802.1X Authentication Services Configuration Guide Cisco IOS Release 12.4T

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

Configuring IEEE 802.1X Port-Based Authentication

This document describes how to configure IEEE 802.1X port-based authentication on Cisco integrated services routers (ISRs). IEEE 802.1X authentication prevents unauthorized devices (supplicants) from gaining access to the network.

Cisco ISRs can combine the functions of a router, a switch, and an access point, depending on the fixed configuration or installed modules. The switch functions are provided by either built in switch ports or a plug-in module with switch ports.

Note This document describes IEEE 802.1X security features available only on the switch ports in a Cisco ISR.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Prerequisites for Configuring IEEE 802.1X Port-Based Authentication

The features described in this document are available only on switch ports installed in Cisco ISR routers. The IEEE 802.1X port-based authentication features are available in Cisco IOS Release 12.4(11)T on Cisco 800, 870, 1800, 2800, and 3800 series ISRs that support switch ports.

The fixed configuration Cisco 1800 series router platforms and the Cisco 870 series routers have integrated 4-port and 8-port switches.

The following cards or modules support switch ports:

- High-speed WAN interface cards (HWIC)
  - HWIC-4ESW
  - HWICD-9ESW
- EtherSwitch Network Modules
  - NM-16ESW
  - NMD-36ESW

Note Not all Cisco ISR routers support all the components listed. For information about module compatibility with a specific router platform, see Cisco EtherSwitch Modules Comparison .

To determine whether your router has switch ports that can be configured with the IEEE 802.1X port-based authentication feature, use the **show interfaces switchport**command.

To configure IEEE 802.1X port-based authentication, you must enable authentication, authorization, and accounting (AAA) and specify the authentication method list. A method list describes the sequence and authentication method to be queried to authenticate a user.

Restrictions for Configuring IEEE 802.1X Port-Based Authentication

IEEE 802.1X Authentication Configuration Restrictions

- When IEEE 802.1X authentication is enabled, ports are authenticated before any other Layer 2 or Layer 3 features are enabled.
- If you try to change the mode (for example, from access to trunk) of an IEEE 802.1X-enabled port, an error message appears, and the port mode is not changed.
- If the VLAN to which an IEEE 802.1X-enabled port is assigned changes, this change is transparent and does not affect the switch port. For example, this change occurs if a port is assigned to a RADIUS server-assigned VLAN and is then assigned to a different VLAN after reauthentication.

If the VLAN to which an IEEE 802.1X port is assigned is shut down, disabled, or removed, the port becomes unauthorized. For example, the port is unauthorized after the access VLAN to which a port is assigned shuts down or is removed.

- The IEEE 802.1X protocol is supported on Layer 2 static-access ports, voice VLAN enabled ports, and Layer 3 routed ports, but it is not supported on these port types:
  - Dynamic-access ports--If you try to enable IEEE 802.1X authentication on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and IEEE 802.1X authentication is not enabled. If you try to change an IEEE 802.1X-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
  - Dynamic ports--If you try to enable IEEE 802.1X authentication on a dynamic port, an error message appears, and IEEE 802.1X authentication is not enabled. If you try to change the mode of an IEEE 802.1X-enabled port to dynamic, an error message appears, and the port mode is not changed.
  - Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) destination ports--You can enable IEEE 802.1X authentication on a port that is a SPAN or RSPAN destination port. However, IEEE 802.1X authentication is disabled until the port is removed as a SPAN or RSPAN destination port. You can enable IEEE 802.1X authentication on a SPAN or RSPAN source port.
  - Trunk port--If you try to enable IEEE 802.1X authentication on a trunk port, an error message appears, and IEEE 802.1X authentication is not enabled. If you try to change the mode of an IEEE 802.1X-enabled port to trunk, an error message appears, and the port mode is not changed.

Note A port in dynamic mode can negotiate with its neighbor to become a trunk port.

VLAN Assignment Configuration Restrictions

- When IEEE 802.1X authentication is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.

Guest VLAN Configuration Restrictions

- You can configure any VLAN except an RSPAN VLAN or a voice VLAN as an IEEE 802.1X guest VLAN. The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.
- After you configure a guest VLAN for an IEEE 802.1X port to which a DHCP client is connected, you might have to get a host IP address from a DHCP server. You can change the settings for restarting the IEEE 802.1X authentication process on the switch before the DHCP process on the client times out and tries to get a host IP address from the DHCP server. Decrease the settings for the IEEE 802.1X authentication process (using the **dot1x max-reauth-req** and **dot1x timeout tx-period** interface configuration commands). The amount of decrease depends on the connected IEEE 802.1X client type.

Upgrading from a Previous Software Release

In Cisco IOS Release 12.4(11)T, the implementation for IEEE 802.1X authentication changed from the previous releases. When IEEE 802.1X authentication is enabled, information about Port Fast is no longer added to the configuration.

Note When you enter any IEEE 802.1X-related commands on a port, this information is automatically added to the running configuration to address any backward compatibility issues: dot1xpae authenticator

Information About IEEE 802.1X Port-Based Authentication

Note This section describes IEEE 802.1X security features available only on the switch ports in a Cisco ISR.

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that prevents unauthorized clients from connecting to a LAN through publicly accessible ports unless they are properly authenticated. The authentication server authenticates each client connected to a port before making available any services offered by the device or the network.

Until the client is authenticated, IEEE 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

- IEEE 802.1X Authenticator, page 4
- IEEE 802.1X with RADIUS Accounting, page 10

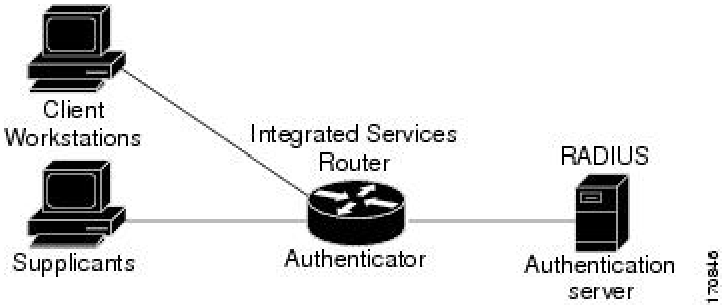
IEEE 802.1X Authenticator

- Device Roles, page 4
- Authentication Initiation and Message Exchange, page 5
- Authentication Process, page 6
- IEEE 802.1X Host Mode, page 7
- IEEE 802.1X Authentication with Guest VLAN, page 7
- IEEE 802.1X--Common Session ID, page 8
- Ports in Authorized and Unauthorized States, page 8
- Troubleshooting and IEEE 802.1X--Conditional Logging, page 9

Device Roles

With IEEE 802.1X port-based authentication, the devices in the network have specific roles as shown in the figure below.

Figure 1 IEEE 802.1X Device Roles



- *Supplicant* --Device (workstation) that requests access to the LAN and switch services and responds to requests from the router. The workstation must be running IEEE 802.1X-compliant client software such as that offered in the Microsoft Windows XP operating system. (The *supplicant* is sometimes called the client.)

Note To resolve Windows XP network connectivity and IEEE 802.1X authentication issues, read the Microsoft Knowledge Base article at this URL: http://support.microsoft.com/kb/q303597/

- *Authentication server* --Device that performs the actual authentication of the supplicant. The authentication server validates the identity of the supplicant and notifies the router whether or not the supplicant is authorized to access the LAN and switch services. The Network Access Device (or ISR router in this instance) transparently passes the authentication messages between the supplicant and the authentication server, and the authentication process is carried out between the supplicant and the authentication server. The particular EAP method used will be decided between the supplicant and the authentication server (RADIUS server). The RADIUS security system with EAP extensions is available in Cisco Secure Access Control Server Version 3.0 or later. RADIUS operates in a client and server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.
- *Authenticator (integrated services router (* ISR) or wireless access point)--Router that controls the physical access to the network based on the authentication status of the supplicant. The router acts as an intermediary between the supplicant and the authentication server, requesting identity information from the supplicant, verifying that information with the authentication server, and relaying a response to the supplicant. The router includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server.

When the authenticator receives EAPOL frames and relays them to the authentication server, the EAPOL is stripped and the remaining EAP frame is reencapsulated in the RADIUS format. The EAP frames are not modified during encapsulation, and the authentication server must support EAP within the native frame format. When the authenticator receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

Authentication Initiation and Message Exchange

During IEEE 802.1X authentication, the router or the supplicant can initiate authentication. If you enable authentication on a port by using the **dot1x port-control auto** interface configuration command, the router initiates authentication when the link state changes from down to up or periodically if the port remains up and unauthenticated. The router sends an EAP-request/identity frame to the supplicant to request its identity. Upon receipt of the frame, the supplicant responds with an EAP-response/identity frame.

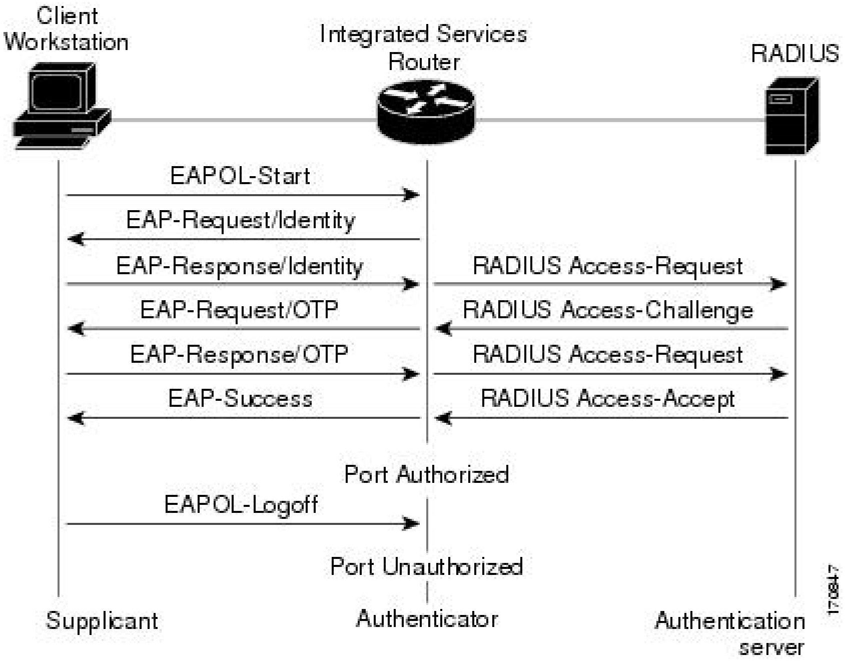
However, if during bootup, the supplicant does not receive an EAP-request/identity frame from the router, the supplicant can initiate authentication by sending an EAPOL-start frame, which prompts the router to request the supplicant's identity.

Note If IEEE 802.1X authentication is not enabled or supported on the network access device, any EAPOL frames from the supplicant are dropped. If the supplicant does not receive an EAP-request/identity frame after three attempts to start authentication, the supplicant sends frames as if the port is in the authorized state. A port in the authorized state effectively means that the supplicant has been successfully authenticated. For more information, see the Ports in Authorized and Unauthorized States module.

When the supplicant supplies its identity, the router begins its role as the intermediary, passing EAP frames between the supplicant and the authentication server until authentication succeeds or fails. If the authentication succeeds, the router port becomes authorized. If the authentication fails, authentication can be retried, the port might be assigned to a VLAN that provides limited services, or network access is not granted. For more information, see the Ports in Authorized and Unauthorized States module.

The specific exchange of EAP frames depends on the authentication method being used. The figure below shows a message exchange initiated by the supplicant using the One-Time-Password (OTP) authentication method with a RADIUS server.

Figure 2 Message Exchange



Authentication Process

To configure IEEE 802.1X port-based authentication, you must enable authentication, authorization, and accounting (AAA) and specify the authentication method list. A method list describes the sequence and authentication method to be queried to authenticate a user.

The AAA process begins with authentication. When IEEE 802.1X port-based authentication is enabled and the device attempting to authenticate is IEEE 802.1x-capable (meaning it supports the supplicant functionality) these events occur:

- If the supplicant identity is valid and the IEEE 802.1X authentication succeeds, the router grants the supplicant access to the network.

The router reauthenticates a supplicant when one of these situations occurs:

- Periodic reauthentication is enabled, and the reauthentication timer expires.

You can configure the reauthentication timer to use a router-specific value or to be based on values from the RADIUS server.

After IEEE 802.1X authentication using a RADIUS server is configured, the router uses timers based on the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute [29]).

The Session-Timeout RADIUS attribute (Attribute[27]) specifies the time after which reauthentication occurs.

The Termination-Action RADIUS attribute (Attribute [29]) specifies the action to take during reauthentication. The actions can be *Initialize* or *ReAuthenticate* . When the *Initialize* action is set (the attribute value is *DEFAULT*), the IEEE 802.1x session ends, and connectivity is lost during reauthentication. When the *ReAuthenticate* action is set (the attribute value is RADIUS-Request), the session is not affected during reauthentication.

- You manually reauthenticate the supplicant by entering the **dot1x re-authenticate interface***interface-id* privileged EXEC command.

IEEE 802.1X Host Mode

Note This section describes IEEE 802.1X security features available only on the switch ports in a Cisco ISR.

You can configure an IEEE 802.1X port for single-host or for multi-host mode. In single-host mode (see the figure IEEE 802.1X Device Roles in the Device Roles section of this module), only one supplicant can be authenticated by the IEEE 802.1X-enabled switch port. The router detects the supplicant by sending an EAPOL frame when the port link state changes to the up state. If a supplicant leaves or is replaced with another supplicant, the router changes the port link state to down, and the port returns to the unauthorized state.

In multi-host mode, you can attach multiple hosts to a single IEEE 802.1X-enabled port. In this mode, only one of the attached supplicants must be authorized for all supplicants to be granted network access. If the port becomes unauthorized (reauthentication fails or an EAPOL-logoff message is received), the router denies network access to all of the attached supplicants.

Note Cisco 870 series platforms do not support single-host mode.

IEEE 802.1X Authentication with Guest VLAN

You can configure a guest VLAN for each IEEE 802.1X-capable switch port on the router to provide limited services to clients, such as downloading the IEEE 802.1X client. These clients might be upgrading their system for IEEE 802.1X authentication, and some hosts, such as Windows 98 systems, might not be IEEE 802.1X-capable.

When you enable a guest VLAN on an IEEE 802.1X port, the router assigns clients to a guest VLAN when the router does not receive a response to its EAP request/identity frame or when EAPOL packets are not sent by the client.

The router maintains the EAPOL packet history. If an EAPOL packet is detected on the interface during the lifetime of the link, the router determines that the device connected to that interface is an IEEE 802.1X-capable client, and the interface does not change to the guest VLAN state. EAPOL history is cleared if the interface link status goes down. If no EAPOL packet is detected on the interface, the interface changes to the guest VLAN state.

In Cisco IOS Release 12.4(11)T and later releases, if devices send EAPOL packets to the router during the lifetime of the link, the router does not allow clients that fail authentication access to the guest VLAN.

Note If an EAPOL packet is detected after the interface has changed to the guest VLAN, the interface reverts to an unauthorized state, and IEEE 802.1X authentication restarts.

Any number of IEEE 802.1X-incapable clients are allowed access when the router port is moved to the guest VLAN. If an IEEE 802.1X-capable client joins the same port on which the guest VLAN is configured, the port is put into the unauthorized state in the user-configured access VLAN, and authentication is restarted.

Note Guest VLANs are supported on IEEE 802.1X ports in single-host or multi-host mode.

IEEE 802.1X--Common Session ID

Authentication manager uses a single session ID (referred to as a common session ID) for a client no matter which authentication method is used. This ID is used for all reporting purposes, such as the show commands and MIBs. The session ID appears with all per-session syslog messages.

The session ID includes:

- The IP address of the Network Access Device (NAD).
- A monotonically increasing unique 32 bit integer.
- The session start time stamp (a 32 bit integer).

This example shows how the session ID appears in the output of the **show authentication** command. The session ID in this example is 160000050000000B288508E5:

```
Switch# show authentication sessions

Interface MAC Address    Method Domain Status        Session ID
Fa4/0/4   0000.0000.0203 mab    DATA   Authz Success 160000050000000B288508E5
```

This is an example of how the session ID appears in the syslog output. The session ID in this example is also160000050000000B288508E5:

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

The session ID is used by the NAD, the AAA server, and other report-analyzing applications to identify the client. The ID appears automatically. No configuration is required.

Ports in Authorized and Unauthorized States

During IEEE 802.1X authentication, depending on the port state, the router can grant a supplicant access to the network. The port starts in the *unauthorized* state. While in this state, the port that is not configured as a voice VLAN port disallows all ingress traffic except for IEEE 802.1X authentication, CDP, and STP packets. When a supplicant is successfully authenticated, the port changes to the *authorized* state, allowing all traffic for the supplicant to flow normally. If the port is configured as a voice VLAN port, the port allows VoIP traffic and IEEE 802.1X protocol packets before the supplicant is successfully authenticated.

If a client that does not support IEEE 802.1X authentication connects to an unauthorized IEEE 802.1X port, the router requests the client’s identity. In this situation, if the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an IEEE 802.1X-enabled supplicant connects to a port that is not running the IEEE 802.1X standard, the supplicant initiates the authentication process by sending the EAPOL-start frame. When no response is received, the supplicant sends the request for a fixed number of times. Because no response is received, the supplicant begins sending frames as if the port is in the authorized state.

You control the port authorization state by using the **dot1x port-control** interface configuration command and these keywords:

- **force-authorized** --Disables IEEE 802.1X authentication and causes the port to change to the authorized state without any authentication exchange required. The port sends and receives normal traffic without IEEE 802.1X-based authentication of the client. This is the default setting.
- **force-unauthorized** --Causes the port to remain in the unauthorized state, ignoring all attempts by the supplicant to authenticate. The router cannot provide authentication services to the supplicant through the port.
- **auto** --Enables IEEE 802.1X authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes from down to up or when an EAPOL-start frame is received. The router requests the identity of the supplicant and begins relaying authentication messages between the supplicant and the authentication server. Each supplicant attempting to access the network is uniquely identified by the router by using the supplicant MAC address.

If the supplicant is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated supplicant are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the router can resend the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a supplicant logs off, it sends an EAPOL-logoff message, causing the router port to change to the unauthorized state.

If the link state of a port changes from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

For information about configuring IEEE 802.1X port-based authentication, see the “Configuring IEEE 802.1X Authentication” section of the “Configuring IEEE 802.1X Port-Based Authentication” chapter in the *Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE.*

Troubleshooting and IEEE 802.1X--Conditional Logging

Use the IEEE 802.1X--Conditional Logging feature for troubleshooting. When the Conditional Logging feature is enabled, the router generates debugging messages for packets entering or leaving the router on a specified interface; the router will not generate debugging output for packets entering or leaving through a different interface. You can specify the interfaces explicitly. For example, you may only want to see debugging messages for one interface or subinterface. You can also turn on debugging for all interfaces that meet specified condition. This feature is useful on dial access servers, which have a large number of ports.

Normally, the router will generate debugging messages for every interface, resulting in a large number of messages. The large number of messages consumes system resources, and can affect your ability to find the specific information you need. By limiting the number of debugging messages, you can receive messages related to only the ports you wish to troubleshoot.

For more information on Conditional Logging and enabling conditionally triggered debugging, see the "Enabling Conditionally Triggered Debugging" section of the "Troubleshooting and Fault Management" chapter in the *Basic System Management Configuration Guide, Cisco IOS Release 15.0M*.

IEEE 802.1X with RADIUS Accounting

Note This section describes IEEE 802.1X security features available only on the switch ports in a Cisco ISR.

IEEE 802.1X RADIUS Accounting

Note If you plan to implement system-wide accounting, you should also configure IEEE 802.1X accounting. Moreover, you need to inform the accounting server of the system reload event when the system is reloaded to ensure that the accounting server is aware that all outstanding IEEE 802.1X sessions on this system are closed.

Note To enable IEEE 802.1X accounting, you must first configure IEEE 802.1X authentication and switch-to-RADIUS server communication.

IEEE 802.1X RADIUS accounting relays important events to the RADIUS server (such as the supplicant’s connection session). This session is defined as the interval beginning when the supplicant is authorized to use the port and ending when the supplicant stops using the port.

Note You must configure the IEEE 802.1X supplicant to send an EAP-logoff (Stop) message to the switch when the user logs off. If you do not configure the IEEE 802.1X supplicant, an EAP-logoff message is not sent to the switch and the accompanying accounting Stop message is not sent to the authentication server. See the Microsoft Knowledge Base article at the location: http://support.microsoft.com and set the SupplicantMode registry to 3 and the AuthMode registry to 1.

After the supplicant is authenticated, the switch sends accounting-request packets to the RADIUS server, which responds with accounting-response packets to acknowledge the receipt of the request.

A RADIUS accounting-request packet contains one or more Attribute-Value (AV) pairs to report various events and related information to the RADIUS server. The following events are tracked:

- User successfully authenticates.
- User logs off.
- Link-down occurs on an IEEE 802.1X port.
- Reauthentication succeeds.
- Reauthentication fails.

When the port state transitions between authorized and unauthorized, the RADIUS messages are transmitted to the RADIUS server.

The switch does not log any accounting information. Instead, it sends such information to the RADIUS server, which must be configured to log accounting messages.

This is the IEEE 802.1X RADIUS accounting process

1. A user connects to a port on the router.
2. Authentication is performed.
3. VLAN assignment is enabled, as appropriate, based on the RADIUS server configuration.
4. The router sends a start message to an accounting server.
5. Reauthentication is performed, as necessary.
6. The port sends an interim accounting update to the accounting server that is based on the result of reauthentication.
7. The user disconnects from the port.
8. The router sends a stop message to the accounting server.

The switch port does not log IEEE 802.1X accounting information. Instead, it sends this information to the RADIUS server, which must be configured to log accounting messages.

To configure IEEE 802.1X accounting, you need to do the following tasks:

- Enable accounting in your RADIUS server.
- Enable IEEE 802.1X accounting on your switch.
- Enable AAA accounting by using the **aaa system accounting** command.

Enabling AAA system accounting along with IEEE 802.1X accounting allows system reload events to be sent to the accounting RADIUS server for logging. When the accounting RADIUS server receives notice of a system reload event, the server can infer that all active IEEE 802.1X sessions are appropriately closed.

Because RADIUS uses the unreliable transport protocol User Datagram Protocol (UDP), accounting messages may be lost due to poor network conditions. If the switch does not receive the accounting response message from the RADIUS server after a configurable number of retransmissions of an accounting request, the following system message appears:

```
Accounting message %s for session %s failed to receive Accounting Response.
```

When the stop message is not transmitted successfully, a message like the following appears:

```
00:09:55: %RADIUS-3-NOACCOUNTINGRESPONSE: Accounting message Start for session
172.20.50.145 sam 11/06/03 07:01:16 11000002 failed to receive Accounting Response.
```

Note Use the **debug radius** command or **debug radius accounting** command to enable the %RADIUS-3-NO ACCOUNTING RESPONSE message.

Use the **show radius statistics**command to display the number of RADIUS messages that do not receive the accounting response message.

For information about configuring IEEE 802.1X RADIUS accounting, see the “Enabling 802.1X Accounting” section of the “Configuring 802.1X Port-Based Authentication” chapter in the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*, 12.2(31)SGA.

IEEE 802.1X Accounting Attribute-Value Pairs

The information sent to the RADIUS server is represented in the form of AV pairs. These AV pairs provide data for different applications. (For example, a billing application might require information that is in the Acct-Input-Octets or the Acct-Output-Octets attributes of a RADIUS packet.)

AV pairs are automatically sent by a router that is configured for IEEE 802.1X accounting. Three types of RADIUS accounting packets are sent by a router:

- START-sent when a new user session starts
- INTERIM-sent during an existing session for updates
- STOP-sent when a session terminates

The following table lists the AV pairs and when they are sent by the router:

Table 1 Accounting AV Pairs

Attribute Number	AV Pair Name	START	INTERIM	STOP
Attribute[1]	User-Name	Always	Always	Always
Attribute[4]	NAS-IP-Address	Always	Always	Always
Attribute[5]	NAS-Port	Always	Always	Always
Attribute[6]	Service-Type	Always	Always	Always
Attribute[8]	Framed-IP-Address	Never	Sometimes[1]	Sometimes 1
Attribute[25]	Class	Always	Always	Always
Attribute[30]	Called-Station-ID	Always	Always	Always
Attribute[31]	Calling-Station-ID	Always	Always	Always
Attribute[40]	Acct-Status-Type	Always	Always	Always
Attribute[41]	Acct-Delay-Time	Always	Always	Always
Attribute[42]	Acct-Input-Octets	Never	Always	Always
Attribute[43]	Acct-Output-Octets	Never	Always	Always
Attribute[44]	Acct-Session-ID	Always	Always	Always
Attribute[45]	Acct-Authentic	Always	Always	Always
Attribute[46]	Acct-Session-Time	Never	Never	Always
Attribute[47]	Acct-Input-Packets	Never	Always	Always
Attribute[48]	Acct-Output-Packets	Never	Always	Always
Attribute[49]	Acct-Terminate-Cause	Never	Never	Always
Attribute[61]	NAS-Port-Type	Always	Always	Always

You can configure the ISR to send Cisco vendor-specific attributes (VSAs) to the RADIUS server. The following table lists the available Cisco AV pairs.

[1] The Framed-IP-Address AV pair is sent only if a valid Dynamic Host Control Protocol (DHCP) binding exists for the host in the DHCP snooping bindings table.

Note To enable VSAs to be sent in the accounting records you must configure the **radius-server vsa send accounting** command.

Table 2 Cisco Vendor-Specific Attributes

Attribute Number	AV Pair Name	START	INTERIM	STOP
Attribute[26,9,1]	Cisco-Avpair: connect-progress	Always	Always	Always
Attribute[26,9,2]	cisco-nas-port	Always	Always	Always
Attribute[26,9,1]	Cisco-Avpair: disc-cause	Never	Never	Always

You can view the AV pairs that are being sent by the router by entering the **debug radius accounting** privileged EXEC command. For more information about this command, see the *Cisco IOS Debug Command Reference*. For more information about AV pairs, see RFC 3580, *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines* .

How to Use IEEE 802.1X Authentication with Other Features

Configuring the Host Mode

Beginning in privileged EXEC mode, follow these steps to allow a single host (client) or multiple hosts on an 802.1X-authorized port. Use the multi-domain keyword to configure multidomain authentication (MDA) to enable authentication of both a host and a voice device, such as an IP phone (Cisco or non-Cisco) on the same switch port.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server vsa send authentication**
4. **interface** *interface-id*
5. **authentication host-mode**[**multi-auth**|**multi-domain**|**multi-host**|**single-host**] *interface-id*
6. **switchportvoicevlan** *vlan-id*
7. **end**
8. **show authentication interface** *interface-id*
9. **copy running-config startup-config**

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	**radius-server vsa send authentication** **Example:** `Router# (config)# radius-server vsa send authentication`	Configures the Network Access Server (NAS) to recognize and use vendor-specific attributes.
Step 4	**interface** *interface-id* **Example:** `Router# (config)# interface fastethernet 2/1`	Specifies the port to which multiple hosts are indirectly attached, and enters interface configuration mode.
Step 5	**authentication host-mode**[**multi-auth**|**multi-domain**|**multi-host**|**single-host**] *interface-id* **Example:** `Router# (config-if)# authentication host-mode single-host`	Allows a single client on the 802.1X-authorized port.

	Command or Action	Purpose
Step 6	**switchportvoicevlan** *vlan-id* **Example:** `Router# (config-if)# switchport voice vlan 2`	(Optional) Configures the voice VLAN.

Step 7	**end**
	Example:
	`Router# (config-if)# end`
		Returns to privileged EXEC mode.

Step 8	**show authentication interface** *interface-id* **Example:** `Router# show authentication interface`	Verifies your entries.
Step 9	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	Saves your entries in the configuration file.

IEEE 802.1X Authentication with VLAN Assignment

Note This section describes IEEE 802.1X security features available only on the switch ports in a Cisco ISR.

In Cisco IOS Release 12.4(11)T and later releases, the switch ports support IEEE 802.1X authentication with VLAN assignment. After successful IEEE 802.1X authentication of a port, the RADIUS server sends the VLAN assignment to configure the switch port. You can use the VLAN Assignment feature to limit network access for certain users.

The RADIUS server database maintains the username-to-VLAN mappings, assigning the VLAN based on the username of the supplicant connected to the switch port.

This section contains the following information about IEEE 802.1X VLAN assignment:

- Prerequisites for IEEE 802.1X VLAN Assignment, page 15
- Restrictions for IEEE 802.1X VLAN Assignment, page 16
- Configuring VLAN Assignment, page 16

Prerequisites for IEEE 802.1X VLAN Assignment

- IEEE 802.1X must be enabled on the switch port.
- EAP support must be enabled on the RADIUS server.
- AAA authorization must be configured on the port for all network-related service requests.
- The port must be successfully authenticated.

Restrictions for IEEE 802.1X VLAN Assignment

- The switch port is always assigned to the configured access VLAN when any of the following conditions occurs:
    - No VLAN is supplied by the RADIUS server.
    - The VLAN information from the RADIUS server is not valid.
    - IEEE 802.1X authentication is disabled on the port.
    - The port is in the force authorized, force unauthorized, unauthorized, or shutdown state.

Note An access VLAN is a VLAN assigned to an access port. All packets sent from or received on this port belong to this VLAN.

- Assignment to the configured access VLAN prevents ports from appearing unexpectedly in an inappropriate VLAN because of a configuration error. Examples of configuration errors include the following:
    - A nonexistent or malformed VLAN ID
    - Attempted assignment to a voice VLAN ID
- The IEEE 802.1X authentication with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN Membership Policy Server (VMPS).
- If the multi-host mode is enabled on an IEEE 802.1X port, all hosts are placed in the same VLAN (specified by the RADIUS server) as the first authenticated host.
- If an IEEE 802.1X port is authenticated and put in the RADIUS server-assigned VLAN, any change to the port access VLAN configuration does not take effect.

Configuring VLAN Assignment

Note This section describes IEEE 802.1X security features available only on the switch ports in a Cisco ISR.

- Enable AAA authorization by using the **network** keyword to allow interface configuration from the RADIUS server. For detailed instructions, see the Configuring RADIUS Authorization for User Privileged Access and Network Services section of the Configuring Switch-Based Authentication chapter in the *Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE*.
- Enable IEEE 802.1X authentication. For detailed instructions, see the Configuring RADIUS Login Authentication section of the Configuring Switch-Based Authentication chapter in the *Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE*.

Note The VLAN assignment feature is automatically enabled when you configure IEEE 802.1X authentication on an access port.

- Assign vendor-specific tunnel attributes in the RADIUS server. The RADIUS server must return these attributes to the router:

- [64] Tunnel-Type = VLAN
- [65] Tunnel-Medium-Type = 802
- [81] Tunnel-Private-Group-ID = VLAN name or VLAN ID

Attribute [64] must contain the value “VLAN” (type 13). Attribute [65] must contain the value “802” (type 6). Attribute [81] specifies the VLAN name or VLAN ID assigned to the IEEE 802.1X-authenticated user.

For examples of tunnel attributes, see the Configuring the Switch to Use Vendor-Specific RADIUS Attributes section of the Configuring Switch-Based Authentication chapter in the *Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE*.

Configuring IEEE 802.1X Guest VLAN

When you configure a guest VLAN, clients that are not 802.1X-capable are put into the guest VLAN when the server does not receive a response to its EAP request/identity frame. Clients that are 802.1X-capable but that fail authentication are not granted network access. The switch supports guest VLANs in single-host, multiple-host and multi-domain modes. The switch does not support guest VLANs in multi-auth mode.

Beginning in privileged EXEC mode, follow these steps to configure a guest VLAN. This procedure is optional.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *type slot/port*
3. **authentication port-control auto**
4. **exit**
5. **dot1x guest-vlan supplicant**
6. **end**
7. **show authentication interface** *interface-id*
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**interface** *type slot/port* **Example:** `Switch(config)# interface gigabitethernet0/1`	Specifies the port to be configured, and enters interface configuration mode. For the supported port types, see the “802.1x Authentication Configuration Guidelines” section of the "Configuring IEEE 1802.1X Port-Based Authentication" module.

	Command or Action	Purpose
Step 3	**authentication port-control auto** **Example:** `Switch(config-if)# authentication port-control auto`	Enables 802.1X authentication on the port.
Step 4	**exit** **Example:** `Switch(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 5	**dot1x guest-vlan supplicant** **Example:** `Switch(config)# dot1x guest-vlan supplicant`	Specifies the supplicant as an 802.1X guest VLAN. You can configure any active VLAN except an RSPAN VLAN or a voice VLAN as an 802.1X guest VLAN.

Step 6	**end**
	Example:
	`Switch(config-if)# end`
		Returns to privileged EXEC mode.

Step 7	**show authentication interface** *interface-id* **Example:** `Switch# show authentication interface interface gigabitethernet0/1`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

To disable and remove the guest VLAN, use the **no dot1x guest-vlan** in interface configuration mode. The port returns to the unauthorized state.

IEEE 802.1X with RADIUS-Supplied Session Timeout

Note This section describes IEEE 802.1X security features available only on the switch ports in a Cisco ISR.

You can specify whether a switch port uses a locally configured or a RADIUS-provided reauthentication timeout. If the switch port is configured to use the local timeout, it reauthenticates the host when the timer expires.

If the switch port is configured to use the RADIUS-provided timeout, it looks in the RADIUS Access-Accept message for the Session-Timeout and optional Termination-Action attributes. The switch port uses the value of the Session-Timeout attribute to determine the duration of the session, and it uses the value of the Termination-Action attribute to determine the switch action when the session's timer expires.

If the Termination-Action attribute is present and its value is RADIUS-Request, the switch port reauthenticates the host. If the Termination-Action attribute is not present, or its value is Default, the switch port terminates the session.

Note The supplicant on the port detects that its session has been terminated and attempts to initiate a new session. Unless the authentication server treats this new session differently, the supplicant may see only a brief interruption in network connectivity as the switch sets up a new session.

If the switch port is configured to use the RADIUS-supplied timeout, but the Access-Accept message does not include a Session-Timeout attribute, the switch port never reauthenticates the supplicant. This behavior is consistent with Cisco’s wireless access points.

IEEE 802.1X Authentication with Voice VLAN Ports

Note This section describes IEEE 802.1X security features available only on the switch ports in a Cisco ISR.

A voice VLAN port is a special access port associated with two VLAN identifiers:

- Voice VLAN identifier (VVID) to carry voice traffic to and from the IP phone. The VVID is used to configure the IP phone connected to the port.
- Port VLAN identifier (PVID) to carry the data traffic to and from the workstation connected to the router through the IP phone. The PVID is the native VLAN of the port.

The IP phone uses the VVID for its voice traffic, regardless of the authorization state of the port. This allows the phone to work independently of IEEE 802.1X authentication.

In single-host mode, only the IP phone is allowed on the voice VLAN. In multi-host mode, additional supplicants can send traffic on the voice VLAN after a supplicant is authenticated on the PVID. When multi-host mode is enabled, the supplicant authentication affects both the PVID and the VVID.

A voice VLAN port becomes active when there is a link, and the device MAC address appears after the first CDP message from the IP phone. Cisco IP phones do not relay CDP messages from other devices. As a result, if several IP phones are connected in series, the router recognizes only the one directly connected to it. When IEEE 802.1X authentication is enabled on a voice VLAN port, the router drops packets from unrecognized IP phones more than one hop away.

When IEEE 802.1X authentication is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.

Note If you enable IEEE 802.1X authentication on an access port on which a voice VLAN is configured and to which a Cisco IP Phone is connected, the Cisco IP phone loses connectivity to the router for up to 30 seconds.

For information about configuring IEEE 802.1X with voice VLANs, see "Configuring Voice VLAN" in the Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE.

Enabling IEEE 802.1X SNMP Notifications on Switch Ports

Note This section describes IEEE 802.1X security features available only on the switch ports in a Cisco ISR.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps dot1x** *notification-type*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps dot1x** *notification-type* **Example:** `Router (config)# snmp-server enable traps dot1x no-guest-vlan`	Enables SNMP logging and reporting when no Guest VLAN is configured or available.

IEEE 802.1X MIB Support

Cisco IOS Release 12.4(11)T provides support for the following MIBs that provide SNMP access to IEEE 802.1X feature components:

- IEEE8021-PAE-MIB
- Cisco-PAE-MIB

The IEEE8021-PAE-MIB supports reporting of the following information:

- The state of the IEEE 802.1X state machine on a particular port
- Statistics associated with the state of the IEEE 802.1X state machine

The Cisco-PAE-MIB provides SNMP support for the logging and reporting of events, including:

- Port mode
- Guest VLAN number (Details the Guest VLAN number configured on a port.)
- InGuestVLAN (Indicates whether a port is in the Guest VLAN.)

Configuration Examples for IEEE 802.1x Features

Enabling IEEE 802.1X and AAA on a Port Example

Note Whenever you configure any IEEE 802.1X parameter on a port, a dot1x authenticator is automatically created on the port. As a result **dot1x pae authenticator** appears in the configuration to ensure that IEEE 802.1X authentication still works without manual intervention on legacy configurations. The appearance of the IEEE 802.1X information in the configuration is likely to change in future releases.

This example shows how to enable IEEE 802.1X and AAA on Fast Ethernet port 2/1, and how to verify the configuration:

```
Router# configure terminal
Router(config)# dot1x system-auth-control
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# interface fastethernet2/1
Router(config-if)# switchport mode access
Router(config-if)# dot1x pae authenticator
Router(config-if)# dot1x port-control auto
Router(config-if)# end
Router# show dot1x interface fastethernet7/1 details
Dot1x Info for FastEthernet7/1
-----------------------------------
```

```
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Dot1x Authenticator Client List
-------------------------------
Supplicant                = 1000.0000.2e00
        Auth SM State     = AUTHENTICATED
        Auth BEND SM Stat = IDLE
Port Status               = AUTHORIZED

Authentication Method     = Dot1x
Authorized By             = Authentication Server
Vlan Policy               = N/A
```

Example Configuring the IEEE 802.1X Host Mode

This example shows how to enable 802.1X authentication and to allow multiple hosts:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication host-mode multi-host
Switch(config-if)# end
```

Enabling IEEE 802.1X RADIUS Accounting Example

This example shows how to specify the server with IP address 172.20.39.46 as the RADIUS server. The first command configures the RADIUS server, specifying port 1612 as the authorization port, 1813 as the UDP port for accounting, and rad123 as the encryption key:

```
Router# configure terminal
Router(config)# radius-server host 172.20.39.46 auth-port 1812 acct-port 1813 key rad123
Router(config)# aaa accounting dot1x default start-stop group radius
Router(config)# aaa accounting system default start-stop group radius
Router(config)# end
Router#
```

Note You must configure the RADIUS server to perform accounting tasks.

Configuring IEEE 802.1X with Guest VLAN Example

This example shows how to enable the VLAN as an 802.1X guest VLAN:

```
Switch(config)# interface fastethernet 5/1
Switch(config-if)# authentication port-control auto
Switch(config-if)# exit
Switch(config)# dot1x guest-vlan supplicant
```

Configuring RADIUS-Provided Session Timeout Example

This example assumes you have enabled IEEE 802.1X reauthentication and shows how to configure the switch port to derive the reauthentication period from the server and to verify the configuration:

```
Router# configure terminal
Router(config)# interface fastethernet7/1
Router(config-if)# switchport mode access
Router(config-if)# dot1x pae authenticator
Router(config-if)# dot1x timeout reauth-period server
Router(config-if)# end
Router#
```

Configuring IEEE 802.1X with Voice VLAN Example

This example shows how to enable IEEE 802.1X with voice VLAN feature on Fast Ethernet interface 5/9:

```
Router# configure terminal
Router(config)# interface fastethernet5/9
Router(config-if)# switchport access vlan 2
Router(config-if)# switchport mode access
Router(config-if)# switchport voice vlan 10
Router(config-if)# dot1x pae authenticator
Router(config-if)# dot1x port-control auto
Router(config-if)# end
Router(config# end
Router#
```

Displaying IEEE 802.1X Statistics and Status Example

To display IEEE 802.1X statistics for all ports, use the **show dot1x all statistics** privileged EXEC command. To display IEEE 802.1X statistics for a specific port, use the **show dot1x statistics interface***interface-id* privileged EXEC command.

To display the IEEE 802.1X administrative and operational status for the switch, use the **show dot1x all**[**details** | **statistics**| **summary**] privileged EXEC command. To display the IEEE 802.1X administrative and operational status for a specific port, use the **show dot1x interface***interface-id* privileged EXEC command. For detailed information about the fields in these displays, see the command reference for this release.

This example shows the output of the **show dot1x all**command:

```
Router-871# show dot1x all
Sysauthcontrol                 Enabled
Dot1x Protocol Version     2
Dot1x Info for FastEthernet1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Router-871#
```

This example shows the output of the **show dot1x summary**command:

```
Router-871# show dot1x all summary

Interface           PAE             Client                         Status
------------------------------------------------------------------------------------------
Fa1                 AUTH             000d.bcef.bfdc           AUTHORIZED
```

Additional References

Related Documents

Related Topic	Document Title
Configuring IEEE 802.1X Port-Based Authentication	The chapter Configuring 802.1X Port-Based Authentication in the *Catalyst 3750 Series Switch Cisco IOS Software Configuration Guide*, 12.2(31)SEE
IEEE 802.1X commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	• *Catalyst 4500 Series Switch Cisco IOS Command Reference, Release 12.2(25)SGA* • *Catalyst 3750 Switch Command Reference , Cisco IOS Release 12.2(25)SEE*
VPN Access Control Using IEEE 802.1x Authentication	The VPN Access Control Using 802.1X Authentication feature module.

Standards

Standard	Title
IEEE 802.1X	*Port Based Network Access Control*

MIBs

MIB	MIBs Link
• IEEE8021-PAE-MIB • Cisco-PAE-MIB	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

RFCs

RFC	Title
RFC 3580	*IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*

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 Configuring IEEE 802.1X Port-Based Authentication

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 3 Feature Information for Configuring IEEE 802.1X Port-Based Authentication

Feature Name	Releases	Feature Information
IEEE 802.1X Authenticator	12.3(4)T 15.2(2)T	This feature was introduced to prevent unauthorized devices (supplicants) from gaining access to the network. This feature is available on the following Cisco ISRs equipped with cards or modules that include switch ports: • Cisco 800 Series ISR • Cisco 870 Series ISR • Cisco 1800 Series ISR • Cisco 2800 Series ISR • Cisco 3800 Series ISR In Cisco IOS Release 12.4(11)T, this feature was modified to include the other features listed in this table. The following commands were introduced or modified: **aaa accounting , dot1x guest-vlan , snmp-server enable traps**.
IEEE 802.1X RADIUS Accounting	12.4(11)T	This feature relays important events to the RADIUS server (such as the supplicant's connection session). This information is used for security and billing purposes. In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports: • Cisco 800 Series ISR • Cisco 870 Series ISR • Cisco 1800 Series ISR • Cisco 2800 Series ISR • Cisco 3800 Series ISR

Feature Name	Releases	Feature Information
IEEE 802.1X--VLAN Assignment	12.4(11)T	This feature allows the RADIUS server to send the VLAN assignment to configure the switch port. In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports: • Cisco 800 Series ISR • Cisco 870 Series ISR • Cisco 1800 Series ISR • Cisco 2800 Series ISR • Cisco 3800 Series ISR
IEEE 802.1X Guest VLAN	12.4(11)T	This feature allows you to configure a guest VLAN for each IEEE 802.1X-capable switch port on the router to provide limited services to clients, such as downloading the IEEE 802.1X client. In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports: • Cisco 800 Series ISR • Cisco 870 Series ISR • Cisco 1800 Series ISR • Cisco 2800 Series ISR • Cisco 3800 Series ISR

Feature Name	Releases	Feature Information
IEEE 802.1X RADIUS-Supplied Session Timeout	12.4(11)T	This feature allows you to specify whether a switch port uses a locally configured or a RADIUS-provided reauthentication timeout. In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports: • Cisco 800 Series ISR • Cisco 870 Series ISR • Cisco 1800 Series ISR • Cisco 2800 Series ISR • Cisco 3800 Series ISR
IEEE 802.1X--Voice VLAN	12.4(11)T	This feature allows you to configure a special access port associated with two VLAN identifiers: • Voice VLAN identifier (VVID) to carry voice traffic to and from the IP phone. The VVID is used to configure the IP phone connected to the port. • Port VLAN identifier (PVID) to carry the data traffic to and from the workstation connected to the router through the IP phone. The PVID is the native VLAN of the port. In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports: • Cisco 800 Series ISR • Cisco 870 Series ISR • Cisco 1800 Series ISR • Cisco 2800 Series ISR • Cisco 3800 Series ISR

Feature Name	Releases	Feature Information
IEEE 802.1X MIB Support	12.4(11)T	This feature provides support for the following MIBs: • IEEE8021-PAE-MIB • Cisco-PAE-MIB In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports: • Cisco 800 Series ISR • Cisco 870 Series ISR • Cisco 1800 Series ISR • Cisco 2800 Series ISR • Cisco 3800 Series ISR
IEEE 802.1X —Common Session ID	15.2(2)T	This feature allows you to use a session ID identifier for all 802.1X and MAB authenticated sessions. The session ID is used for all reporting purposes such as show commands, MIBs, and RADIUS messages. The ID allows users to distinguish messages for one session from messages for other sessions.
CDP Enhancement - Host presence TLV	15.2(2)T	This features allows you to ensure that only one client can be connected to the 802.1X-enabled port. The switch detects the client by sending an EAPOL frame when the port link state changes to the up state. If a client leaves or is replaced with another client, the switch changes the port link state to down, and the port returns to the unauthorized state

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Remote Site IEEE 802.1X Local Authentication Service

The Remote Site IEEE 802.1X Local Authentication Service feature provides the ability to configure an access point or wireless-aware router to act as a local RADIUS server. Configuring local authentication service provides a backup authentication service in the event of a WAN link or server failure.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Restrictions for Configuring Remote Site IEEE 802.1X Local Authentication Service

- The local authentication server does not synchronize its database with the main RADIUS servers. It is necessary to manually configure the local authentication server with client usernames and passwords.
- LEAP is the only supported authentication protocol.
- Although multiple local authentication servers can exist on one network, only one authentication server can be configured on any single device.

Information About Configuring Remote Site IEEE 802.1X Local Authentication Service

On typical wireless LANs that use 802.1X authentication, access points and wireless-aware routers rely on remote site RADIUS servers to authenticate client devices. This authentication traffic must cross a WAN link. If the WAN link fails, or if the access points and routers cannot reach the RADIUS servers, then the client devices cannot access the wireless network even if their requirements for access are strictly local.

To provide for local authentication service or backup authentication service in the event of a WAN link or server failure, you can configure an access point or wireless-aware router to act as a local RADIUS server. The access point or wireless-aware router can authenticate Light Extensible Authentication Protocol (LEAP)-enabled wireless client devices and allow them to join your network.

Because the local authentication device does not synchronize its database with the main RADIUS servers. You must configure the local authentication server with client usernames and passwords. The local authentication server also permits you to specify a VLAN and a list of service set identifiers (SSIDs) that a client is allowed to use.

Follow these guidelines when you configure an access point or wireless-aware router as a local authentication server:

- To prevent performance degradation, configure local authentication service on an access point or a wireless-aware router that does not have a high CPU load.
- Physically secure the access point or router to protect its configuration.

The table below shows the maximum number of clients that can be configured on a local authentication server.

Table 4 Maximum Number of Clients That Can be Configured on a Local Authentication Server

Local Authentication Server	Maximum Number of Clients
Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200	50
Cisco 2610XM, Cisco 2611XM routers	50
Cisco 2620XM, Cisco 2621XM routers	50
Cisco 2650XM, Cisco 2651XM routers	50
Cisco 2691 routers	50
Cisco 2811 routers	50
Cisco 2821 routers	50
Cisco 2851 routers	50
Cisco 3725 routers	50
Cisco 3745 routers	50
Cisco 3825 routers	50

Local Authentication Server	Maximum Number of Clients
Cisco 3845 routers	50

Note Users that are associated to the local authentication server might notice a drop in performance during authentication of client devices. However, if your wireless LAN contains only one access point, you can configure that device as both the 802.1X authenticator and the local authentication server.

You configure access points and routers to use the local authentication server when they cannot reach the main servers or when a RADIUS server is not available.

The access points and wireless-aware routers stop using the local authentication server automatically when the link to the main servers is restored.

If your local authentication server also serves client devices, you must enter the local authentication server access point or router as a network access server (NAS). When a LEAP client associates to the local authentication server access point, the access point uses itself to authenticate the client.

Caution The access point or wireless-aware router that you use as an authentication server contains detailed authentication information about your wireless LAN, so you should secure it physically to protect its configuration.

How to Configure Remote Site IEEE 802.1X Local Authentication Service

Configuring the Local Authentication Server

Perform this task to configure the access point as a local authentication server.

SUMMARY STEPS

1. Router> **enable**
2. Router# **configure terminal**
3. Router(config)# **aaa new-model**
4. Router(config)# **radius-server local**
5. Router(config-radsrv)# **nas** ip-address **key** shared-key

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router> **enable** **Example:** `Router> enable`	Enables privileged EXEC mode.
Step 2	Router# **configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Router(config)# **aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA.
Step 4	Router(config)# **radius-server local** **Example:** `Router(config)# radius-server local`	Enables the access point or router as a local authentication server and enters configuration mode for the authentication server.
Step 5	Router(config-radsrv)# **nas** ip-address **key** shared-key **Example:** `Router(config)# nas 192.168.12.17 key shared256` **Example:**	Adds an access point or wireless domain services (WDS) device to the list of units that use the local authentication server. Enter the IP address of the access point or WDS device, and the shared key used to authenticate communication between the local authentication server and other access points. You must enter this shared key on the WDS devices that use the local authentication server. Each access point and candidate WDS that uses the local authentication server is a network access server (NAS). If an access point is the local authentication server that also serves client devices, you must enter the local authentication server access point as a NAS. **Note** Leading spaces in the key string are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. Repeat this step to add each access point and candidate WDS device that uses the local authentication server.

Configuring User Groups on the Local Authentication Server

Perform this optional task (beginning in local RADIUS server configuration mode) to configure user groups on the local authentication server.

Note If you do not wish to configure user groups on the local authentication server, skip this task and go to the Creating the User List on the Local Authentication_Server module.

SUMMARY STEPS

1. Router(config-radsrv)# **group** group-name
2. Router(config-radsrv-group)# **vlan** vlan
3. Router(config-radsrv-group)# **ssid** ssid
4. Router(config-radsrv-group)# **reauthentication time** seconds
5. Router(config-radsrv-group)# **block count***count***time** {seconds | **infinite**}
6. Router(config-radsrv-group)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config-radsrv)# **group** group-name	Enters user group configuration mode and configures a user group to which you can assign shared settings.
Step 2	Router(config-radsrv-group)# **vlan** vlan	(Optional) Specifies a VLAN to be used by members of the user group. The access point moves group members into that VLAN, overriding other VLAN assignments. You can assign only one VLAN to the group.
Step 3	Router(config-radsrv-group)# **ssid** ssid	(Optional) Enters up to 20 service set identifiers (SSIDs) to limit members of the user group to those SSIDs. The access point checks whether the client's SSID matches an SSID in the list. If the SSID does not match, the client is disassociated.
Step 4	Router(config-radsrv-group)# **reauthentication time** seconds	(Optional) Configures the number of seconds after which access points should reauthenticate members of the group. The reauthentication provides users with a new encryption key. The default setting is 0, which means that group members are never required to reauthenticate.
Step 5	Router(config-radsrv-group)# **block count***count***time** {seconds | **infinite**}	(Optional) To help protect against password-guessing attacks, you can lock out group members for a length of time after a set number of incorrect passwords. • Count--The number of failed passwords that triggers a lockout of the username. • Time--The number of seconds that the lockout should last. If you enter infinite, an administrator must manually unblock the locked username. For more information, see the Unblocking Usernames module.
Step 6	Router(config-radsrv-group)# **exit**	Returns to authenticator configuration mode.

- Unblocking Usernames, page 36

Unblocking Usernames

You can unblock usernames before the lockout time expires or when the lockout time is set to infinite. To unblock a locked username, enter the following command in privileged EXEC mode on the local authentication server.

```
Router# clear radius local-server user username
```

Creating the User List on the Local Authentication Server

Perform the required task described in the following paragraphs to create a user list on the local authentication server and to configure the users that are allowed to authenticate using the local authentication server.

Note If you do not wish to configure users on the local authentication server, skip this task and go to the Saving the Configuration on the Local Authentication Server module.

You must enter a username and password for each user. If you know only the NT hash value of the password, which you can often find in the authentication server database, you can enter the NT hash as a string of hexadecimal digits.

To add the user to a user group, enter the group name. If you do not specify a group, the user is not assigned to a specific VLAN and is never forced to reauthenticate.

Beginning in local RADIUS server configuration mode, enter the **user** command for each username:

```
Router(config-radsrv)# user
 username {password
 | nthash
} password [group
 group-name]
```

Saving the Configuration on the Local Authentication Server

Perform this optional task to save the current configuration.

SUMMARY STEPS

1. Router(config-radsrv)# **end**
2. Router# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config-radsrv)# **end**	Returns to privileged EXEC mode.
Step 2	Router# **copy running-config startup-config**	Saves your entries in the configuration file.

Configuring Access Points or Routers to Use the Local Authentication Server

Perform this required task to add the local authentication server to the list of servers on the client access point or wireless-aware router.

Note If your local authentication server access point also serves client devices, you must configure the local authentication server to use itself to authenticate client devices.

On the wireless devices that use the local authentication server, use the radius-server host command in privileged EXEC mode to enter the local authentication server as a RADIUS server. The order in which the devices attempt to use the servers matches the order in which you enter the servers in the device configuration. If you are configuring the device to use a RADIUS server for the first time, enter the main RADIUS servers first, and enter the local authentication server last.

Note You must enter 1812 as the authentication port and 1813 as the accounting port. The local authentication server listens on User Datagram Protocol (UDP) port 1813 for RADIUS accounting packets. It discards the accounting packets but sends acknowledge packets back to the RADIUS clients to prevent the clients from reacting as though the server is down.

Use the radius-server deadtime command in global configuration mode to set an interval during which the access point or router does not attempt to use servers that do not respond, thus avoiding the wait for a request to time out before trying the next configured server. A server marked as dead is skipped by additional requests for the duration of minutes that you specify, up to 1440 (24 hours).

To remove the local authentication server from the access point or router configuration, use the **no radius-server host** command in global configuration mode.

SUMMARY STEPS

1. Router> **enable**
2. Router# **configure terminal**
3. Router(config)# **aaa new-model**
4. Router(config)# **radius-server host** {*hostname* | *ip-address* } [**auth-port***port-number*] [**acct-port***port-number*] [**timeout***seconds*] [**retransmit***retries*] [**key***string*]
5. **aaa group server** {**radius** | **tacacs+**} *group-name*
6. Router(config-sg-radius)# **server ip-address auth-port 1812 acct-port 1813**
7. Router(config)# **aaa authentication login***named-authentication-list*
8. Router(config)# **end**
9. Router# **show running-config**
10. Router# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router> **enable**	Enables privileged EXEC mode.
Step 2	Router# **configure terminal**	Enters global configuration mode.
Step 3	Router(config)# **aaa new-model**	Enables authentication, authorization, and accounting (AAA). This step must be configured before the rest of the AAA configuration steps.
Step 4	Router(config)# **radius-server host** {*hostname* | *ip-address* } [**auth-port***port-number*] [**acct-port***port-number*] [**timeout***seconds*] [**retransmit***retries*] [**key***string*]	Specifies the IP address or hostname of the remote RADIUS server host. • (Optional) For **auth-port** *port-number*, specify the UDP destination port for authentication requests. • (Optional) For **acct-port** *port-number*, specify the UDP destination port for accounting requests. • (Optional) For **timeout***seconds* , specify the time interval that the access point waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the setting made using the **radius-server timeout** command in global configuration mode. If no timeout is set with the **radius-server host** command, the setting made using the **radius-server timeout** command is used. • (Optional) For **retransmit***retries* , specify the number of times that a RADIUS request is re-sent to a server if that server is not responding or is responding slowly. The range is 1 to 1000. If no retransmit value is set using the **radius-server host** command, the setting made using the **radius-server retransmit** command in global configuration command mode is used. • (Optional) For **key***string* , specify the authentication and encryption key used between the access point and the RADIUS daemon running on the RADIUS server. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host**command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. To configure the access point to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure to use a different UDP port number for each host. The access point software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.
Step 5	**aaa group server** {**radius** | **tacacs+**} *group-name*	Defines the AAA server-group with a group name.
Step 6	Router(config-sg-radius)# **server ip-address auth-port 1812 acct-port 1813**	Defines the AAA server IP address, authentication port, and accounting port.

	Command or Action	Purpose
Step 7	Router(config)# **aaa authentication login***named-authentication-list*	Creates an authentication method list for the server group.
Step 8	Router(config)# **end**	Returns to privileged EXEC mode.
Step 9	Router# **show running-config**	Displays the current configuration for your verification.
Step 10	Router# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Verifying the Configuration for Local Authentication Service

Use the **show running-config** command in global configuration mode to verify the current configuration for local authentication service.

SUMMARY STEPS

1. Router> **enable**
2. Router# **show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router> **enable**	Enables privileged EXEC mode.
Step 2	Router# **show running-config**	Displays the current access point operating configuration

Monitoring and Maintaining 802.1X Local Authentication Service

To view statistics collected by the local authentication server, enter the following command in privileged EXEC mode:

```
Router# show radius local-server statistics
```

To reset local authentication server statistics to zero, enter the following command in privileged EXEC mode:

```
Router# clear radius local-server statistics
```

Configuration Examples for Remote Site IEEE 802.1X Local Authentication Service

- Setting Up a Local Authentication Server Example, page 40

- Setting Up Two Main Servers and a Local Authentication Server Example, page 40
- Displaying Local Authentication Server Configuration Example, page 41
- Displaying Local Authentication Server Statistics Example, page 42

Setting Up a Local Authentication Server Example

This example shows how to set up a local authentication server used by three access points with three user groups and several users:

```
AP# configure terminal
AP(config)# aaa new-model
AP(config)# aaa group server radius RADIUS_SERVER_GROUP
AP(config-sg-radius)# server 10.0.0.1 auth-port 1812 acct-port 1813
AP(config)# aaa authentication login RADIUS_METHOD_LIST
AP(config)# radius-server host 10.0.0.1 auth-port 1812 acct-port 1813 key 110337
AP(config)# radius-server local
AP(config-radsrv)# nas 10.91.6.159 key 110337
AP(config-radsrv)# nas 10.91.6.162 key 110337
AP(config-radsrv)# nas 10.91.6.181 key 110337
AP(config-radsrv)# group clerks
AP(config-radsrv-group)# vlan 87
AP(config-radsrv-group)# ssid batman
AP(config-radsrv-group)# ssid robin
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# group cashiers
AP(config-radsrv-group)# vlan 97
AP(config-radsrv-group)# ssid deer
AP(config-radsrv-group)# ssid antelope
AP(config-radsrv-group)# ssid elk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# group managers
AP(config-radsrv-group)# vlan 77
AP(config-radsrv-group)# ssid mouse
AP(config-radsrv-group)# ssid chipmunk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# exit
AP(config-radsrv)# user jsmith password twain74 group clerks
AP(config-radsrv)# user stpatrick password snake100 group clerks
AP(config-radsrv)# user nick password uptown group clerks
AP(config-radsrv)# user sam password rover32 group cashiers
AP(config-radsrv)# user patsy password crowder group cashiers
AP(config-radsrv)# user carl password 272165 group managers
AP(config-radsrv)# user vic password lid178 group managers
AP(config-radsrv)# end
```

Setting Up Two Main Servers and a Local Authentication Server Example

This example shows how to set up two main servers and a local authentication server with a server deadtime of 10 minutes:

```
Router(config)# aaa new-model
Router(config)# aaa group server radius RADIUS_SERVER_GROUP
Router(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Router(config-sg-radius)# server 172.10.0.1 auth-port 1645 acct-port 1646
Router(config-sg-radius)# server 10.91.6.151 auth-port 1812 acct-port 1813
Router(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001 key 77654
Router(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
 key 77654
Router(config)# radius-server host 10.91.6.151
auth-port 1812 acct-port 1813 key
110337
Router(config)# radius-server deadtime 10
```

In this example, if the WAN link to the main servers fails, the access point or wireless-aware router completes these steps when a LEAP-enabled client device associates:

1. It tries the first server, times out multiple times, and marks the first server as dead.
2. It tries the second server, times out multiple times, and marks the second server as dead.
3. It tries and succeeds using the local authentication server.

If another client device needs to authenticate during the 10-minute deadtime interval, the access point skips the first two servers and tries the local authentication server first. After the deadtime interval, the access point tries to use the main servers for authentication. When setting a deadtime, you must balance the need to skip dead servers with the need to check the WAN link and begin using the main servers again as soon as possible.

Each time an access point or wireless-aware router tries to use the main servers while they are down, the client device that is trying to authenticate might report an authentication timeout. The client device retries and succeeds when the main servers time out and the access point or wireless-aware router tries the local authentication server. You can extend the timeout value on Cisco client devices to accommodate expected server timeouts.

Displaying Local Authentication Server Configuration Example

The following is sample output for configuration of a local authentication server on the Cisco 2621 router.

```
2621-1# show run
Building configuration...
Current configuration : 2954 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2621-1
!
!
aaa new-model
!
!
aaa group server radius RADIUS_LEAP_GROUP
 server 10.0.0.1 auth-port 1812 acct-port 1813
!
aaa authentication login AUTH_LEAP group RADIUS_LEAP_GROUP
aaa session-id common
ip subnet-zero
!
!
ip dhcp pool 2621-dhcp-pool
   network 10.0.0.0 255.0.0.0
!
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
```

```
!
interface FastEthernet1/1
 switchport mode trunk
 no ip address
!
interface FastEthernet1/2
 no ip address
 shutdown
!
interface FastEthernet1/3
 no ip address
 shutdown
!
interface FastEthernet1/4
 no ip address
 shutdown
!
interface FastEthernet1/5
 no ip address
!
!
interface GigabitEthernet1/0
 no ip address
 shutdown
!
interface Vlan1
 ip address 10.0.0.1 255.0.0.0
!
ip classless
!
ip http server
no ip http secure-server
!
!
!
radius-server local
  nas 10.0.0.1 key 0 cisco
  user ap-1 nthash 7 101B2A415547345A5F25790801706510064152425325720D7D04075D523D4F780A
  user ap-5 nthash 7 144231535C540C7A77096016074B51332753030D0877705A264F450A09720A7307
  user user1 nthash 7 1350344A5B5C227B78057B10107A452232515402097C77002B544B45087D0E7200
!
radius-server host 10.0.0.1 auth-port 1812 acct-port 1813
radius-server key cisco
!
wlccp authentication-server infrastructure AUTH_LEAP
wlccp authentication-server client leap AUTH_LEAP
wlccp wds priority 255 interface Vlan1
!
line con 0
line aux 0
line vty 0 4
!
!
!
end
```

Displaying Local Authentication Server Statistics Example

The following is sample output for configuration for the **show radius local-server statistics** command:

```
router-2621-1# show radius local-server statistics
Successes              : 11262       Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 8
Unknown NAS            : 0           Invalid packet from NAS: 0
NAS : 10.0.0.1
Successes              : 11262       Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 8
Corrupted packet       : 0           Unknown RADIUS message : 0
No username attribute  : 0           Missing auth attribute : 0
Shared key mismatch    : 0           Invalid state attribute: 0
Unknown EAP message    : 0           Unknown EAP auth type  : 0
```

```
Maximum number of configurable users: 50, current user count: 11
Username                  Successes  Failures  Blocks
vayu-ap-1                      2235         0       0
vayu-ap-2                      2235         0       0
vayu-ap-3                      2246         0       0
vayu-ap-4                      2247         0       0
vayu-ap-5                      2247         0       0
vayu-11                           3         0       0
vayu-12                           5         0       0
vayu-13                           5         0       0
vayu-14                          30         0       0
vayu-15                           3         0       0
scm-test                          1         8       0
router-2621-1#
```

The first section shows cumulative statistics from the local authentication server. The second section shows statistics for each access point (NAS) that is authorized to use the local authentication server. The third section shows statistics for individual users. If a user is blocked and the lockout time is set to infinite, Blocked appears at the end of the line of statistics for that user. If the lockout time is not set to infinite, Unblocked in x seconds appears at the end of the statistics line for that user.

Additional References

Related Documents

Related Topic	Document Title
Comprehensive set of software configuration commands	Cisco IOS Software Configuration Guide for Cisco Aironet Access Points
Configuration commands for wireless roaming	Configuring Fast Secure Roaming

MIBs

MIB	MIBs Link
Non.	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 Remote Site IEEE 802.1X Local Authentication Service

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 Remote Site IEEE 802.1X Local Authentication Service

Feature Name	Releases	Feature Information
Remote Site IEEE 802.1X Local Authentication Service	12.2(11)JA 12.3(11)T	The Remote Site IEEE 802.1X Local Authentication Service feature provides the ability to configure an access point or wireless-aware router to act as a local RADIUS server. Configuring local authentication service provides a backup authentication service in the event of a WAN link or server failure. This feature was introduced in Cisco IOS Release 12.2(11)JA on Cisco Aironet access points. This feature was integrated in Cisco IOS Release 12.3(11)T on the Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700 series, and Cisco 3800 series routers.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

VPN Access Control Using 802.1X Authentication

The home access router provides connectivity to the corporate network through a Virtual Private Network (VPN) tunnel through the Internet. In the home LAN, apart from the employee, other members of the household may also be using the same access router. The VPN Access Control Using 802.1X Authentication feature allows enterprise employees to access their enterprise networks from home while allowing other household members to access only the Internet. The feature uses the IEEE 802.1X protocol framework to achieve the VPN access control. The authenticated employee has access to the VPN tunnel and others (unauthenticated users on the same LAN) have access only to the Internet.

An authentication manager has been added to allow more flexible authentication between different authentication methods like, dot1x, MAC address bypass, and web authentication. See the 802.1X Flexible Authentication feature for more information.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Prerequisites for VPN Access Control Using 802.1X Authentication

- The PCs connecting behind the router should have 802.1X clients running on them.
- You should know how to configure authentication, authorization, and accounting (AAA) and RADIUS.
- You should be familiar with IP Security (IPSec).
- You should be familiar with Dynamic Host Configuration Protocol (DHCP).
- You should know how to configure user lists on a Cisco access control server (ACS).

Restrictions for VPN Access Control Using 802.1X Authentication

- Easy VPN is not supported.
- VLAN interfaces are currently not supported.
- If there is a switch located between the router and the supplicant (client PC), the Extensible Authentication Protocol over LAN (EAPOL) frames will not reach the router because the switch discards them.

Information About VPN Access Control Using 802.1X Authentication

- How VPN Control Using 802.1X Authentication Works, page 48
- Authentication Using Passwords and MD5, page 50

How VPN Control Using 802.1X Authentication Works

The home access router provides connectivity to the corporate network through a VPN tunnel through the Internet. In the home LAN, both authenticated (employee) and unauthenticated (other household members) users exist, and both have access to the corporate VPN tunnel. Currently there is no existing mechanism to prevent the unauthenticated user from accessing the VPN tunnel.

To distinguish between the users, the VPN Access Control Using 802.1X Authentication feature uses the IEEE 802.1X protocol that allows end hosts to send user credentials on Layer 2 of the network operating system. Unauthenticated traffic users will be allowed to pass through the Internet but will be blocked from accessing the corporate VPN tunnel. The VPN Access Control Using 802.1X feature expands the scope of the 802.1X standard to authenticate devices rather than ports, meaning that multiple devices can be independently authenticated for any given port. This feature separates traffic from authenticated and unauthenticated users so that separate access policies can be applied.

When an 802.1X-capable host starts up, it will initiate the authentication phase by sending the EAPOL-Start 802.1X protocol data unit (PDU) to the reserved IEEE multicast MAC address (01-80-C2-00-00-03) with the Ethernet type or length set to 0x888E.

All 802.1X PDUs will be identified as such by the Ethernet driver and will be enqueued to be handled by an 802.1X process. On some platforms, Ethernet drivers have to program the interface address filter so that EAPOL packets can be accepted.

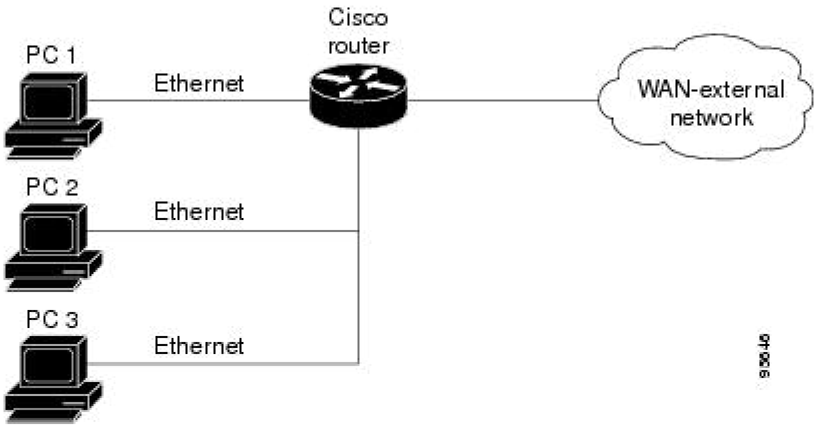
On the router, the receipt of the EAPOL-Start message will result in the source MAC address being "remembered," and an EAPOL-request or identity PDU being sent to the host. The router will send all host-addressed PDUs to the individual MAC address of the host rather than to the multicast address.

- 802.1X Authentication Sample Topology and Configuration, page 49
- Converged 802.1X Authenticator Support, page 49
- 802.1X Supplicant Support, page 49
- Converged 802.1X Supplicant Support, page 50

802.1X Authentication Sample Topology and Configuration

The figure below illustrates a typical scenario in which VPN access control using 802.1X authentication is in place.

Figure 3 Typical 802.1X Authentication Setup



In the figure above, all the PCs are 802.1X capable hosts, and the Cisco router is an authenticator. All the PCs are connected to the built-in hub or to an external hub. If a PC does not support 802.1X authentication, MAC-based authentication is supported on the Cisco router. You can have any kind of connectivity or network beyond the Cisco router WAN.

Note If there is a switch located between the router and the supplicant (client PC), the EAPOL frames will not reach the router because the switch discards them.

- A supplicant is an entity at one end of a point-to-point LAN segment that is being authenticated by an authenticator that is attached to the other end of that link.

Converged 802.1X Authenticator Support

The Cisco IOS commands in Cisco IOS Release 12.4(6)T for 802.1X authenticators have been standardized to work the same way on various Cisco IOS platforms.

802.1X Supplicant Support

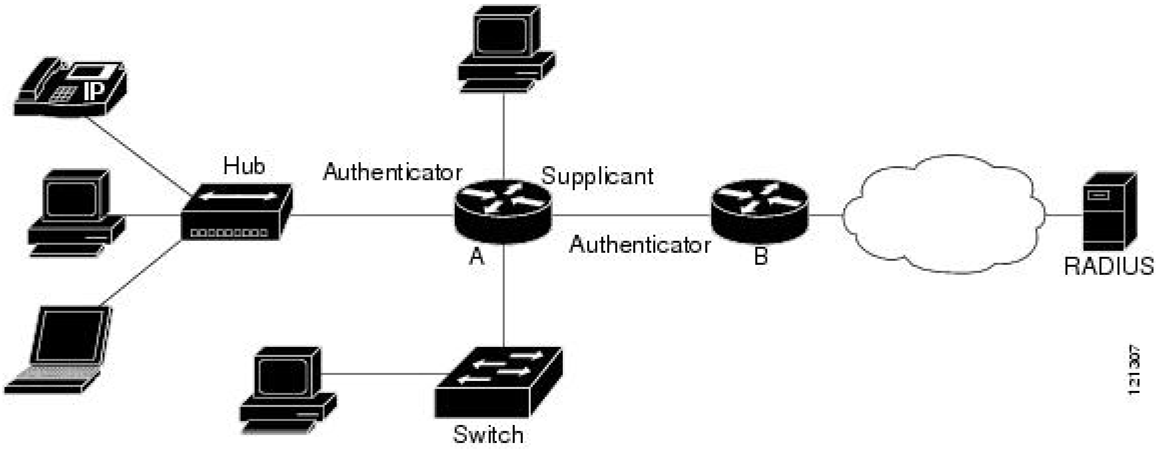
There are deployment scenarios in which a network device (a router acting as an 802.1X authenticator) is placed in an unsecured location and cannot be trusted as an authenticator. This scenario requires that a network device be able to authenticate itself against another network device. The 802.1X supplicant support functionality provides the following solutions for this requirement:

- An Extensible Authentication Protocol (EAP) framework has been included so that the supplicant has the ability to “understand” and “respond” to EAP requests. EAP-Message Digest 5 (EAP-MD5) is currently supported.
- Two network devices that are connected through an Ethernet link can act as a supplicant and as an authenticator simultaneously, thus providing mutual authentication capability.
- A network device that is acting as a supplicant can authenticate itself with more than one authenticator (that is, a single port on a supplicant can be connected to multiple authenticators).

The following illustration is an example of 802.1X supplicant support. The illustration shows that a single supplicant port has been connected to multiple authenticators. Router A is acting as an authenticator to devices that are sitting behind it on the LAN while those devices are acting as supplicants. At the same time, Router B is an authenticator to Router A (which is acting as a supplicant). The RADIUS server is located in the enterprise network.

When Router A tries to authenticate devices on the LAN, it needs to “talk” to the RADIUS server, but before it can allow access to any of the devices that are sitting behind it, it has to prove its identity to Router B. Router B checks the credential of Router A and gives access.

Figure 4 Multiple Instances of Supplicant Support



Converged 802.1X Supplicant Support

The Cisco IOS commands in Cisco IOS Release 12.4(6)T for 802.1X supplicants have been standardized to work the same way on various Cisco IOS platforms. See the Configuring a Router As an 802.1X Supplicant module.

Authentication Using Passwords and MD5

For information about using passwords and Message Digest 5 (MD5), see the following document on Cisco.com:

- Improving Security on Cisco Routers

How to Configure VPN Access Control Using 802.1X Authentication

Configuring a AAA RADIUS Server

To configure an AAA RADIUS server, perform the following steps.

SUMMARY STEPS

1. Configure entries for the network access server and associated shared secrets.
2. Add the username and configure the password of the user.
3. Configure a global or per-user authentication scheme.

DETAILED STEPS

Step 1 Configure entries for the network access server and associated shared secrets.

Note The AAA server can be FreeRADIUS or Cisco Secure ACS or any other similar product with 802.1X support.

Step 2 Add the username and configure the password of the user.

Step 3 Configure a global or per-user authentication scheme.

Configuring a Router

Enabling 802.1X Authentication

To enable 802.1X port-based authentication, you should configure the router so that it can communicate with the AAA server, enable 802.1X globally, and enable 802.1X on the interface. To enable 802.1X port-based authentication, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication dot1x** {**default** | *listname*} *method1* [*method2...*]
5. **dot1x system-auth-control**
6. **identity profile default**
7. **interface** *type slot* / *port*
8. **dot1x port-control auto**

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 dot1x** {**default** | *listname*} *method1* [*method2...*] **Example:** `Router (config)# aaa authentication dot1x default group radius`	Creates a series of authentication methods that are used to determine user previlege to access the privileged command level.

	Command or Action	Purpose
Step 5	**dot1x system-auth-control** **Example:** `Router (config)# dot1x system-auth-control`	Globally enables 802.1X port-based authentication.
Step 6	**identity profile default** **Example:** `Router (config)# identity profile default`	Creates an identity profile and enters dot1x profile configuration mode.
Step 7	**interface** *type slot* / *port* **Example:** `Router (config-identity-prof)# interface fastethernet 0/1`	Enters interface configuration mode and specifies the interface to be enabled for 802.1X port-based authentication.
Step 8	**dot1x port-control auto** **Example:** `Router (config-if)# dot1x port-control auto`	Enables 802.1X port-based authentication on the interface.

Examples

The following example shows that 802.1X authentication has been configured on a router:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius group radius
Router(config)# dot1x system-auth-control
Router(config)# interface fastethernet 1
Router(config-if)# dot1x port-control auto
```

The following **show dot1x** command sample output shows that 802.1X authentication has been configured on a router:

```
Router# show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version           2
Dot1x Info for FastEthernet1
-----------------------------------
PAE                        = AUTHENTICATOR
PortControl                = AUTO
ControlDirection           = Both
HostMode                   = MULTI_HOST
ReAuthentication           = Enabled
QuietPeriod                = 600
ServerTimeout              = 60
SuppTimeout                = 30
ReAuthPeriod               = 1800 (Locally configured)
ReAuthMax                  = 2
MaxReq                     = 3
```

```
TxPeriod                  = 60
RateLimitPeriod           = 60
```

Configuring Router and RADIUS Communication

To configure RADIUS server parameters, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip radius source-interface** *interface-name*
4. **radius-server host** {*hostname* | *ip-address*}
5. **radius-server key** *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	**ip radius source-interface** *interface-name* **Example:** `Router (config)# ip radius source-interface fastethernet1`	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.

Step 4	**radius-server host** {*hostname* | *ip-address*}
	Example:
	`Router (config)# radius-server host 192.0.2.0`
		Configures the RADIUS server host name or IP address of the router.
		• To use multiple RADIUS servers, reenter this command for each server.

	Command or Action	Purpose
Step 5	**radius-server key** *string* **Example:** `Router (config)# radius-server key radiuskey`	Configures the authorization and encryption key used between the router 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.

Example

The following example shows that RADIUS server parameters have been configured on the router:

```
Router# configure terminal
Router(config)# ip radius source-interface ethernet1
Router(config)# radius-server host 192.0.2.1
Router(config)# radius-server key radiuskey
```

Configuring 802.1X Parameters Retransmissions and Timeouts

Various 802.1X retransmission and timeout parameters can be configured. Because all of these parameters have default values, configuring them is optional. To configure the retransmission and timeout parameters, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *port*
4. **dot1x max-req** *number-of-retries*
5. **dot1x port-control** [**auto**| **force-authorized**| **force-unauthorized**]
6. **dot1x control-direction** {**both** | **in**}
7. **dot1x reauthentication**
8. **dot1x timeout tx-period** *seconds*
9. **dot1x timeout server-timeout** *seconds*
10. **dot1x timeout reauth-period** *seconds*
11. **dot1x timeout quiet-period** *seconds*
12. **dot1x timeout ratelimit-period** *seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot* / *port* **Example:** `Router (config)# interface FastEthernet 0/1`	Enters interface configuration mode and specifies the interface to be enabled for 802.1X port-based authentication.
Step 4	**dot1x max-req** *number-of-retries* **Example:** `Router (config-if)# dot1x max-req 3`	Sets the maximum number of times that the router sends an EAP request/ identity frame (assuming that no response is received) to the supplicant before concluding that the supplicant does not support 802.1X.
Step 5	**dot1x port-control** [**auto**| **force-authorized**| **force-unauthorized**] **Example:** `Router (config-if)# dot1x port-control auto`	Sets the port control value. • **auto (optional)** --Authentication status of the supplicant will be determined by the authentication process. • **force-authorized (optional)** --All the supplicants on the interface will be authorized. The **force-authorized** keyword is the default. • **force-unauthorized (optional)** --All the supplicants on the interface will be unauthorized.

Step 6	**dot1x control-direction** {**both** | **in**}
	Example:
	`Router (config-if)# dot1x control-direction both`
		Changes the port control to unidirectional or bidirectional.

Step 7	**dot1x reauthentication** **Example:** `Router (config-if)# dot1x reauthentication`	Enables periodic reauthentication of the supplicants on the interface. • The reauthentication period can be set using the **dot1x timeout** command.

	Command or Action	Purpose
Step 8	**dot1x timeout tx-period** *seconds* **Example:** `Router (config-if)# dot1x timeout tx-period 60`	Sets the timeout for supplicant retries. • If an 802.1X packet is sent to the supplicant and the supplicant does not send a response, the packet will be sent again after the time that was set using the *seconds* argument. • The value is 1 through 65535 seconds. The default is 30 seconds.
Step 9	**dot1x timeout server-timeout** *seconds* **Example:** `Router (config-if)# dot1x timeout server-timeout 60`	Sets the timeout for RADIUS retries. • If an 802.1X packet is sent to the server, and the server does not send a response, the packet will be sent again after the time that was set using the *seconds* argument. • The value is from 1 to 65535 seconds. The default is 30 seconds.
Step 10	**dot1x timeout reauth-period** *seconds* **Example:** `Router (config-if)# dot1x timeout reauth-period 1800`	Sets the time after which an automatic reauthentication should be initiated. • The value is from 1 to 65535 seconds. The default is 3600 seconds.
Step 11	**dot1x timeout quiet-period** *seconds* **Example:** `Router (config-if)# dot1x timeout quiet-period 600`	The time after which authentication is restarted after the authentication has failed. • The value is from 1 to 65535 seconds. The default is 120 seconds.
Step 12	**dot1x timeout ratelimit-period** *seconds* **Example:** `Router (config-if)# dot1x timeout ratelimit-period 60`	The rate limit period throttles the EAP-START packets from misbehaving supplicants. • The value is from 1 to 65535 seconds.

Examples

The following configuration example shows that various retransmission and timeout parameters have been configured:

```
Router# configure terminal

Router(config)# interface FastEthernet1

Router(config-if)# dot1x port-control auto

Router(config-if)# dot1x reauthentication

Router(config-if)# dot1x timeout reauth-period 1800

Router(config-if)# dot1x timeout quiet-period 600

Router(config-if)# dot1x timeout supp-timeout 60

Router(config-if)# dot1x timeout server-timeout 60
```

Configuring the Identity Profile

The **identity profile default** command allows you to configure the static MAC addresses of the client that do not support 802.1X and to authorize or unauthorize them statically. The VPN Access Control Using 802.1X Authentication feature allows authenticated and unauthenticated users to be mapped to different interfaces. Under the **dot1x profile** configuration mode, you can specify the virtual template interface that should be used to create the virtual-access interface to which unauthenticated supplicants will be mapped. To specify which virtual template interface should be used to create the virtual access interface, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **identity profile default**
4. **description** *line-of-description*
5. **template** *virtual-template*
6. **device** [**authorize** | **not-authorize**] **mac-address** *mac-address*
7. **device authorize type** *device-type*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**identity profile default** **Example:** `Router (config)# identity profile default`	Creates an identity profile and enters identity profile configuration mode.
Step 4	**description** *line-of-description* **Example:** `Router (config-identity-prof)# description description 1`	Associates descriptive text with the profile.
Step 5	**template** *virtual-template* **Example:** `Router (config-identity-prof)# template virtual-template 1`	Specifies the virtual template interface that will serve as the configuration clone source for the virtual interface that is dynamically created for authenticated users.
Step 6	**device** [**authorize** | **not-authorize**] **mac-address** *mac-address* **Example:** `Router (config-identity-prof)# device authorize mac-address 1.1.1`	Statically authorizes or unauthorizes a supplicant (by giving its MAC address) if the supplicant does not "understand" 802.1X.
Step 7	**device authorize type** *device-type* **Example:** `Router (config-identity-prof)# device authorize type cisco ip phone`	Statically authorizes or unauthorizes a device type.

Examples

The following example shows that Cisco IP phones and a specific MAC address have been statically authorized:

```
Router# configure terminal
Router (config)# identity profile default
Router(config-1x-prof)# description put the description here
Router(config-1x-prof)# template virtual-template1
Router(config-1x-prof)# device authorize type cisco ip phone
Router(config-1x-prof)# device authorize mac-address 0001.024B.B4E7
```

Configuring the Identity Profile

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **identity profile default**
4. **description** *description-string*
5. **template** *virtual-template*
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	**identity profile default** **Example:** `Router (config)# identity profile default`	Creates an identity profile and enters identity profile configuration mode.
Step 4	**description** *description-string* **Example:** `Router (config-identity-prof)# description description_string_goes_here`	Associates descriptive text with the identity profile.
Step 5	**template** *virtual-template* **Example:** `Router (config-identity-prof)# template virtualtemplate1`	Specifies the virtual template interface that will serve as the configuration clone source for the virtual interface that is dynamically created for authenticated users.
Step 6	**exit** **Example:** `Router (config-template)# exit`	Exits identity profile configuration mode.

Configuring the DHCP Private Pool

The VPN Access Control Using 802.1X Authentication feature can be configured with one DHCP pool or two. If there are two pools, the unauthenticated and authenticated devices will get their addresses from separate DHCP pools. For example, the public pool can have an address block that has only local significance, and the private pool can have an address that is routable over the VPN tunnel.

SUMMARY STEPS

1. **ip dhcp pool** *name*
2. **network** *network-number* [*mask*]
3. **default-router** *address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ip dhcp pool** *name* **Example:** `Router (config)# ip dhcp pool private`	Configures a DHCP private address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
Step 2	**network** *network-number* [*mask*] **Example:** `Router (dhcp-config)# network 209.165.200.225 255.255.255.224`	Configures the subnet number and mask for a DHCP private address pool on a Cisco IOS DHCP server.
Step 3	**default-router** *address* **Example:** `Router (dhcp-config)# default-router 192.0.2.2`	Specifies the default router list for a DHCP client.

Configuring the DHCP Public Pool

The VPN Access Control Using 802.1X Authentication feature can be configured with one DHCP pool or two. If there are two pools, the unauthenticated and authenticated devices will get their addresses from separate DHCP pools. For example, the public pool can have an address block that has only local significance, and the private pool can have an address that is routable over the VPN tunnel.

SUMMARY STEPS

1. **ip dhcp pool** *name*
2. **network** *network-number* [*mask*]
3. **default-router** *address*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ip dhcp pool** *name* **Example:** `Router (config-dhcp)# ip dhcp pool public`	Configures the DHCP public address pool on a Cisco IOS DHCP server.

	Command or Action	Purpose
Step 2	**network** *network-number* [*mask*] **Example:** `Router (config-dhcp)# network 209.165.200.226 255.255.255.224`	Configures the subnet number and mask for a DHCP public address pool on a Cisco IOS DHCP server.
Step 3	**default-router** *address* **Example:** `Router (config-dhcp)# default-router 192.0.2.3`	Specifies the default router list for a DHCP client.
Step 4	**exit** **Example:** `Router (config-dhcp)# exit`	Exits DHCP pool configuration mode.

Configuring the Interface

SUMMARY STEPS

1. **configure terminal**
2. **interface** *type slot* / *port*
3. **ip address** *ip-address mask* [**secondary**]
4. **interface virtual-template** *number*
5. **ip address** *ip-address mask* [**secondary**]
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**interface** *type slot* / *port* **Example:** `Router (config)# interface loopback 0/1`	Enters interface configuration mode and specifies the interface to be enabled.
Step 3	**ip address** *ip-address mask* [**secondary**] **Example:** `Router (config-if)# ip address 209.165.200.227 255.255.255.224`	Sets the private IP address for the interface.
Step 4	**interface virtual-template** *number* **Example:** `Router (config-if)# interface virtual-template 1`	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
Step 5	**ip address** *ip-address mask* [**secondary**] **Example:** `Router (config-if)# ip address 209.165.200.227 255.255.255.224`	Sets the public IP address for the interface.
Step 6	**exit** **Example:** `Router (config-if)# exit`	Exits interface configuration mode.

Configuring an Interface Without Assigning an Explicit IP Address to the Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *port*
4. **ip unnumbered** *type number*

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 virtual-template 1`	Enters interface configuration mode and specifies the interface to be enabled.
Step 4	**ip unnumbered** *type number* **Example:** `Router (config-if)# ip unnumbered loopback 0`	Enables IP processing on an interface without assigning an explicit IP address to the interface.

Example

The following example shows that the identity profile associates virtual-template1 with unauthenticated supplicants. Virtual-template1 gets its IP address from interface loopback 0, and unauthenticated supplicants are associated with a public pool. Authenticated users are associated with a private pool.

```
Router(config)# identity profile default
Router(config-identity-prof)# description put the description here
Router(config-identity-prof)# template virtual-template1
Router(config-identity-prof)# exit
Router(config)# ip dhcp pool private
Router(dhcp-config)# default-router 192.0.2.0
Router(dhcp-config)# exit
Router(config)#ip dhcp pool public
Router(dhcp-config)# default-router 192.0.2.1
Router(dhcp-config)# exit
Router(config)# interface
Router(dhcp-config)# network 209.165.200.225 255.255.255.224
Router(dhcp-config)# default-router 192.0.2.1
Router(dhcp-config)# exit
Router(config)# interface loopback0
Router(config-if)# interface ethernet0
Router(config-if)# ip address 209.165.200.226 255.255.255.224
Router(config-if)# exit
Router(config)# interface virtual-template1
Router(config-if)# ip unnumbered loopback 0
```

Configuring the Necessary Access Control Policies

802.1X authentication separates traffic from authenticated and unauthenticated devices. Traffic from authenticated devices transit through the physical interface, and unauthenticated traffic transits through the Virtual-Template1. Therefore, different policies can be applied on each interface. The configuration will also depend on whether two DHCP pools or a single DHCP pool is being used. If a single DHCP pool is being used, access control can be configured on Virtual-Template1, which will block any traffic from going to the networks to which unauthenticated devices should not have access. These networks (to which unauthenticated devices should not have access) could be the corporate subnetworks protected by the VPN or encapsulated by generic routing encapsulation (GRE). There can also be access control that restricts the access between authenticated and unauthenticated devices.

If two pools are configured, the traffic from a non-trusted pool is routed to the Internet using Network Address Translation (NAT), whereas trusted pool traffic is forwarded through a VPN tunnel. The routing can be achieved by configuring ACLs used by NAT and VPN accordingly.

For an example of an access control policy configuration, see the Access Control Policies Example section.

Configuring a PC As an 802.1X Supplicant

Configuring a PC for VPN Access Control Using 802.1X Authentication

To configure your PC for VPN Access Control Using 802.1X Authentication, perform the following steps.

SUMMARY STEPS

1. Enable 802.1X for MD5.
2. Enable DHCP.

DETAILED STEPS

Step 1 Enable 802.1X for MD5.

Step 2 Enable DHCP.

Enabling 802.1X Authentication on a Windows 2000 XP PC

802.1X implementation on a Windows 2000/XP PC is unstable. A more stable 802.1X client, AEGIS (beta) for Microsoft Windows, is available at the Meetinghouse Data Communications website at www.mtghouse.com.

Enabling 802.1X Authentication on a Windows 2000 PC

To enable 802.1X authentication on your Windows 2000 PC, perform the following steps.

SUMMARY STEPS

1. Make sure that the PC has at least Service Pack 3.
2. Reboot your PC after installing the client.
3. Go to the Microsoft Windows registry and add or install the following entry:
4. Reboot your PC.

DETAILED STEPS

Step 1 Make sure that the PC has at least Service Pack 3.
Go to the page “Microsoft 802.1x Authentication Client” on the Microsoft Windows 2000 website at the following URL:

http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/8021xclient.asp.

At the above site, download and install 802.1X client for Windows 2000.

If the above site is unavailable, search for the “Q313664: Recommended Update” page on the Microsoft Windows 2000 website at the following URL: http://www.microsoft.com/windows2000/downloads/recommended/q313664/default.asp

Step 2 Reboot your PC after installing the client.

Step 3 Go to the Microsoft Windows registry and add or install the following entry:
“HKLM\Software\Microsoft\EAPOL\Parameters\General\Global\SupplicantMode REG_DWORD 3”

(“SupplicantMode” key entry is not there by default under Global option in the registry. So add a new entry named “SupplicantMode” as REG_DOWORD and then set its value to 3.)

Step 4 Reboot your PC.

Enabling 802.1X Authentication on a Windows XP PC

To enable 802.1X authentication on a Windows XP PC, perform the following steps.

SUMMARY STEPS

1. Go to the Microsoft Windows registry and install the following entry there:
2. Reboot your PC.

DETAILED STEPS

Step 1 Go to the Microsoft Windows registry and install the following entry there:
“HKLM\Software\Microsoft\EAPOL\Parameters\General\Global\SupplicantMode REG_DWORD 3”

Step 2 Reboot your PC.

Enabling 802.1X Authentication on Windows 2000 and Windows XP PCs

To enable 802.1X authentication on Windows 2000 and Windows XP PCs, that is, if you are operating both at the same time, perform the following steps.

SUMMARY STEPS

1. Open the Network and Dial-up Connections window on your computer.
2. Right-click the Ethernet interface (Local Area Connection) to open the properties window. It should have a tab called “Authentication.”

DETAILED STEPS

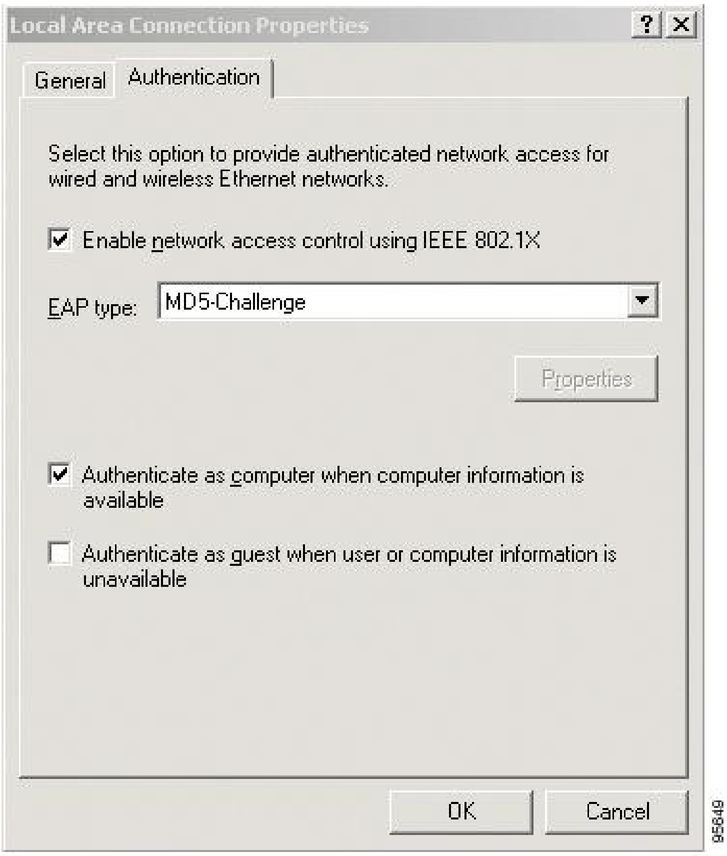
Step 1 Open the Network and Dial-up Connections window on your computer.

Step 2 Right-click the Ethernet interface (Local Area Connection) to open the properties window. It should have a tab called “Authentication.”

Click the Authentication tab. Select the check box titled “Enable network access control using IEEE 802.1X.”

In a short period of time you should see a dialog box (for Windows 2000) or a floating window asking you to select it. Select it, and when the next window appears, enter the username and password in this dialog box. See the figure below.

Figure 5 ***Local Area Connection Properties Window***



Local Area Connection Properties

Select this option to provide authenticated network access for wired and wireless Ethernet networks.

☑ Enable network access control using IEEE 802.1X

EAP type: MD5-Challenge

☑ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

Configuring a Router As an 802.1X Supplicant

To configure a router as an 802.1X supplicant, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authentication dot1x** {**default** | *listname*} *method1* [*method2...*]
4. **dot1x credentials** *name*
5. **username** *name*
6. **password** [**0** | **7**] *password*
7. **exit**
8. **interface** *type number*
9. **dot1x pae supplicant**
10. **dot1x credentials** *name*
11. **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	**aaa authentication dot1x** {**default** | *listname*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication dot1x default group radius`	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X.
Step 4	**dot1x credentials** *name* **Example:** `Router(config)# dot1x credentials name1`	Specifies the 802.1X credential profile to use when configuring a supplicant.

	Command or Action	Purpose
Step 5	**username** *name* **Example:** `Router(config-dot1x-creden)# username username1`	Specifies the username for an 802.1X credentials profile.
Step 6	**password** [**0** | **7**] *password* **Example:** `Router(config-dot1x-creden)# password 0 password1`	Specifies the password for an 802.1X credentials profile.
Step 7	**exit** **Example:** `Router(config-dot1x-creden)# exit`	Enters global configuration mode.
Step 8	**interface** *type number* **Example:** `Router(config)# interface Fastethernet0/0`	Enters interface configuration mode.
Step 9	**dot1x pae supplicant** **Example:** `Router(config-if)# dot1x pae supplicant`	Sets the Port Access Entity (PAE) type as supplicant.
Step 10	**dot1x credentials** *name* **Example:** `Router(config-if)# dot1x credentials name1`	Specifies the 802.1X credential profile to use when configuring a supplicant.

Step 11	**end**
	Example:
	`Router(config-if)# end`
		(Optional) Exits the current configuration mode.

- Troubleshooting Tips, page 71

Troubleshooting Tips

Use the debug commands in the Monitoring VPN Access Control Using 802.1X Authentication section to debug the supplicant.

Monitoring VPN Access Control Using 802.1X Authentication

To monitor VPN Access Control Using 802.1X Authentication, perform the following steps. The commands shown in the steps may be used one at a time and in no particular order.

SUMMARY STEPS

1. **enable**
2. **clear dot1x** {**all** | **interface**}
3. **clear eap sessions** [**credentials** *credentials-name* | **interface** *interface-name* | **method** *method-name* | **transport***transport-name*]]
4. **debug dot1x [all | errors | events | feature | packets | redundancy | registry | state-machine]**
5. **debug eap** [**all** | *method*] [**authenticator** | **peer**] {**all** | **errors** | **events** | **packets** | **sm**}
6. **dot1x initialize** [**interface** *interface-name*]
7. **dot1x re-authenticate** *interface-type interface-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	**clear dot1x** {**all** | **interface**}
	Example:
	`Router# clear dot1x all`
		Clears 802.1X interface information.

Step 3	**clear eap sessions** [**credentials** *credentials-name* | **interface** *interface-name* | **method** *method-name* | **transport***transport-name*]] **Example:** `Router# clear eap sessions credentials type1`	Clears EAP information on a switch or for a specified port.

	Command or Action	Purpose
Step 4	**debug dot1x [all | errors | events | feature | packets | redundancy | registry | state-machine]** **Example:** `Router# debug dot1x all`	Displays 802.1X debugging information. • **all** -Enables all 802.1X debugging messages. • **errors** -Provides information about all 802.1X errors. • **events** -Provides information about all 802.1X events. • **feature** -Provides information about 802.1X features for switches only. • **packets** -Provides information about all 802.1X packets. • **redundancy** -Provides information about 802.1X redundancy. • **registry** -Provides information about 802.1X registries. • **state-machine** --Provides information regarding the 802.1X state machine.

Step 5	**debug eap** [**all** | *method*] [**authenticator** | **peer**] {**all** | **errors** | **events** | **packets** | **sm**}
	Example:
	`Router# debug eap all`
		Displays information about EAP.

Step 6	**dot1x initialize** [**interface** *interface-name*] **Example:** `Router# dot1x initialize interface FastEthernet1`	Initializes an interface.
Step 7	**dot1x re-authenticate** *interface-type interface-number* **Example:** `Router# dot1x re-authenticate FastEthernet1`	Reauthenticates all the authenticated devices that are attached to the specified interface.

Verifying VPN Access Control Using 802.1X Authentication

To verify VPN Access Control Using 802.1X Authentication, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show dot1x** [**interface** *interface-name*[**details**]]
3. **show eap registrations** [**method** | **transport**]
4. **show eap sessions** [**credentials** *credentials-name* | **interface***interface-name* | **method** *method-name* | **transport** *transport-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show dot1x** [**interface** *interface-name*[**details**]] **Example:** `Router# show dot1x interface FastEthernet 1 details`	Shows details for an identity profile.
Step 3	**show eap registrations** [**method** | **transport**] **Example:** `Router# show eap registrations method`	Displays EAP registration information.
Step 4	**show eap sessions** [**credentials** *credentials-name* | **interface***interface-name* | **method** *method-name* | **transport** *transport-name*] **Example:** `Router# show eap sessions interface gigabitethernet1/0/1`	Displays active EAP session information.

Configuration Examples for VPN Access Control Using 802.1X Authentication

- Typical VPN Access Control Using 802.1X Configuration Example, page 74
- Access Control Policies Example, page 77

Typical VPN Access Control Using 802.1X Configuration Example

The following sample output shows that VPN access control using 802.1X authentication has been configured. Output is shown for the router and for the gateway.

Router

```
Router# show running-config
Building configuration...
Current configuration : 2457 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 871-1
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
aaa new-model
!
!
aaa authentication dot1x default group radius group radius
!
!
aaa session-id common
!
!
dot11 syslog
ip source-route
!
ip dhcp pool private
   network 209.165.200.225 255.255.255.224
   default-router 192.0.2.18
!
ip dhcp pool public
   network 209.165.200.226 255.255.255.224
   default-router 192.0.2.17
!
ip dhcp pool name
   default-router 192.0.2.16
!
!
ip cef
no ip domain lookup
ip host sjc-tftp02 192.0.2.15
ip host sjc-tftp01 192.0.2.14
ip host dirt 192.0.2.13
!
!
!
template virtualtemplate1
!
dot1x system-auth-control
dot1x credentials basic-user
 description This credentials profile should be used for most configured ports
 username router1
 password 0 secret
!
identity profile default
 description description 1
 device authorize mac-address 0001.024b.b4e7
 device authorize mac-address 0001.0001.0001
 device authorize type cisco ip phone
 template Virtual-Template1
!
!
!
!
!
archive
 log config
  hidekeys
!
!
!
!
!
interface Loopback0
 ip address 209.165.200.227 255.255.255.224
!
interface FastEthernet0
!
interface FastEthernet1
 dot1x pae authenticator
 dot1x port-control auto
 dot1x timeout quiet-period 600
 dot1x timeout server-timeout 60
 dot1x timeout reauth-period 1800
 dot1x timeout tx-period 60
 dot1x timeout ratelimit-period 60
 dot1x max-req 3
 dot1x reauthentication
!
interface FastEthernet2
!
interface FastEthernet3
!
interface FastEthernet4
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Virtual-Template1
 ip unnumbered Loopback0
!
interface Dot11Radio0
 no ip address
 shutdown
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0
 station-role root
 no cdp enable
!
interface Vlan1
 ip address 209.165.200.228 255.255.255.224
!
ip default-gateway 192.0.2.10
ip default-network 192.0.2.11
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.0.2.11
ip route 209.165.200.229 255.255.255.224 192.0.2.12
no ip http server
no ip http secure-server
!
!
ip radius source-interface FastEthernet1
!
!
!
radius-server host 192.0.2.9 auth-port 1645 acct-port 1646
radius-server key radiuskey
!
control-plane
!
!
line con 0
```

```
 exec-timeout 30 0
 logging synchronous
 no modem enable
line aux 0
line vty 0 4
 privilege level 15
 password lab
!
scheduler max-task-time 5000
end
```

Peer Router As Gateway

```
Router# show running-config
Building configuration...
Current configuration: 1828 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname c3725
!
!
no aaa new-model
ip subnet-zero
!
vpdn enable
!
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
!
mpls ldp logging neighbor-changes
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key 0 test address 192.0.2.8
!
!
crypto ipsec transform-set t1 ah-md5-hmac esp-des
crypto mib ipsec flowmib history tunnel size 2
crypto mib ipsec flowmib history failure size 2
!
crypto map test 1 ipsec-isakmp
 set peer 192.0.2.7
 set transform-set t1
 match address 101
!
no voice hpi capture buffer
no voice hpi capture destination
!
interface Loopback0
 description corporate
 ip address 209.165.200.230 255.255.255.224
!
interface Loopback1
 description internet
 ip address 209.165.200.231 255.255.255.224
!
interface FastEthernet0/0
 ip address 209.165.200.232 255.255.255.224
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 speed auto
 half-duplex
 pppoe enable
```

```
!
interface ATM1/0
 ip address 209.165.200.233 255.255.255.224
 no atm ilmi-keepalive
 pvc 1/43
  protocol ip 192.0.2.6 broadcast
  encapsulation aal5snap
!
!
interface FastEthernet2/0
 no ip address
 speed auto
 full-duplex
!
interface FastEthernet2/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Virtual-Template1
 ip address 209.165.200.234 255.255.255.224
 ip mtu 1492
 crypto map test
!
!
router rip
 network 192.0.2.5
 network 192.0.2.4
 network 192.0.2.3
 network 192.0.2.2
 network 192.0.2.1
!
ip http server
no ip http secure-server
ip classless
!
access-list 101 permit ip 10.5.0.0 0.0.0.255 10.0.0.1 0.0.0.255
no cdp log mismatch duplex
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
!
end
```

Access Control Policies Example

The following output example shows that access control policies have been configured.

Single DHCP pool

```
ip dhcp pool private
 network 209.165.200.236 255.255.255.224
 default-router 20.0.0.1
 exit
crypto isakmp policy 1
 authentication pre-share
!
crypto isakmp key test address address
 crypto ipsec transform-set t1 esp-3des esp-sha-hmac
 mode tunnel
 crypto map test 1 ipsec-isakmp
 set peer address
 set transform-set t1
 match address 101
 access-list 101 permit ip 10.0.0.0 0.0.0.255 50.0.0.0 0.0.0.255
 access-list 102 deny ip 10.0.0.0 0.0.0.255 50.0.0.0 0.0.0.255
 access-list 102 permit  ip any any
!
interface Ethernet0
! inside interface
! dot1x configs
!
interface Virtual-Template1
! Deny traffic from going to VPN
 ip access-group 102 in
!
Interface Ethernet1
! outside interface
 crypto map test
```

Two DHCP Pools

```
ip dhcp pool private
 network 209.165.200.237 255.255.255.224
 default-router 192.0.2.1
 exit
!
ip dhcp pool public
 network 209.165.200.238 255.255.255.224
 default-router 192.0.2.0
 exit
!
crypto isakmp policy 1
 authentication pre-share
!
crypto isakmp key test address address
 crypto ipsec transform-set t1 esp-3des esp-sha-hmac
 mode tunnel
 crypto map test 1 ipsec-isakmp
 set peer address
 set transform-set t1
 match address 101
 access-list 101 permit ip 10.0.0.0 0.0.0.255 10.10.0.0 0.0.0.255
 access-list 102 permit ip 10.0.0.1 0.0.0.255 any
!
interface Ethernet0
!inside interface
! dot1x configs
!
interface Loopback0
 ip address 209.165.200.239 255.255.255.224
!
interface Virtual-Template1
 ip unnumbered Loopback0
 ip nat inside
!
Interface Ethernet1
! outside interface
 crypto map test
 ip nat outside
!
ip nat inside source list 102 interface Ethernet1 overload
```

Additional References

Related Documents

Related Topic	Document Title
Configuring 802.1X port-based authentication	Configuring IEEE 802.1X Port-Based Authentication module.
DHCP	*Cisco IOS IP Addressing Services Configuration Guide*
IPSec	*Cisco IOS Security Configuration Guide: Secure Connectivity*, Release 15.0.
RADIUS	Configuring RADIUS module.
Security commands	*Cisco IOS Security Command Reference*
User lists on a Cisco ACS	*User Guide for Cisco Secure ACS for Windows Server* Version 3.2.

Standards

Standard	Title
IEEE 802.1X protocol	--

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

RFCs

RFC	Title
RFC-2284	*RFC 2284 (PPP Extensible Authentication Protocol [EAP])* document from The Internet Requests for Comments (RFC) document series

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 VPN Access Control Using 802.1X Authentication

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 VPN Access Control Using 802.1X Authentication

Feature Name	Releases	Feature Information
VPN Access Control Using 802.1X Authentication	12.3(2)XA	The VPN Access Control Using 802.1X Authentication feature was introduced. This feature allows enterprise employees to access their enterprise networks from home while allowing other household members to access only the Internet.
VPN Access Control Using 802.1X Authentication	12.3(4)T	This feature was integrated into Cisco IOS Release 12.3(4)T, and the following platform support was added: Cisco 1751, Cisco 2610XM - Cisco 2611XM, Cisco 2620XM - Cisco 2621XM, Cisco 2650XM - Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.
802.1X Supplicant Support	12.3(11)T	802.1X supplicant support was added.

Feature Name	Releases	Feature Information
Converged 802.1X Authenticator and Converged 802.1X Supplicant Support	12.4(6)T	Converged 802.1X authenticator and converged 802.1X supplicant support was added. (This update is a standardization of Cisco IOS 802.1X commands for various Cisco IOS platforms. This is no change in 802.1X features.) Affected commands include the following: **clear eap , debug dot1x , debug eap , description (dot1x credentials) , dot1x control-direction , dot1x credentials , dot1x default , dot1x host-mode , dot1x max-reauth-req , dot1x max-start , dot1x multiple-hosts , dot1x timeout , eap , identity profile , password (dot1x credentials) , show eap registrations , show eap sessions**, and **username**
VPN Access Control Using 802.1X Authentication	12.4(4)XC	Various 802.1X commands were integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only. Affected commands include the following: **dot1x control-direction , dot1x default , dot1x guest-vlan , dot1x host-mode , dot1x max-reauth-req , dot1x max-req , dot1x max-start , dot1x pae , dot1x port-control , dot1x re-authenticate (privileged EXEC) , dot1x reauthentication , dot1x system-auth-control , dot1x timeout, macro global , macro name**, and **show ip igmp snooping**

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.