS

1. **enable**
2. **show eou ip 10.0.0.1**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show eou ip 10.0.0.1** **Example:** `Router#` **show eou ip 10.0.0.1**	Displays information about the EAPoUDP configuration for the specified interface.

Enabling EOU Logging

A set of new system logs is included in Cisco IOS Release 12.4(11)T. These new logs track the status of the servers defined by the methodlist, and the NAC Auth Fail policy configuration. You should enable EOU logging to generate syslog messages that notify you when the AAA servers defined by the methodlist are unavailable, and display the configuration of the NAC--Auth Fail Open policy. The display shows

whether a global or rule-specific policy is configured for the NAD or interface. If no policy is configured, the existing policy is retained.

This task enables EOU logging.

SUMMARY STEPS

1. **configure terminal**
2. **eou logging**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router#` **configure terminal**	Enters global configuration mode.
Step 2	**eou logging** **Example:** `Router (config) #` **eou logging**	Enables EOU logging.

Configuration Examples for NAC-Auth Fail Open

Sample NAC-Auth Fail Open Configuration Example

The example below shows how to configure the NAC--Auth Fail Open feature:

```
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
```

Sample RADIUS Server Configuration Example

The example below shows that the RADIUS server is considered unreachable after 3 unsuccessful tries:

```
Switch(config)# radius-server host 10.0.0.4 test username administrator idle-time 1 key
sample
Switch(config)# radius-server dead-criteria tries 3
Switch(config)# radius-server deadtime 30
Switch(config)# radius-server vsa send authentication
Switch(config)# radius-server attribute 8 include-in-access-req
Switch(config)# int fastEthernet 2/1
3
Switch(config-if)# ip admission AAA_DOWN
Switch(config-if)# exit
```

show ip admission configuration Output Example

The following example shows that a policy called “global policy” has been configured for use when the AAA server is unreachable:

```
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
```

show eou Output Example

The example below shows the configuration of the AAA servers defined for a NAC--Auth Fail policy configuration:

```
Router# show eou ip 10.0.0.1


Address : 10.0.0.1
MAC Address : 0001.027c.f364
Interface : Vlan333
! Authtype is show as AAA DOWN when in AAA is not reachable.
AuthType : AAA DOWN
! AAA Down policy name:
AAA Down policy : rule_policy
Audit Session ID : 00000000011C11830000000311000001
PostureToken : -------
Age(min) : 0
URL Redirect : NO URL REDIRECT
URL Redirect ACL : NO URL REDIRECT ACL
ACL Name : rule_acl
Tag Name : NO TAG NAME
User Name : UNKNOWN USER
Revalidation Period : 500 Seconds
Status Query Period : 300 Seconds
Current State : AAA DOWN
```

show aaa servers Output Example

The example below shows sample status information for a configured AAA server:

```
Switch# show aaa servers
RADIUS: id 1, priority 1, host 10.0.0.4, 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: 2h13mS
```

EOU Logging Output Example

The example below shows the display when EOU logging is enabled:

```
Router (config)# eou
 logging
EOU-5-AAA_DOWN: AAA unreachable.
METHODLIST=Default| HOST=17.0.0.1| POLICY=Existing policy retained.
EOU-5-AAA_DOWN: AAA unreachable.
METHODLIST=Default| HOST=17.0.0.1| POLICY=aaa_unreachable_policy
```

Additional References

Related Documents

Related Topic	Document Title
Configuring NAC	Network Admission Control module.
Security commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
IEEE 802.1x	IEEE Standard 802.1X - 2004 Port-Based Network Access Control

MIBs

MIB	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for NAC-Auth Fail Open

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5 Feature Information for NAC--Auth Fail Open

Feature Name	Releases	Feature Information
NAC--Auth Fail Open	12.3(8)T	In network admission control (NAC) deployments, authentication, authorization, and accounting (AAA) servers validate the antivirus status of clients before granting network access. This process is called posture validation. If the AAA server is unreachable, clients do not have access to the network. The NAC--Auth Fail Open feature enables the administrator to apply a policy that allows users to have network access when the AAA server is unreachable. The administrator can configure a global policy that applies to a device, or a rule-based policy that applies to a specific interface. When the AAA server returns to a reachable status, the posture validation process resumes for clients that are using the NAC--Auth Fail Open policy. This feature was introduced in Cisco IOS Release 12.3(8)T. The following commands were introduced or modified: **ip admission**, **ip admission name**, **show eou**, **show ip admission**

Network Admission Control Agentless Host Support

The Network Admission Control: Agentless Host Support feature allows for an exhaustive examination of agentless hosts (hosts that are not running the Cisco Trust Agent software). This examination allows customers to build a robust host or examination functionality by integrating any third-party audit mechanisms into the Network Admission Control architecture.

This feature also allows for Extensible Authentication Protocol over UDP (EAPoUDP) bypass, which speeds up the posture validation of hosts that are not using Cisco Trust Agent.

Prerequisites for Network Admission Control Agentless Host Support

- You must be running Cisco IOS Release 12.4(6)T or a later release.
- You must be using a Cisco access control server (ACS) version 4.0 or a later version.
- You must have a Cisco or third-party audit server setup.

Information About Network Admission Control Agentless Host Support

Network Admission Control

The Cisco Network Admission Control functionality enables the credentials of the endpoint device to be checked for compliance with the security policy before the device is granted access to network resources. This checking requires a security application called Cisco Trust Agent (CTA) to be installed on end devices that gather security state information and communicate it to access servers where policy decisions are made and eventually enforced on Cisco network access devices (such as routers and switches).

Agentless Hosts

End devices that do not run CTA cannot provide credentials when challenged by network access devices (NADs). Such hosts are termed “agentless” or “nonresponsive.” In the Phase l release of Network Admission Control, agentless hosts were supported by either a static configuration using exception lists (an identity profile) or by using “clientless” username and password authentication on an ACS. These methods are restrictive and do not convey any specific information about the host while making policy decisions.

EAPoUDP Bypass

You can use the EAPoUDP Bypass feature to reduce latency of the validation of hosts that are not using CTA. If EAPoUDP bypass is enabled, the NAD does not contact the host to request the antivirus condition (the NAD does not try to establish an EAPoUDP association with the host if the EAPoUDP Bypass option is configured). Instead, the NAD 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 NAD.

If EAPoUDP bypass is enabled, the NAD sends an agentless host request to the Cisco Secure ACS and applies the access policy from the server to the host.

If EAPoUDP bypass is enabled and the host uses the Cisco Trust Agent, the NAD also sends a nonresponsive-host request to the Cisco Secure ACS and applies the access policy from the server to the host.

Vendor-Specific Attributes for This Feature

The following new attributes are supported for various RADIUS message exchanges:

- audit-session-id, page 46
- url-redirect-acl, page 46

audit-session-id

The audit-session-id vendor-specific attribute (VSA) is a 32-byte string that uniquely identifies a host session. This identifier is generated by a NAD when the host is detected, and it remains the same until the session is deleted. Session revalidation or reinitialization does not change this identifier. Every time a session is detected, a new identifier is generated. This attribute is included in access requests to the authentication, authorization, and accounting (AAA) server and in web requests to the audit server. The value of this attribute is displayed in **show eou** command output (using the **ip** keyword).

url-redirect-acl

The url-redirect-acl VSA string specifies the name of the access control list (ACL) for URL redirection. Any ingress HTTP from the host that matches the access list that is specified by this attribute is subjected to

redirection to the URL address specified by the url-redirect VSA. The access list specified in this attribute has to be locally configured on the NAD as an “ip access-list extended” named ACL. This attribute is specified only in RADIUS access-accept messages. The value of the url-redirect-acl attribute is displayed using the **show eou** command (with the **ip** keyword).

Note Phase 1 of the Network Admission Control feature introduced the url-redirect VSA that allowed the HTTP sessions of users to be redirected to the address specified by the url-redirect VSA. This redirection is useful if you want to remediate hosts that do not comply to network security policy. However, to determine to which users HTTP requests are to be redirected, Phase 1 of Network Admission Control assumed that any HTTP traffic that was intercepted and denied by the host policy ACL (the access control server ACL) was subjected to redirection. The url-redirect-acl VSA provides an option so that users can customize the redirect criteria. The url-redirect-acl VSA supports backward compatibility. If the url-redirect-acl is specified in the access-accept message for the host, any user HTTP sessions that match the ACL are subjected to redirection. However, if the url-redirect-acl attribute is not received, the Phase 1 logic to perform redirection is used. The Phase 1 logic to perform redirection applies only to Cisco IOS routers. The url-redirect-acl attribute is mandatory for Cisco IOS switches.

How to Configure Network Admission Control Agentless Host Support

Configuring a NAD to Bypass EAPoUDP Communication

To configure a NAD to bypass EAPoUDP, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission name** *admission-name* **eapoudp bypass**
4. **eou allow clientless**
5. **interface type** *slot* / *port*
6. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip admission name** *admission-name* **eapoudp bypass** **Example:** `Router (config)# ip admission name greentree eapoudp bypass`	The IP network admission control rule bypasses EAPoUDP communication.
Step 4	**eou allow clientless** **Example:** `Router (config)# eou allow clientless`	Allows authentication of clientless hosts (systems that do not run Cisco Trust Agent).
Step 5	**interface type** *slot* / *port* **Example:** `Router (config)# interface ethernet 2/4`	Configures an interface type and enters interface configuration mode.
Step 6	end **Example:** `Router (config-if)# end`	Exits configuration modes.

Verifying Agentless Host and EAPoUDP Bypass

To verify your configuration for Agentless Host and EOUoUDP Bypass, perform the following steps. The **debug** and **show**commands can be used independently of each other.

SUMMARY STEPS

1. **enable**
2. **debug eou**
3. **show eou ip** *ip-address*
4. **show ip admission configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug eou** **Example:** `Router# debug eou`	Displays information about EAUoUDP.
Step 3	**show eou ip** *ip-address* **Example:** `Router# show eou ip 10.0.0.0`	Displays information about EAPoUDP global values or EAPoUDP session cache entries.
Step 4	**show ip admission configuration** **Example:** `Router# show ip admission configuration`	Displays information about the agentless and EAPoUDP Bypass configuration.

Configuration Examples for Network Admission Control Agentless Host Support

RADIUS Message Exchange url-redirect-acl VSA Example

ACS Configuration

```
url-redirect=http://audit-server.com/host_session_id=$host_session_id
url-redirect-acl=RedirectACL
```

NAD Configuration

```
Router(config)# ip access-list extended RedirectACL
Router (config-ext-nacl)# permit tcp any 10.0.0.0 0.0.0.255 eq www
Router (config-ext-nacl)# end
```

Show Output Displaying the Value of a Newly Defined VSA

The following **show eou** command output displays EAPoUPD session cache information for a given IP address. The value of the newly defined VSA is also shown.

```
Router# show eou ip 10.0.0.1
Address              : 10.0.0.1
MAC Address          : 0001.027c.f364
Interface            : FastEthernet1/0/3
AuthType             : EAP
Audit Session ID     : 000000001C8A6A330000001812000001
PostureToken         : Infected
Age(min)             : 444
URL Redirect         : http://wwwin.cisco.com
URL Redirect ACL     : RedirectACL
ACL Name             : #ACSACL#-IP-Infected-42835ff7
User Name            : NAC-DEV-PC-3:Administrator
Revalidation Period  : 30000 Seconds
Status Query Period  : 300 Seconds
Current State        : AUTHENTICATED
```

Additional References

Related Documents

Related Topic	Document Title
Configuring AAA and RADIUS for EAPoUDP	Network Admission Control feature module
Network Admission Control	
Security commands	*Cisco IOS Security Command Reference*

MIBs

MIB	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Network Admission Control Agentless Host Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 6 Feature Information for Network Admission Control: Agentless Host Support

Feature Name	Releases	Feature Information
Network Admission Control: Agentless Host Support	12.4(6)T	The Network Admission Control: Agentless Host Support feature allows for an exhaustive examination of agentless hosts (hosts that are not running the Cisco Trust Agent software). This examination allows customers to build a robust host or examination functionality by integrating any third-party audit mechanisms into the Network Admission Control architecture. This feature also allows for Extensible Authentication Protocol over UDP (EAPoUDP) bypass, which speeds up the posture validation of hosts that are not using Cisco Trust Agent. This feature was introduced in Cisco IOS Release 12.4(6)T. The following commands were introduced or modified: **eou clientless**, **ip admission name**, **show eou**