



VPN Access Control Using 802.1X Authentication

First Published: August 11, 2003

Last Updated: June 2, 2006

The home access router provides connectivity to the corporate network via 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.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for VPN Access Control Using 802.1X Authentication”](#) section on page 103.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for VPN Access Control Using 802.1X Authentication, page 2](#)
- [Restrictions for VPN Access Control Using 802.1X Authentication, page 2](#)
- [Information About VPN Access Control Using 802.1X Authentication, page 2](#)
- [How to Configure VPN Access Control Using 802.1X Authentication, page 5](#)
- [Configuration Examples for VPN Access Control Using 802.1X Authentication, page 24](#)
- [Additional References, page 31](#)



Corporate Headquarters:

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

Copyright © 2003 – 2006 Cisco Systems, Inc. All rights reserved.

- [Command Reference, page 32](#)
- [Feature Information for VPN Access Control Using 802.1X Authentication, page 103](#)

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

To configure the VPN Access Control Using 802.1X Authentication feature, you should understand the following concepts:

- [How VPN Control Using 802.1X Authentication Works, page 2](#)
- [802.1X Supplicant Support, page 4](#)
- [Authentication Using Passwords and MD5, page 5](#)

How VPN Control Using 802.1X Authentication Works

The home access router provides connectivity to the corporate network via 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.

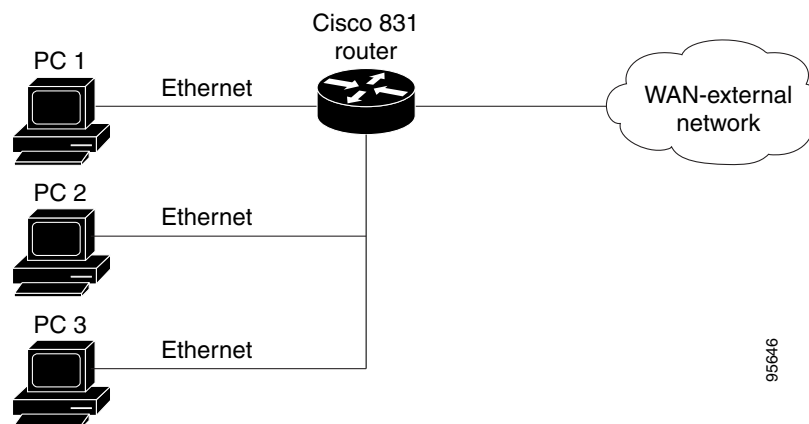
All 802.1X PDUs will be identified as such by the Ethernet driver and will be enqueued to be handled by an 802.1X process. On some platforms, Ethernet drivers have to program the interface address filter so that EAPOL packets can be accepted.

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

Figure 1 illustrates a typical scenario in which VPN access control using 802.1X authentication is in place.

Figure 1 Typical 802.1X Authentication Setup



In Figure 1, all the PCs are 802.1X capable hosts, and the Cisco 831 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 831 router.



Note

- You can have any kind of connectivity or network beyond the Cisco 831 WAN.
- 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

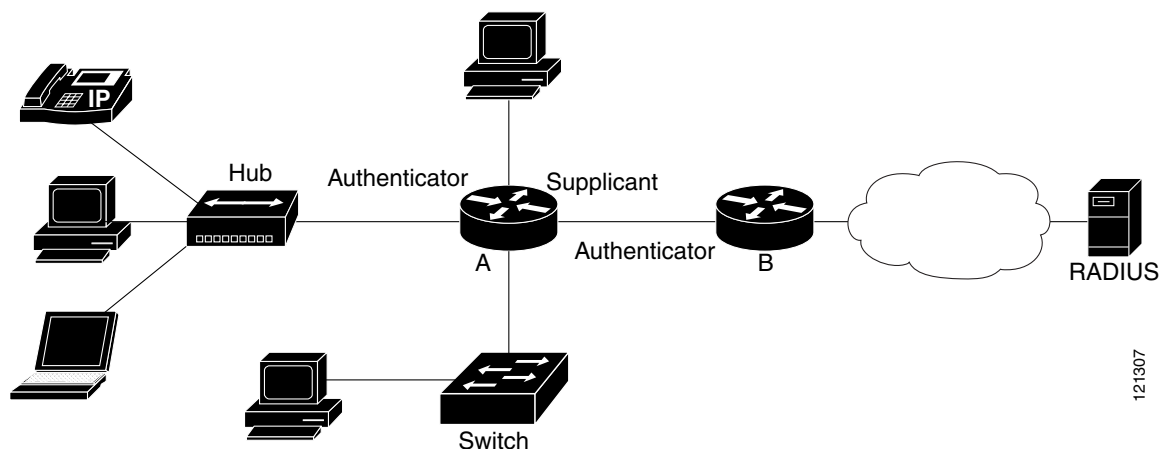
There are deployment scenarios in which a network device (a router acting as an 802.1X authenticator) is placed in an unsecured location and cannot be trusted as an authenticator. This scenario requires that a network device be able to authenticate itself against another network device. The 802.1X supplicant 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 2 Multiple Instances of Supplicant Support



121307

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.

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

This section includes the following procedures:

- [Configuring an AAA RADIUS Server, page 5](#)
- [Configuring a Router, page 5](#)
- [Configuring a PC, page 19](#)
- [Monitoring VPN Access Control Using 802.1X Authentication, page 21](#)
- [Verifying VPN Access Control Using 802.1X Authentication, page 23](#)

Configuring an AAA RADIUS Server

To configure an AAA RADIUS server, perform the following 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

This section contains the following procedures:

- [Enabling 802.1X Authentication, page 6](#) (required)
- [Configuring Router and RADIUS Communication, page 7](#) (required)
- [Configuring 802.1X Parameters \(Retransmissions and Timeouts\), page 8](#) (optional)
- [Configuring the Identity Profile, page 11](#) (required)
- [Configuring the Virtual Template and DHCP, page 12](#) (required)
- [Configuring the Necessary Access Control Policies, page 17](#) (optional)
- [Configuring a Router As a Supplicant, page 17](#) (optional)

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 group radius**
5. **dot1x system-auth-control**
6. **identity profile default**
7. **interface type slot/port**
8. **dot1x port-control auto**

DETAILED STEPS

	Command	Description
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • 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 group radius Example: Router (config)# aaa authentication dot1x default group radius	Creates an 802.1X port-based authentication method list.
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.

	Command	Description
Step 7	interface <i>type slot/port</i> Example: Router (config)# interface fastethernet 5/1	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.

Example

This section provides the following examples:

- [802.1X Configuration](#)
- [Verifying 802.1X Authentication](#)

802.1X Configuration

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
Router(config)# dot1x system-auth-control
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x port-control auto
```

Verifying 802.1X Authentication

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

```
Router# show dot1x all

PortControl          = AUTO
ReAuthentication     = Disabled
ReAuthPeriod         = 3600 Seconds
ServerTimeout        = 30 Seconds
SuppTimeout          = 30 Seconds
QuietWhile           = 120 Seconds
MaxReq                = 2
```

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	Description
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip radius source-interface <i>interface-name</i> Example: Router (config)# ip radius source-interface ethernet1	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.
Step 4	radius-server host (<i>hostname</i> <i>ip-address</i>) Example: Router (config)# radius-server host 172.16.39.46	Configures the RADIUS server host name or IP address of the router. <ul style="list-style-type: none"> To use multiple RADIUS servers, reenter this command for each server.
Step 5	radius-server key <i>string</i> 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. <ul style="list-style-type: none"> 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 172.16.39.46
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 configuring the retransmission and timeout parameters, perform the following steps.

SUMMARY STEPS

- enable**
- configure terminal**
- interface** *type slot/port*
- 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	Description
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type slot/port</i> Example: Router (config)# interface ethernet 0/1	Enters interface configuration mode and specifies the interface to be enabled for 802.1X port-based authentication.
Step 4	dot1x max-req <i>number-of-retries</i> 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. <ul style="list-style-type: none"> 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.

	Command	Description
Step 7	dot1x reauthentication Example: Router (config-if)# dot1x reauthentication	Enables periodic reauthentication of the supplicants on the interface. <ul style="list-style-type: none"> The reauthentication period can be set using the dot1x timeout command.
Step 8	dot1x timeout tx-period seconds Example: Router (config-if)# dot1x timeout tx-period 60	Sets the timeout for supplicant retries. <ul style="list-style-type: none"> 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 <i>seconds</i> 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. <ul style="list-style-type: none"> 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 <i>seconds</i> 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. <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> The value is from 1 to 65535 seconds.

Example

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

```
Router# configure terminal
Router(config)# interface ethernet 0
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 text** *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	Description
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
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 <i>line-of-description</i> Example: Router (config-identity-prof)# description description 1	Associates descriptive text with the profile.
Step 5	template <i>virtual-template</i> 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.

	Command	Description
Step 6	device [authorize not-authorize] mac-address <i>mac-address</i>	Statically authorizes or unauthorizes a supplicant (by giving its MAC address) if the supplicant does not “understand” 802.1X.
	Example: Router (config-identity-prof)# device authorize mac-address mac-address H.H.H	
Step 7	device authorize type <i>device-type</i>	Statically authorizes or unauthorizes a device type.
	Example: Router (config-identity-prof)# device authorize type cisco ip phone	

Example

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-lx-prof)# description put the description here
Router(config-lx-prof)# template virtual-templatel
Router(config-lx-prof)# device authorize type cisco ip phone
Router(config-lx-prof)# device authorize mac-address 0001.024B.B4E7
```

Configuring the Virtual Template and DHCP

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. To configure your router for a private pool and for a public pool, perform the following steps.

SUMMARY STEPS

Configuring the Identity Profile

1. **enable**
2. **configure terminal**
3. **identity profile default**
4. **description** *description-string*
5. **template** *virtual-template*
6. **exit**

Configuring the DHCP Private Pool

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

Configuring the DHCP Public Pool

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

Configuring the Interface

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**

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

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

DETAILED STEPS**Configuring the Identity Profile**

	Command	Description
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
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 <i>description-string</i> Example: Router (config-identity-prof)# description description_string_goes_here	Associates descriptive text with the identity profile.

	Command	Description
Step 5	<code>template virtual-template</code> Example: Router (config-identity-prof)# template virtualtemplatel	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	<code>exit</code> Example: Router (config-identity-prof)# exit	Exits identity profile configuration mode.

Configuring the DHCP Private Pool

	Command	Description
Step 1	<code>ip dhcp pool name</code> 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	<code>network network-number [mask]</code> Example: Router (config-dhcp)# network 10.0.0.1 255.0.0.0	Configures the subnet number and mask for a DHCP private address pool on a Cisco IOS DHCP server.
Step 3	<code>default-router address</code> Example: Router (config-dhcp)# default-router 10.2.2.2	Specifies the default router list for a DHCP client.

Configuring the DHCP Public Pool

	Command	Description
Step 1	<code>ip dhcp pool name</code> Example: Router (config-dhcp)# ip dhcp pool public	Configures the DHCP public address pool on a Cisco IOS DHCP server.
Step 2	<code>network network-number [mask]</code> Example: Router (config-dhcp)# network 10.4.4.4.255.0.0.0	Configures the subnet number and mask for a DHCP public address pool on a Cisco IOS DHCP server.

	Command	Description
Step 3	default-router <i>address</i>	Specifies the default router list for a DHCP client.
	Example: Router (config-dhcp)# default-router 10.12.12.12	
Step 4	exit	Exits DHCP pool configuration mode.
	Example: Router (config-dhcp)# exit	

Configuring the Interface

	Command	Description
Step 1	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	
Step 2	interface <i>type slot/port</i>	Enters interface configuration mode and specifies the interface to be enabled.
	Example: Router (config)# interface loopback 0/1	
Step 3	ip address <i>ip-address mask</i> [secondary]	Sets the private IP address for the interface.
	Example: Router (config-if)# ip address 10.5.5.5 255.255.255.0	
Step 4	interface virtual-template <i>number</i>	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
	Router (config-if)# interface virtual-template 1	
Step 5	ip address <i>ip-address mask</i> [secondary]	Sets the public IP address for the interface.
	Example: Router (config-if)# ip address 10.6.6.6 255.255.255.0	
Step 6	exit	Exits interface configuration mode.
	Example: Router (config-if)# exit	

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

	Command	Description
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type slot/port</i> Example: Router (config)# interface virtual-template 1/2	Enters interface configuration mode and specifies the interface to be enabled.
Step 4	ip unnumbered <i>type number</i> 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-lx-prof)# description put the description here
Router(config-lx-prof)# template virtual-template1
Router(config-lx-prof)# exit
```

```
Router(config)# ip dhcp pool private
Router(config-dhcp)# network 10.0.0.1 255.0.0.0
Router(config-dhcp)# default-router 10.2.2.2
Router(config-dhcp)# exit
```

```
Router(config)# ip dhcp pool public
Router(config-dhcp)# network 10.4.4.4 255.0.0.0
Router(config-dhcp)# default-router 10.12.12.12
Router(config-dhcp)# exit
```

```
Router(config)# interface loopback0
Router(config-if)# ip address 10.5.5.5 255.255.255.0
Router(config-if)# interface ethernet0
Router(config-if)# ip address 10.6.6.6 255.255.255.0
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 via the physical interface, and unauthenticated traffic transits via 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 via 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 Router As a Supplicant

To configure a router to act as a supplicant, you have to first configure the identity profile that the supplicant will use to obtain its EAP credentials. Then you have to configure the interface as a supplicant Port Access Entity (PAE) type. To configure a router as a supplicant, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot1x credentials** *name*
4. **username** *name*
5. **password** [0 | 7] *password*
6. **description** *text*
7. **exit**
8. **interface** *type number*
9. **dot1x pae supplicant**
10. **exit**
11. **exit**

DETAILED STEPS

	Command	Description
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	dot1x credentials name Example: Router (config)# dot1x credentials basic-user	Specifies which 802.1X credential profile to use when configuring a supplicant and enters dot1x credentials configuration mode.
Step 4	username name Example: Router (config-dot1x-creden)# username router1	Specifies the username for an 802.1X credentials profile.
Step 5	password [0 7] password Example: Router (config-dot1x-creden)# password secret	Specifies the password for an 802.1X credentials profile.
Step 6	description text Example: Router (config-dot1x-creden)# description This credentials profile should be used for most configured ports	Specifies a description for an 802.1X profile.
Step 7	exit Example: Router (config-dot1x-creden)# exit	Exits dot1x credentials configuration mode.
Step 8	interface type number Example: Router# interface Ethernet1	Configures an interface type and enters interface configuration mode.
Step 9	dot1x pae supplicant Example: Router (config-if)# dot1x pae supplicant	Sets the PAE type. <ul style="list-style-type: none"> The supplicant keyword specifies that the interface will be acting only as a supplicant and will not respond to messages that are meant for an authenticator.

	Command	Description
Step 10	<code>exit</code>	Exits interface configuration mode.
	Example: Router (config-if)# <code>exit</code>	
Step 11	<code>exit</code>	Exits global configuration mode.
	Example: Router (config-dot1x-creden)# <code>exit</code>	

Configuring a PC

This section includes the following procedures.

- [Configuring a PC for VPN Access Control Using 802.1X Authentication, page 19](#)
- [Enabling 802.1X Authentication on a Windows 2000/XP PC, page 19](#)
- [Enabling 802.1X Authentication on a Windows 2000 PC, page 19](#)
- [Enabling 802.1X Authentication on a Windows XP PC, page 20](#)
- [Enabling 802.1X Authentication on Windows 2000 and Windows XP PCs, page 20](#)

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.

-
- 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.

-
- 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_DWORD 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.

- 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.
-

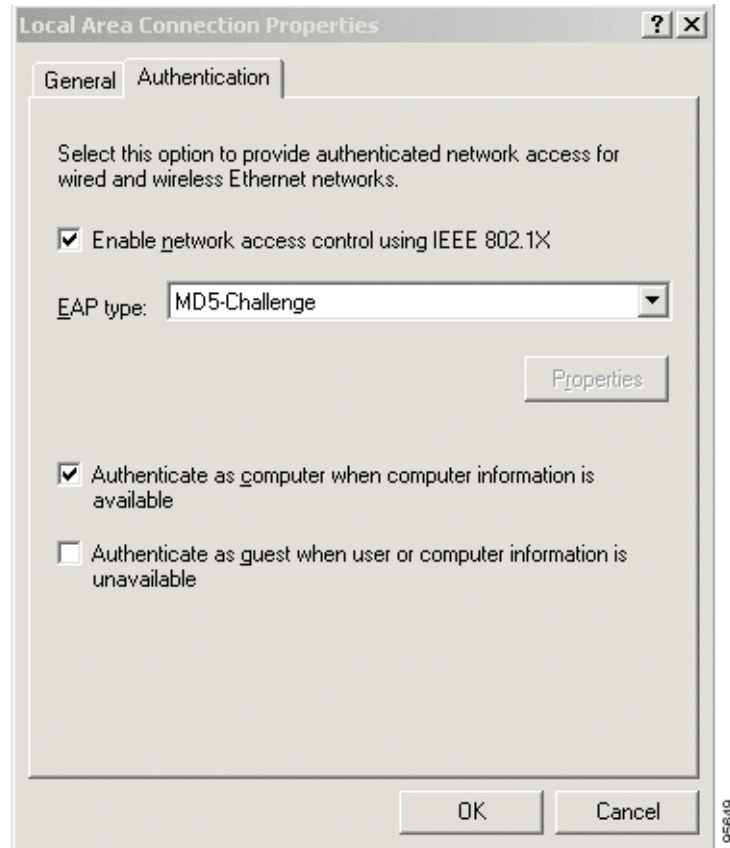
Enabling 802.1X Authentication on Windows 2000 and Windows XP PCs

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.

- 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 [Figure 3](#).

Figure 3 Local Area Connection Properties Window


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**
3. **clear eap** [sessions [credentials *credentials-name* | interface *interface-name* | method *method-name* | transport *transport-name*]]
4. **debug dot1x** [aaa | all | process | rxdata | state-machine | txdata | vlan]
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	<pre>enable</pre> <p>Example: Router> enable </p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<pre>clear dot1x</pre> <p>Example: Router# clear dot1x </p>	Clears 802.1X interface information.
Step 3	<pre>clear eap [sessions [credentials credentials-name interface interface-name method method-name transport transport-name]]</pre> <p>Example: Router# clear eap sessions credentials type1 </p>	Clears EAP information on a switch or for a specified port.
Step 4	<pre>debug dot1x [aaa all process rxdata state-machine txdata vlan]</pre> <p>Example: Router# debug dot1x all </p>	Displays 802.1X debugging information. <ul style="list-style-type: none"> aaa—Information is provided for AAA communications. all—All 802.1X debugging messages are turned on. process—Information is provided regarding the 802.1X process. rxdata—Information is provided for packets that have been received from clients. state-machine—Information is provided regarding the 802.1X state-machine. txdata—Information is provided regarding packets that have been transmitted to clients. vlan—Information is provided regarding the MAC address-based VLAN operation. <p> Note VLAN interfaces are currently not supported.</p>
Step 5	<pre>debug eap [all method] [authenticator peer] {all errors events packets sm}</pre> <p>Example: Router# debug eap all </p>	Displays information about EAP.

	Command or Action	Purpose
Step 6	dot1x initialize [interface <i>interface-name</i>] Router# dot1x initialize interface ethernet 0	Initializes an interface.
Step 7	dot1x re-authenticate <i>interface-type</i> <i>interface-number</i> Example: Router# dot1x re-authenticate ethernet 0	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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show dot1x [interface <i>interface-name</i> [details]] Example: Router# show dot1x interface ethernet 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 <i>credentials-name</i> interface <i>interface-name</i> method <i>method-name</i> transport <i>transport-name</i>] Example: Router# show eap sessions interface gigabitethernet1/0/1	Displays active EAP session information.

Configuration Examples for VPN Access Control Using 802.1X Authentication

This section includes the following example:

- [Typical VPN Access Control Using 802.1X Configuration: Example, page 24](#)
- [Access Control Policies: Example, page 27](#)
- [Router Acting As a Supplicant: Example, page 29](#)

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: 2100 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname c831-tb
!
memory-size iomem 15
!
aaa new-model
!
!
aaa authentication dot1x default group radius
aaa session-id common
ip subnet-zero
!
ip dhcp pool private
    network 10.0.0.0 255.255.255.0
    default-router 10.0.0.1
    lease 0 0 2
!
ip dhcp pool public
    network 10.3.0.0 255.255.255.0
    default-router 10.3.0.1
!
!
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
!
crypto isakmp policy 1
    authentication pre-share
crypto isakmp key 0 test address 150.0.0.2
!
```

```
!
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 150.0.0.2
  set transform-set t1
  match address 101
!
dot1x system-auth-control
identity profile default
  template Virtual-Template1
!
!
interface Loopback0
  ip address 10.3.0.1 255.255.255.0
!
interface Ethernet0
  ip address 10.0.0.1 255.255.255.0
  dot1x port-control auto
  dot1x reauthentication
  dot1x timeout reauth-period 36000
!
interface Ethernet1
  no ip address
  duplex auto
  pppoe enable
  pppoe-client dial-pool-number 1
!
interface Virtual-Template1
  ip unnumbered Loopback0
  ip access-group 102 in
  ip access-group 102 out
!
interface Dialer0
  ip address 172.0.0.1 255.255.255.0
  ip mtu 1492
  encapsulation ppp
  dialer pool 1
  crypto map test
!
interface Dialer1
  no ip address
!
router rip
  network 10.0.0.0
  network 10.3.0.0
  network 172.0.0.0
!
ip classless
ip http server
no ip http secure-server
!
!
ip access-list extended list1
access-list 101 permit ip 10.0.0.0 0.0.0.255 10.5.0.0 0.0.0.255
access-list 102 deny ip 10.3.0.0 0.0.0.255 10.5.0.0 0.0.0.255
access-list 102 deny ip 10.2.0.0 0.0.0.255 10.5.0.0 0.0.0.255
access-list 102 permit ip any any
radius-server host 192.168.140.50 auth-port 1812 acct-port 1646 key radiuskey
!
line con 0
  exec-timeout 0 0
```

```

no modem enable
line aux 0
line vty 0 4
!
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 172.0.0.1
!
!
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 172.0.0.1
 set transform-set t1
 match address 101
!
no voice hpi capture buffer
no voice hpi capture destination
!
interface Loopback0
 description corporate
 ip address 10.5.5.5 255.255.255.0
!
interface Loopback1
 description internet
 ip address 10.6.6.6 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.140.100 255.255.255.0
 duplex auto

```

```
    speed auto
    !
interface FastEthernet0/1
  no ip address
  speed auto
  half-duplex
  pppoe enable
  !
interface ATM1/0
  ip address 10.0.0.10 255.255.255.0
  no atm ilmi-keepalive
  pvc 1/43
    protocol ip 10.75.0.4 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 10.150.0.2 255.255.255.0
  ip mtu 1492
  crypto map test
  !
  !
router rip
  network 10.5.0.0
  network 10.6.0.0
  network 10.75.0.0
  network 172.0.0.0
  network 192.168.140.0
  !
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 10.0.0.0 255.255.255.0
 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 10.0.0.0 255.255.255.0
 default-router 20.0.0.1
 exit
!
ip dhcp pool public
 network 10.0.0.1 255.255.255.0
 default-router 10.0.0.2
 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 10.0.0.3 255.255.255.0
!

```

```

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

```

Router Acting As a Supplicant: Example

The following example shows that dot1x module debugging has been turned on. The **show debugging** command output shows that 802.1X interface information has been cleared for all interfaces.

```
Router# debug dot1x supplicant
```

```
dot1x supplicant module debugging is on
```

```
Router# show debugging
```

```

dot1x:
  dot1x supplicant module debugging is on

3w6d: supp_pae_state_transition: Supplicant State Transition: DISCONNECTED -> CONNECTING
3w6d: supp_pae_txStart: << txStart >>: EAPOL-Start to Authenticator
3w6d: dot1x_pakio_send_pak: Zero destination address, sending to multicast
3w6d: dot1x_pakio_send_pak: Sending packet to group PAE address 0180.c200.0003
3w6d: dot1x_pakio_send_pak: Sending packet to address 0180.c200.0003
3w6d: dot1x_start_supp_timer: Started the Timer for client 0000.0000.0000, 30 seconds
3w6d: dot1x_reset_client: sm->state == CONNECTING
3w6d: clear_dot1x_client_supp_table: Clearing all dot1x supplicant instances
3w6d: supp_pae_state_transition: Supplicant State Transition: AUTHENTICATED -> LOGOFF
3w6d: supp_pae_txLogoff: << Router#txLogoff >>: EAPOL-Logoff to Authenticator
3w6d: dot1x_pakio_send_pak: Sending packet to address 000f.23c4.a401
3w6d: dot1x_client_logoff: sm->state == LOGOFF
3w6d: clear_dot1x_client_supp_bucket: Logoff Sent !!
3w6d: dot1x_reset_client: Stopping timers before re-initialization
3w6d: dot1x_reset_client: Re-initializing the default supplicant
3w6d: supp_pae_state_transition: Supplicant State Transition: CONNECTING -> DISCONNECTED
3w6d: supp_pae_state_transition: Supplicant State Transition: DISCONNECTED -> CONNECTING
3w6d: supp_pae_txStart: << txStart >>: EAPOL-Start to Authenticator
3w6d: dot1x_pakio_send_pak: Zero destination address, sending to multicast
3w6d: dot1x_pakio_send_pak: Sending packet to group PAE address 0180.c200.0003
3w6d: dot1x_pakio_send_pak: Sending packet to address 0180.c200.0003
3w6d: dot1x_start_supp_timer: Started the Timer for client 0000.0000.0000, 30 seconds
3w6d: dot1x_reset_client: sm->state == CONNECTING
3w6d: dot1x_get_def_client_supp_entry: Using the default supplicant instance
3w6d: dot1x_input: Stopping timers on the default supp instance
3w6d: dot1x_stop_supp_timer: Stopped the Timer for client 0000.0000.0000
3w6d: dot1x_get_client_supp_entry: Supplicant 000f.23c4.a401 not found in the supplicant
list
3w6d: dot1x_input: Creating a new supplicant entry
3w6d: dot1x_get_supp_config: Using the default EAP method
3w6d: dot1x_pakio_uplink_addr_set: Uplink address set to 00:0F:23:C4:A4:01
3w6d: dot1x_pakio_init_ios: Initialising common IOS structures for dot1x
3w6d: dot1x_pakio_init_ios: Done.
3w6d: dot1x_eap_init: Initialising EAP method 4
3w6d: dot1x_eap_init: Username:user, password:cisco
3w6d: dot1x_eap_init: sm->state == DISCONNECTED

```

```

3w6d: supp_pae_state_transition: Supplicant State Transition: INVALID -> DISCONNECTED
3w6d: supp_pae_state_transition: Supplicant State Transition: DISCONNECTED -> CONNECTING
3w6d: supp_pae_txStart: << txStart >>: EAPOL-Start to Authenticator
3w6d: dot1x_pakio_send_pak: Sending packet to address 000f.23c4.a401
3w6d: dot1x_start_supp_timer: Started the Timer for client 000f.23c4.a401, 30 seconds
3w6d: dot1x_eap_init: sm->state == CONNECTING
3w6d: add_dot1x_client_supp_to_table:
3w6d: dot1x_get_def_client_supp_entry: Using the default supplicant instance000f.23c4.a401
is added to the supplicant list
3w6d: dot1x_input: QUEUE_EVENT (active pkt count tx 0, rx 1, total tx 3, total rx 10)
3w6d: dot1x_input: Stopping timers on the default supp instance
3w6d: dot1x_get_client_supp_entry: Supplicant instance found
3w6d: dot1x_input: Found an existing supplicant entry
3w6d: supp_pae_event_handler: Received packet:
3w6d: supp_pae_state_transition: Supplicant State Transition: CONNECTING -> ACQUIRED
3w6d: dot1x_stop_supp_timer: Stopped the Timer for client 000f.23c4.a401
3w6d: supp_pae_txRspId: << txRspId >>: EAPOL-EAP-Response-Id to Authenticator
3w6d: supp_pae_txRspId: ReceivedId is 0x1 and currentId is 0x100
3w6d: dot1x_pakio_send_pak: Sending packet to address 000f.23c4.a401
3w6d: dot1x_start_supp_timer: Started the Timer for client 000f.23c4.a401, 30 seconds
3w6d: dot1x_input: QUEUE_EVENT (active pkt count tx 0, rx 1, total tx 2, total rx 2)
3w6d: supp_pae_event_handler: Received packet:
3w6d: supp_pae_state_transition: Supplicant State Transition: ACQUIRED -> ACQUIRED
3w6d: dot1x_stop_supp_timer: Stopped the Timer for client 000f.23c4.a401
3w6d: supp_pae_txRspId: << txRspId >>: EAPOL-EAP-Response-Id to Authenticator
3w6d: supp_pae_txRspId: ReceivedId is 0x1 and currentId is 0x1
3w6d: dot1x_pakio_send_pak: Sending packet to address 000f.23c4.a401
3w6d: dot1x_start_supp_timer: Started the Timer for client 000f.23c4.a401, 30 seconds
3w6d: dot1x_input: QUEUE_EVENT (active pkt count tx 0, rx 0, total tx 3, total rx 2)
3w6d: dot1x_get_def_client_supp_entry: Using the default supplicant instance
3w6d: dot1x_input: Stopping timers on the default supp instance
3w6d: dot1x_get_client_supp_entry: Supplicant instance found
3w6d: dot1x_input: Found an existing supplicant entry
3w6d: supp_pae_event_handler: Received packet:
3w6d: supp_pae_state_transition: Supplicant State Transition: ACQUIRED -> AUTHENTICATING
3w6d: dot1x_stop_supp_timer: Stopped the Timer for client 000f.23c4.a401
3w6d: supp_pae_txRspAuth: << txRspAuth >>: EAPOL-EAP-Response to Authenticator
3w6d: dot1x_pakio_send_pak: Sending packet to address 000f.23c4.a401
3w6d: dot1x_start_supp_timer: Started the Timer for client 000f.23c4.a401, 30 seconds
3w6d: dot1x_input: QUEUE_EVENT (active pkt count tx 0, rx 0, total tx 4, total rx 3)
3w6d: dot1x_get_def_client_supp_entry: Using the default supplicant instance
3w6d: dot1x_input: Stopping timers on the default supp instance
3w6d: dot1x_get_client_supp_entry: Supplicant instance found
3w6d: dot1x_input: Found an existing supplicant entry
3w6d: supp_pae_event_handler: Received packet:
3w6d: supp_pae_state_transition: Supplicant State Transition: AUTHENTICATING ->
AUTHENTICATED
3w6d: supp_pae_state_transition: Changing IP addr in AUTHENTICATED state
3w6d: supp_pae_state_transition: Stopped client timers
3w6d: dot1x_stop_supp_timer: Stopped the Timer for client 000f.23c4.a401
3w6d: dot1x_input: QUEUE_EVENT (active pkt count tx 0, rx 0, total tx 4, total rx 4)

```

Additional References

The following sections provide references related to VPN Access Control Using 802.1X Authentication.

Related Documents

Related Topic	Document Title
AAA	“ Authentication, Authorization, and Accounting (AAA) ” section of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.3
Configuring 802.1X port-based authentication	“ Configuring IEEE 802.1x Port-Based Authentication ” chapter of the <i>Catalyst 3750 Switch Software Configuration Guide</i> , Release 12.2(25)SEC
DHCP	“ Configuring DHCP ” chapter of the <i>Cisco IOS IP Configuration Guide</i> , Release 12.3
IPSec	“ Security and Encryption ” section of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.3
Passwords and MD5	Improving Security on Cisco Routers
RADIUS	“ Security Server Protocols ” section of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.3
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

Standards	Title
IEEE 802.1X protocol	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	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

RFCs	Title
RFC-2284	“RFC 2284 (PPP Extensible Authentication Protocol [EAP])” document from <i>The Internet Requests for Comments (RFC)</i> document series

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new and modified commands only.

New Commands

- [aaa authentication dot1x](#)
- [clear dot1x](#)
- [clear eap](#)
- [debug dot1x](#)
- [debug eap](#)
- [description \(dot1x credentials\)](#)
- [description \(identity profile\)](#)
- [device \(identity profile\)](#)
- [dot1x control-direction](#)
- [dot1x credentials](#)
- [dot1x default](#)
- [dot1x guest-vlan](#)
- [dot1x host-mode](#)
- [dot1x initialize](#)
- [dot1x max-reauth-req](#)
- [dot1x max-req](#)
- [dot1x max-start](#)
- [dot1x multiple-hosts](#)
- [dot1x pae](#)
- [dot1x port-control](#)
- [dot1x re-authenticate \(privileged EXEC\)](#)
- [dot1x reauthentication](#)
- [dot1x system-auth-control](#)
- [dot1x timeout](#)
- [eap](#)

- **identity profile**
- **macro global**
- **macro name**
- **password (dot1x credentials)**
- **show dot1x**
- **show eap registrations**
- **show eap sessions**
- **show ip igmp snooping**
- **template (identity profile)**
- **username (dot1x credentials)**

aaa authentication dot1x

To specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X, use the **aaa authentication dot1x** command in global configuration mode. To disable authentication, use the **no** form of this command

```
aaa authentication dot1x {default | listname} method1 [method2...]
```

```
no aaa authentication dot1x {default | listname} method1 [method2...]
```

Syntax Description

default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
listname	Character string used to name the list of authentication methods tried when a user logs in.
<i>method1 [method2...]</i>	At least one of these keywords: <ul style="list-style-type: none"> • enable—Uses the enable password for authentication. • group radius—Uses the list of all RADIUS servers for authentication. • line—Uses the line password for authentication. • local—Uses the local username database for authentication. • local-case—Uses the case-sensitive local username database for authentication. • none—Uses no authentication. The client is automatically authenticated by the switch without using the information supplied by the client.

Defaults

No authentication is performed.

Command Types

Global configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced for the Cisco Ethernet switch network module.
12.2(15)ZJ	This command was implemented on the following platforms for the Cisco Ethernet Switch Module: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.
12.3(2)XA	This command was introduced on the following Cisco router platforms: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. Router support was added for the following platforms: Cisco 1751, Cisco 2610XM – Cisco 2611XM, Cisco 2620XM – Cisco 2621XM, Cisco 2650XM – Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.

Usage Guidelines

The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence to validate the password provided by the client. The only method that is truly 802.1X-compliant is the **group radius** method, in which the client data is validated against a RADIUS authentication server. The remaining methods enable AAA to authenticate the client by using locally configured data. For example, the **local** and **local-case** methods use the username and password that are saved in the Cisco IOS configuration file. The **enable** and **line** methods use the **enable** and **line** passwords for authentication.

If you specify **group radius**, you must configure the RADIUS server by entering the **radius-server host** global configuration command. If you are not using a RADIUS server, you can use the **local** or **local-case** methods, which access the local username database to perform authentication. By specifying the **enable** or **line** methods, you can supply the clients with a password to provide access to the switch.

Use the **show running-config** privileged EXEC command to display the configured lists of authentication methods.

Examples

The following example shows how to enable AAA and how to create an authentication list for 802.1X. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is allowed access with no authentication:

```
Router(config)# aaa new model
Router(config)# aaa authentication dot1x default group radius none
```

Related Commands

Command	Description
debug dot1x	Displays 802.1X debugging information.
identity profile default	Creates an identity profile and enters dot1x profile configuration mode.
show dot1x	Displays details for an identity profile.
show dot1x (EtherSwitch)	Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

clear dot1x

To clear 802.1X interface information, use the **clear dot1x** command in privileged EXEC mode.

```
clear dot1x {all | interface interface-name}
```

Syntax Description	all	Clears 802.1X information for all interfaces.
	interface <i>interface-name</i>	Clears 802.1X information for the specified interface.

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.3(2)XA	This command was introduced.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
	12.2(25)SEE	This command was integrated into Cisco IOS Release 12.2(25)SEE.

Examples

The following configuration shows that 802.1X information will be cleared for all interfaces:

```
Router# clear dot1x all
```

The following configuration shows that 802.1X information will be cleared for the Ethernet 0 interface:

```
Router# clear dot1x interface ethernet 0
```

You can verify that the information was deleted by entering the **show dot1x** command.

Related Commands	Command	Description
	debug dot1x	Displays 802.1X debugging information.
	identity profile default	Creates an identity profile and enters identity profile configuration mode.
	show dot1x	Displays details for an identity profile.

clear eap

To clear Extensible Authentication Protocol (EAP) information on a switch or for a specified port, use the **clear eap** command in privileged EXEC mode.

```
clear eap [sessions [credentials credentials-name | interface interface-name | method
method-name | transport transport-name]]
```

Syntax Description		
sessions	(Optional)	Clears EAP sessions on a switch or a specified port.
credentials <i>credentials-name</i>	(Optional)	Clears EAP credential information for only the specified profile.
interface <i>interface-name</i>	(Optional)	Clears EAP credential information for only the specified interface.
method <i>method-name</i>	(Optional)	Clears EAP credential information for only the specified method.
transport <i>transport-name</i>	(Optional)	Clears EAP credential information for only the specified lower layer.

Command Default All active EAP sessions are cleared.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(25)SEE	This command was introduced.
	12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines You can clear all counters by using the **clear eap** command with the **sessions** keyword, or you can clear only the specified information by using the **credentials**, **interface**, **method**, or **transport** keywords.

Examples The following example shows how to clear all EAP information:

```
Router# clear eap sessions
```

The following example shows how to clear EAP session information for the specified profile:

```
Router# clear eap sessions credentials type1
```

Related Commands	Command	Description
	show eap registrations	Displays EAP registration information.
	show eap sessions	Displays active EAP session information.

debug dot1x

To display 802.1X debugging information, use the **debug dot1x** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug dot1x [**all** | **errors** | **events** | **feature** | **packets** | **redundancy** | **registry** | **state-machine**]

no debug dot1x [**all** | **errors** | **events** | **feature** | **packets** | **redundancy** | **registry** | **state-machine**]

Syntax Description

all	(Optional) Enables all 802.1X debugging messages.
errors	(Optional) Provides information about all 802.1X errors.
events	(Optional) Provides information about all 802.1X events.
feature	(Optional) Provides information about 802.1X features for switches only.
packets	(Optional) Provides information about all 802.1X packets.
redundancy	(Optional) Provides information about 802.1X redundancy.
registry	(Optional) Provides information about 802.1X registries.
state-machine	(Optional) Provides information regarding the 802.1X state machine.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was introduced.
12.1(14)EA1	The authsm , backend , besm , core , and reauthsm keywords were removed. The errors , events , packets , registry , and state-machine keywords were added.
12.3(2)XA	This command was integrated into Cisco IOS Release 12.3(2)XA.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(11)T	The supplicant keyword was added.
12.2(25)SEE	The feature keyword was added for switches only.
12.4(6)T	The redundancy keyword was added. The aaa , process , rxdata , supplicant , txdata , and vlan keywords were deleted.

Examples

The following is sample output for the **debug dot1x** command:

```
Router# debug dot1x

Router-871#debug dot1x all
*Nov  7 13:07:56.872: dot1x-ev:dot1x_mgr_pre_process_eapol_pak: Role determination not
required on FastEthernet1.
*Nov  7 13:07:56.876: dot1x-packet:dot1x_mgr_process_eapol_pak: queuing an EAPOL pkt on
Authenticator Q
*Nov  7 13:07:56.876: dot1x-ev:Enqueued the eapol packet to the global authenticator queue
*Nov  7 13:07:56.876: dot1x-packet:Received an EAPOL frame on interface FastEthernet1
*Nov  7 13:07:56.876: dot1x-ev:Received pkt saddr =000f.23c4.a401 , daddr =
0180.c200.0003,
```

```
                pae-ether-type = 888e.0202.0000
*Nov  7 13:07:56.876: dot1x-packet:Received an EAPOL-Logoff packet on interface
FastEthernet1
*Nov  7 13:07:56.876: EAPOL pak dump rx
*Nov  7 13:07:56.876: EAPOL Version: 0x2  type: 0x2  length: 0x0000
*Nov  7 13:07:56.876: dot1x-sm:Posting EAPOL_LOGOFF on Client=82AC85CC
*Nov  7 13:07:56.876:      dot1x_auth Fa1: during state auth_authenticating, got event
7(eapolLogoff)
```

The fields in the output are self-explanatory.

Related Commands

Command	Description
clear dot1x	Clears 802.1X interface information.
identity profile default	Creates an identity profile and enters identity profile configuration mode.
show dot1x	Displays details for an identity profile.

debug eap

To display information about Extensible Authentication Protocol (EAP), use the **debug eap** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug eap [all | method] [authenticator | peer] {all | errors | events | packets | sm}
```

```
no debug eap [all | method] [authenticator | peer] {all | errors | events | packets | sm}
```

Syntax Description

all <i>method</i>	(Optional) Specifies the method to which the debug command refers. <ul style="list-style-type: none"> The all keyword turns on debugging for all EAP methods, including the EAP framework. The <i>method</i> argument turns on debugging for specific methods. This keyword or argument is dynamically linked into the parse chain and is present only if the method itself is present. If this keyword or argument is omitted, the debug command is applied to the EAP framework.
authenticator	(Optional) Limits the scope of the output to only authenticator contexts.
peer	(Optional) Limits the scope of the output to only peer contexts.
all	Debugging is turned on for all debug types.
errors	Displays information about EAP packet errors.
events	Displays information about EAP events.
packets	Turns on packet debugging for the specified method or methods.
sm	Turns on state machine debugging for the specified method or methods.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(6)T	The <i>method</i> argument and authenticator and peer keywords were added.

Examples

The following sample output from the **debug eap all** command shows all EAP information:

```
Router# debug eap all
```

```
*Nov 7 13:05:58.512: EAP-EVENT: Received get canned status from lower layer (0x00000000)
*Nov 7 13:05:59.460: EAP-EVENT: Received context create from lower layer (0x00000009)
*Nov 7 13:05:59.460: eap_authen : initial state eap_auth_initialize has enter
*Nov 7 13:05:59.460: EAP-EVENT: Started 'Authenticator Start' timer (1s) for EAP sesion
handle 0xD6000008
*Nov 7 13:05:59.460: EAP-EVENT: Allocated new EAP context (handle = 0xD6000008)
*Nov 7 13:05:59.464: EAP-EVENT: Started EAP tick timer
*Nov 7 13:06:00.488: EAP-EVENT: 'Authenticator Start' timer expired for EAP sesion handle
0xD6000008
```

```
*Nov 7 13:06:00.488: eap_authen : during state eap_auth_initialize, got event
21(eapStartTmo)
*Nov 7 13:06:00.488: @@@ eap_authen : eap_auth_initialize -> eap_auth_select_action
*Nov 7 13:06:00.488: eap_authen : during state eap_auth_select_action, got event
17(eapDecisionPropose)
*Nov 7 13:06:00.488: @@@ eap_authen : eap_auth_select_action -> eap_auth_propose_method
```

Related Commands

Command	Description
debug eou	Displays information about EAPoUDP.

description (dot1x credentials)

To specify a description for an 802.1X profile, use the **description** command in dot1x credentials configuration mode. To remove the description, use the **no** form of this command.

description *text*

no description

Syntax Description

<i>text</i>	Text description. The description can be up to 80 characters.
-------------	---

Command Default

A description is not specified.

Command Modes

Dot1x credentials configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Before using this command, the **dot1x credentials** command must have been configured.

An 802.1X credential structure is necessary when configuring a supplicant (client). This credentials structure may contain a username, password, and description.

Examples

The following example shows which credentials profile should be used when configuring a supplicant, and it provides a description of the credentials profile:

```
dot1x credentials basic-user
  username router
  password secret
  description This credentials profile should be used for most configured ports
```

The credentials structure can be applied to an interface, along with the **dot1x pae supplicant** command and keyword, to enable supplicant functionality on that interface.

```
interface fastethernet 0/1
  dot1x credentials basic-user
  dot1x pae supplicant
```

Related Commands

Command	Description
dot1x credentials	Specifies which 802.1X credentials profile to use.

description (identity profile)

To enter a description for an identity profile, use the **description** command in identity profile configuration mode. To remove the description of the identity profile, use the **no** form of this command.

description *line-of-description*

no description *line-of-description*

Syntax Description

<i>line-of-description</i>	Description of the identity profile.
----------------------------	--------------------------------------

Defaults

A description is not entered for the identity profile.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	This command was previously configured in dot1x configuration mode.

Usage Guidelines

The **identity profile** command and one of its keywords (**default**, **dot1x**, or **eapoudp**) must be entered in global configuration mode before the **description** command can be used.

Examples

The following example shows that a default identity profile and its description (“ourdefaultpolicy”) have been specified:

```
Router (config)# identity profile default
Router (config-identity-prof)# description ourdefaultpolicy
```

Related Commands

Command	Description
description (identity policy)	Enters a description for an identity policy.
identity profile	Creates an identity profile and enters identity profile configuration mode.

device (identity profile)

To statically authorize or reject individual devices, use the **device** command in identity profile configuration mode. To disable the authorization or rejection, use the **no** form of this command.

```
device {authorize {ip address ip-address {policy policy-name} | mac-address mac-address | type
{cisco | ip | phone}} | not-authorize}
```

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

Syntax Description

authorize	Configures an authorized device.
ip address	Specifies a device by its IP address.
<i>ip-address</i>	The IP address.
policy	Applies an associated policy with the device.
<i>policy-name</i>	Name of the policy.
mac-address	Specifies a device by its MAC address.
<i>mac-address</i>	The MAC address.
type	Specifies a device by its type.
cisco	Specifies a Cisco device.
ip	Specifies an IP device.
phone	Specifies a Cisco IP phone.
not-authorize	Configures an unauthorized device.

Defaults

A device is not statically authorized or rejected.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	The unauthorize keyword was changed to not authorize . The <i>cisco-device</i> argument was deleted. The ip address keyword and <i>ip-address</i> argument were added. The ip and phone keywords were added.

Usage Guidelines

The **identity profile** command and **default**, **dot1x**, or **eapoudp** keywords must be entered in global configuration mode before the **device** command can be used.

Examples

The following configuration example defines an identity profile for Extensible Authentication Protocol over UDP (EAPoUDP) to statically authorize host 192.168.1.3 with “greentree” as the associated identity policy:

```
Router(config)# identity profile eapoudp  
Router(config-identity-prof)# device authorize ip-address 192.168.1.3 policy greentree
```

Related Commands

Command	Description
identity profile eapoudp	Creates an identity profile.

dot1x control-direction

To change the port control to unidirectional or bidirectional, use the **dot1x control-direction** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

dot1x control-direction { both | in }

no dot1x control-direction

Syntax Description

both	Enables bidirectional control on the port.
in	Enables unidirectional control on the port.

Command Default

The port is set to bidirectional mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(25)SEC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.

Usage Guidelines

Using the **both** keyword or using the **no** form of this command changes the port to its bidirectional default setting.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows how to enable unidirectional control:

```
Router(config-if)# dot1x control-direction in
```

The following examples show how to enable bidirectional control:

```
Router (config-if)# dot1x control-direction both
```

or

```
Router (config-if)# no dot1x control-direction
```

You can verify your settings by entering the **show dot1x all** privileged EXEC command. The **show dot1x all** command output is the same for all devices except for the port names and the state of the port. If a host is attached to the port but is not yet authenticated, a display similar to the following appears:

```
Supplicant MAC 0002.b39a.9275
AuthSM State = CONNECTING
BendSM State = IDLE
PortStatus = UNAUTHORIZED
```

If you enter the **dot1x control-direction in** command to enable unidirectional control, the following appears in the **show dot1x all** command output:

```
ControlDirection = In
```

If you enter the **dot1x control-direction in** command and the port cannot support this mode because of a configuration conflict, the following appears in the **show dot1x all** command output:

```
ControlDirection = In (Disabled due to port settings):
```

The following example shows how to reset the global 802.1X parameters:

```
Router(config)# dot1x default
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)X

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
  description switchport connect to a client
  !
interface FastEthernet1
  description switchport connect to a client
  !
interface FastEthernet2
  description switchport connect to a client
  !
interface FastEthernet3
  description switchport connect to a client
  !
interface FastEthernet4
  description Connect to the public network
  !
interface Vlan1
  description Apply 802.1x functionality on SVI
  dot1x pae authenticator
  dot1x port-control auto
  dot1x reauthentication
```

Related Commands

Command	Description
show dot1x	Displays details for an identity profile.

dot1x credentials

To specify which 802.1X credential profile to use when configuring a supplicant (client) or to apply a credentials structure to an interface and to enter dot1x credentials configuration mode, use the **dot1x credentials** command in global configuration or interface configuration mode. To remove the credential profile, use the **no** form of this command.

dot1x credentials *name*

no dot1x credentials

Syntax Description	<i>name</i>	Name of the credentials profile.
---------------------------	-------------	----------------------------------

Command Default	A credentials profile is not specified.
------------------------	---

Command Modes	Global configuration Interface configuration
----------------------	---

Command History	Release	Modification
	12.4(6)T	This command was introduced.

Usage Guidelines	An 802.1X credential structure is necessary when configuring a supplicant. This credentials structure may contain a username, password, and description.
-------------------------	--

Examples The following example shows which credentials profile should be used when configuring a supplicant:

```
dot1x credentials basic-user
  username router
  password secret
  description This credentials profile should be used for most configured ports
```

The credentials structure can be applied to an interface, along with the **dot1x pae supplicant** command and keyword, to enable supplicant functionality on that interface.

```
interface fastethernet 0/1
  dot1x credentials basic-user
  dot1x pae supplicant
```

Related Commands	Command	Description
	anonymous-id (dot1x credential)	Specifies the anonymous identity that is associated with a credentials profile.
	description (dot1x credential)	Specifies the description for an 802.1X credentials profile.

Command	Description
password (dot1x credential)	Specifies the password for an 802.1X credentials profile.
username (dot1x credential)	Specifies the username for an 802.1X credentials profile.

dot1x default

To reset the global 802.1X parameters to their default values as specified in the latest IEEE 802.1X standard, use the **dot1x default** command in global configuration or interface configuration mode.

dot1x default

Syntax Description This command has no arguments or keywords.

Defaults This command has no default setting.

Command Modes Global configuration
Interface configuration

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.
	12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
	12.4(6)T	Interface configuration was added as a configuration mode for this command.
	12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.

Usage Guidelines Use the **show dot1x** command to verify your current 802.1X settings.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples The following example shows how to reset the global 802.1X parameters:

```
Router(config)# dot1x default
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
  description switchport connect to a client
  !
interface FastEthernet1
  description switchport connect to a client
  !
interface FastEthernet2
  description switchport connect to a client
  !
interface FastEthernet3
  description switchport connect to a client
  !
interface FastEthernet4
  description Connect to the public network
  !
interface Vlan1
  description Apply 802.1x functionality on SVI
  dot1x pae authenticator
  dot1x port-control auto
  dot1x reauthentication
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that the device sends an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
dot1x re-authentication (EtherSwitch)	Enables periodic reauthentication of the client for the Ethernet switch network module.
dot1x timeout (EtherSwitch)	Sets retry timeouts for the Ethernet switch network module.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dot1x guest-vlan

To specify an active virtual LAN (VLAN) as an 802.1X guest VLAN, use the **dot1x guest-vlan** command in interface configuration mode. To remove the VLAN that was specified, use the **no** form of this command.

dot1x guest-vlan *v-lan*

no dot1x guest-vlan

Syntax Description

<i>v-lan</i>	Specifies an active VLAN as an 802.1X guest VLAN. The range is 1 through 4094.
--------------	--

Command Default

A guest VLAN is not configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)EA1	This command was introduced.
12.2(25)SE	This command was modified to change the default guest VLAN behavior.
12.2(25)SEC	The usage guidelines were modified.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs).

Usage Guidelines

You can configure a guest VLAN on one of these ports:

- A static-access port that belongs to a nonprivate VLAN.
- A private-VLAN port that belongs to a secondary private VLAN. All the hosts that are connected to the port are assigned to private VLANs, regardless whether the posture validation was successful. The router or switch determines the primary private VLAN by using the primary- and secondary-private VLAN associations on the device.

For each 802.1X port on the router or switch, you can configure a guest VLAN to provide limited services to clients (a device or workstation connected to the router or switch) that is not currently running 802.1X. These users might be upgrading their systems for 802.1X authentication, and some hosts, such as Windows 98 systems, might not be 802.1X capable.

When you enable a guest VLAN on an 802.1X port, the router or switch assigns clients to a guest VLAN when it does not receive a response to its Extensible Authentication Protocol over LAN (EAPOL) request/identity frame or when EAPOL packets are not sent by the client.

Before Cisco IOS Release 12.2(25)SE, the router or switch did not maintain the EAPOL packet history and allowed clients that failed authentication access to the guest VLAN, regardless of whether EAPOL packets had been detected on the interface. In Cisco IOS Release 12.2(25)SE, you can use the **dot1x guest-vlan supplicant** command to enable this optional behavior. However, in Cisco IOS

Release 12.2(25)SEE, the **dot1x guest-vlan supplicant** command is no longer supported. You can use a restricted VLAN to allow clients that failed authentication access to the network by entering the **dot1x auth-fail vlan vlan-id** command.

With Cisco IOS Release 12.2(25)SE and later, the router or switch maintains the EAPOL packet history. If another EAPOL packet is detected on the interface during the lifetime of the link, the guest VLAN feature is disabled. If the port is already in the guest VLAN state, the port is returned to the unauthorized state, and authentication is restarted. The EAPOL history is reset upon loss of link.

Entering the **dot1x guest-vlan supplicant** command disables this behavior.

Any number of non-802.1X-capable clients are allowed access when the router or switch port is moved to the guest VLAN. If an 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.

Guest VLANs are supported on 802.1X ports in single-host or multiple-hosts mode.

You can configure any active VLAN except a Remote Switched Port Analyzer (RSPAN) VLAN, a primary private VLAN, or a voice VLAN as an 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 802.1X port to which a Dynamic Host Configuration Protocol (DHCP) client is connected, you might need to get a host IP address from a DHCP server. You can change the settings for restarting the 802.1X authentication process on the router or 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 802.1X authentication process (**dot1x timeout quiet-period** and **dot1x timeout tx-period** commands). The amount to decrease the settings depends on the connected 802.1X client type.

For Cisco IOS Release 12.4(4)XC only, this command is available at Layer 2 and Layer 3. However, the command functions at only one layer at a time, that is, if the command is configured at Layer 2, it is blocked at Layer 3 and vice versa.

You can verify your settings by entering the **show dot1x [interface interface-id]** command.

Examples

The following example shows how to specify VLAN 5 as an 802.1X guest VLAN:

```
Router (config-if)# dot1x guest-vlan 5
```

The following example shows how to set 3 as the quiet time on the switch, to set 15 as the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request, and to enable VLAN 2 as an 802.1X guest VLAN when an 802.1X port is connected to a DHCP client:

```
Router (config-if)# dot1x timeout quiet-period 3
Router (config-if)# dot1x timeout tx-period 15
Router (config-if)# dot1x guest-vlan 2
```

The following example shows how to enable the optional guest VLAN behavior and to specify VLAN 5 as an 802.1X guest VLAN:

```
Router (config)# dot1x guest-vlan supplicant
Router (config)# interface gigabitethernet 2/0/1
Router (config-if)# dot1x guest-vlan 5
```

The following output example shows this command has been configured on a Cisco 870 ISR:

```
interface FastEthernet0

  description switchport connect to a client
  !
```

■ dot1x guest-vlan

```

interface FastEthernet1
  description switchport connect to a client
  !
interface FastEthernet2
  description switchport connect to a client
  !
interface FastEthernet3
  description switchport connect to a client
  !
interface FastEthernet4
  description Connect to the public network
  !
interface Vlan1
  description Apply 802.1x functionality on SVI
  dot1x pae authenticator
  dot1x port-control auto
  dot1x reauthentication

```

Related Commands

Command	Description
dot1x	Enables the optional guest VLAN supplicant feature.
show dot1x	Displays 802.1X statistics, administrative status, and operational status for the switch or router or for the specified port.

dot1x host-mode

To allow hosts on an 802.1X-authorized port, use the **dot1x host-mode** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

```
dot1x host-mode {multi-auth | multi-host | single-host}
```

```
no dot1x host-mode {multi-auth | multi-host | single-host}
```

Syntax Description

multi-auth	All clients are authenticated individually on the port. The multi-auth mode is not supported on switch ports and is the default mode for router ports.
multi-host	Ensures that the first client and all subsequent clients are allowed access to the port if the first client is successfully authenticated.
single-host	Ensures that the first, and only the first, client is authenticated. All other clients are ignored and may cause a violation. The single-host mode is the default mode for switch ports.

Command Default

Hosts are not allowed on an 802.1X-authorized port.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)EA1	This command was introduced for switches. It replaced the dot1x multiple-hosts command.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.

Usage Guidelines

Before using this command, the **dot1x port-control** command must have been configured and set to **auto**.

The **multi-auth** mode authenticates each new client separately.

In **multi-host** mode, only one of the attached hosts has to be successfully authorized for all hosts to be granted network access (the **multi-host** mode authenticates one client, but after the client is authenticated, traffic is allowed from all other MAC addresses.). If the port becomes unauthorized (reauthentication fails or an Extensible Authentication Protocol over LAN [EAPOL] logoff message is received), all attached clients are denied access to the network.

The **single-host** mode allows only one client per port, that is, one MAC address to authenticate, and all others are blocked.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows how to enable IEEE 802.1X globally, to enable IEEE 802.1x on a port, and to enable multiple-hosts mode:

```
Router(config)# dot1x system-auth-control
Router (config)# interface gigabitethernet2/0/1
Router (config-if)# dot1x port-control auto
Router (config-if)# dot1x host-mode multi-host:
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
  description switchport connect to a client
  !
interface FastEthernet1
  description switchport connect to a client
  !
interface FastEthernet2
  description switchport connect to a client
  !
interface FastEthernet3
  description switchport connect to a client
  !
interface FastEthernet4
  description Connect to the public network
  !
interface Vlan1
  description Apply 802.1x functionality on SVI
  dot1x pae authenticator
  dot1x port-control auto
  dot1x reauthentication
```

Related Commands

Command	Description
show dot1x	Displays details for an identity profile.

dot1x initialize

To initialize 802.1X state machines on all 802.1X-enabled interfaces, use the **dot1x initialize** command in privileged EXEC mode. This command does not have a **no** form.

```
dot1x initialize [interface interface-name]
```

Syntax Description	interface <i>interface-name</i>	(Optional) Specifies an interface to be initialized. If this keyword is not entered, all interfaces are initialized.
---------------------------	---	--

Defaults State machines are not enabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)EA1	This commands was introduced.
	12.3(2)XA	This command was integrated into Cisco IOS Release 12.3(2)XA.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines Use this command to initialize the 802.1X state machines and to set up a fresh environment for authentication. After you enter this command, the port status becomes unauthorized.

Examples The following example shows how to manually initialize a port:

```
Router# dot1x initialize interface gigabitethernet2/0/2
```

You can verify the unauthorized port status by entering the **show dot1x [interface *interface-name*]** command.

Related Commands	Command	Description
	show dot1x	Displays details for an identity profile.

dot1x max-reauth-req

To set the maximum number of times the authenticator sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client, use the **dot1x max-reauth-req** command in interface configuration mode. To set the maximum number of times to the default setting of 2, use the **no** form of this command.

dot1x max-reauth-req *number*

no dot1x max-reauth-req

Syntax Description	<i>number</i>	Maximum number of times. The range is 1 through 10. The default is 2.
---------------------------	---------------	---

Command Default	The command default is 2.
------------------------	---------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.2(18)SE	This command was introduced.
12.2(25)SEC	The <i>number</i> argument was added.	
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.	
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.	

Usage Guidelines	You should change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.
-------------------------	---

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Verifying Settings

You can verify your settings by entering the **show dot1x [interface *interface-id*]** command.

Examples	The following example shows how to set 4 as the number of times that the authentication process is restarted before changing to the unauthorized state:
-----------------	---

```
Router(config-if)# dot1x max-reauth-req 4
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
  description switchport connect to a client
  !
interface FastEthernet1
  description switchport connect to a client
  !
interface FastEthernet2
  description switchport connect to a client
  !
interface FastEthernet3
  description switchport connect to a client
  !
interface FastEthernet4
  description Connect to the public network
  !
interface Vlan1
  description Apply 802.1x functionality on SVI
  dot1x pae authenticator
  dot1x port-control auto
  dot1x reauthentication
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that a device can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process .
dot1x timeout tx-period	Sets the number of seconds that the switch waits for a response to an EAP request or identity frame from the client before resending the request.
show dot1x	Displays IEEE 802.1X status for the specified port.

dot1x max-req

To set the maximum number of times that a router or Ethernet switch network module can send an Extensible Authentication Protocol (EAP) request/identity frame to a client (assuming that a response is not received) before restarting the authentication process, use the **dot1x max-req** command in interface configuration or global configuration mode. To set the number of times to the default setting of 2, use the **no** form of this command.

dot1x max-req *number*

no dot1x max-req

Syntax Description	<i>number</i>	Maximum number of retries. The value is from 1 through 10. The default value is 2. The value is applicable to all EAP packets except for Request ID.
---------------------------	---------------	--

Defaults	The default number of retries is 2.
-----------------	-------------------------------------

Command Modes	Interface configuration (router) Global configuration (EtherSwitch)
----------------------	--

Command History	Release	Modification
	12.1(6)EA2	This command was introduced for the Cisco Ethernet Switch Module.
	12.1(11)AX	This command was integrated into Cisco IOS Release 12.1(11)AX.
	12.1(14)EA1	This command was integrated into Cisco IOS Release 12.1(14)EA1, and the configuration mode was changed to interface configuration mode.
	12.2(15)ZJ	This command was implemented on the following platforms for the Cisco Ethernet switch network module: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.
	12.3(2)XA	This command was introduced on the following Cisco routers: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. Router support was added for the following platforms: Cisco 1751, Cisco 2610XM – Cisco 2611XM, Cisco 2620XM – Cisco 2621XM, Cisco 2650XM – Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.
	12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.

Usage Guidelines	You should change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.
-------------------------	---

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows that the maximum number of times that the router will send an EAP request or identity message to the client PC is 6:

```
Router (config) configure terminal
Router (config)# interface ethernet 0
Router (config-if)# dot1x max-req 6
```

The following example shows how to set the number of times that a switch sends an EAP request or identity frame to 5 before restarting the authentication process:

```
Router (config-if)# dot1x max-req 5
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
  description switchport connect to a client
  !
interface FastEthernet1
  description switchport connect to a client
  !
interface FastEthernet2
  description switchport connect to a client
  !
interface FastEthernet3
  description switchport connect to a client
  !
interface FastEthernet4
  description Connect to the public network
  !
interface Vlan1
  description Apply 802.1x functionality on SVI
  dot1x pae authenticator
  dot1x port-control auto
  dot1x reauthentication
```

Related Commands

Command	Description
dot1x port-control	Enables manual control of the authorization state of a controlled port.
dot1x re-authentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
dot1x reauthentication (EtherSwitch)	Enables periodic reauthentication of the Ethernet switch network module client on the 802.1X interface.
dot1x timeout	Sets retry timeouts.
dot1x timeout (EtherSwitch)	Sets retry timeouts for the Ethernet switch network module.

Command	Description
show dot1x	Displays details for an identity profile.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dot1x max-start

To set the maximum number of Extensible Authentication Protocol (EAP) start frames that a supplicant sends (assuming that no response is received) to the client before concluding that the other end is 802.1X unaware, use the **dot1x max-start** command in global configuration or interface configuration mode. To remove the maximum number-of-times setting, use the **no** form of this command.

dot1x max-start *number*

no dot1x max-start

Syntax Description	<i>number</i>	Maximum number of times that the router sends an EAP start frame. The value is from 1 to 65535. The default is 3.
---------------------------	---------------	---

Defaults The default maximum number setting is 3.

Command Modes Global configuration
Interface configuration

Command History	Release	Modification
	12.3(11)T	This command was introduced.
	12.4(6)T	Global configuration mode was added for this command.
	12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.

Usage Guidelines For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples The following example shows that the maximum number of EAP over LAN- (EAPOL-) Start requests has been set to 5:

```
Router (config)# interface Ethernet1
Router (config-if)# dot1x pae supplicant
Router (config-if)# dot1x max-start 5
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
 description switchport connect to a client
!
interface FastEthernet1
```

■ dot1x max-start

```

description switchport connect to a client
!
interface FastEthernet2
description switchport connect to a client
!
interface FastEthernet3
description switchport connect to a client
!
interface FastEthernet4
description Connect to the public network
!
interface Vlan1
description Apply 802.1x functionality on SVI
dot1x pae authenticator
dot1x port-control auto
dot1x reauthentication

```

Related Commands

Command	Description
dot1x pae	Sets the PAE type during 802.1X authentication.
interface	Configures an interface type.

dot1x multiple-hosts



Note

This command was replaced by the **dot1x host-mode** command effective with Cisco IOS Release 12.1(14)EA1 and Release 12.4(6)T.

To allow multiple hosts (clients) on an 802.1X-authorized switch port that has the **dot1x port-control** interface configuration command set to **auto**, use the **dot1x multiple-hosts** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

dot1x multiple-hosts

no dot1x multiple-hosts

Syntax Description

This command has no arguments or keywords.

Defaults

Multiple hosts are disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.1(14)EA1	This command was replaced by the dot1x host-mode command in Cisco IOS Release 12.(14)EA1.
12.4(6)T	This command was replaced by the dot1x host-mode command on the T-train.

Usage Guidelines

This command is supported only on switch ports.

This command enables you to attach multiple clients to a single 802.1X-enabled port. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (reauthentication fails or an Extensible Authentication Protocol over LAN [EAPOL]-logoff message is received), all attached clients are denied access to the network.

Use the **show dot1x** (EtherSwitch) privileged EXEC command with the **interface** keyword to verify your current 802.1X multiple host settings.

Examples

The following example shows how to enable 802.1X on Fast Ethernet interface 0/1 and to allow multiple hosts:

```
Router(config)# interface fastethernet0/1  
Router(config-if)# dot1x port-control auto  
Router(config-if)# dot1x multiple-hosts
```

Related Commands

Command	Description
dot1x default	Enables manual control of the authorization state of the port.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dot1x pae

To set the Port Access Entity (PAE) type, use the **dot1x pae** command in interface configuration mode. To disable the PAE type that was set, use the **no** form of this command.

dot1x pae [supplicant | authenticator | both]

no dot1x pae [supplicant | authenticator | both]

Syntax Description

supplicant	(Optional) The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.
authenticator	(Optional) The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.
both	(Optional) The interface behaves both as a supplicant and as an authenticator and thus will respond to all dot1x messages.

Defaults

PAE type is not set.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.

Usage Guidelines

If the **dot1x system-auth-control** command has not been configured, the **supplicant** keyword will be the only keyword available for use with this command. (That is, if the **dot1x system-auth-control** command has not been configured, you cannot configure the interface as an authenticator.)

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows that the interface has been set to act as a supplicant:

```
Router (config)# interface Ethernet1
Router (config-if)# dot1x pae supplicant
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

■ dot1x pae

```

interface FastEthernet0
  description switchport connect to a client
  !
interface FastEthernet1
  description switchport connect to a client
  !
interface FastEthernet2
  description switchport connect to a client
  !
interface FastEthernet3
  description switchport connect to a client
  !
interface FastEthernet4
  description Connect to the public network
  !
interface Vlan1
  description Apply 802.1x functionality on SVI
  dot1x pae authenticator
  dot1x port-control auto
  dot1x reauthentication

```

Related Commands

Command	Description
dot1x	Enables 802.1X SystemAuthControl (port-based authentication).
system-auth-control	
interface	Configures an interface type.

dot1x port-control

To enable manual control of the authorization state of a controlled port, use the **dot1x port-control** command in interface configuration mode. To disable the port-control value, use the **no** form of this command.

```
dot1x port-control {auto | force-authorized | force-unauthorized}
```

```
no dot1x port-control {auto | force-authorized | force-unauthorized}
```

Syntax Description

auto	Determines authentication status of the client PC by the authentication process. The port state will be set to auto.
force-authorized	Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The force-authorized keyword is the default.
force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.

Defaults

The default is **force-authorized**.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced for the Cisco Ethernet switch network module.
12.1(11)AX	This command was integrated into Cisco IOS Release 12.1(11)AX.
12.2(15)ZJ	This command was implemented on the following platforms for the Cisco Ethernet switch network module: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.
12.3(2)XA	This command was introduced on the following Cisco routers: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. Router support was added for the following platforms: Cisco 1751, Cisco 2610XM – Cisco 2611XM, Cisco 2620XM – Cisco 2621XM, Cisco 2650XM – Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.

Usage Guidelines**For Ethernet Switch Network Modules**

The following guidelines apply to Ethernet switch network modules:

The 802.1X protocol is supported on Layer 2 static-access ports.

You can use the **auto** keyword only if the port is not configured as one of these types:

- Trunk port—If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.
- EtherChannel port—Before enabling 802.1X on the port, you must first remove it from the EtherChannel. If you try to enable 802.1X on an EtherChannel or on an active port in an EtherChannel, an error appears, and 802.1X is not enabled. If you enable 802.1X on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.
- Switch Port Analyzer (SPAN) destination port—You can enable 802.1X on a port that is a SPAN destination port; however, 802.1X is disabled until the port is removed as a SPAN destination. You can enable 802.1X on a SPAN source port.

To globally disable 802.1X on the device, you must disable it on each port. There is no global configuration command for this task.

For Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Verifying Settings

You can verify your settings by entering the **show dot1x** (EtherSwitch) privileged EXEC command and checking the Status column in the 802.1X Port Summary section of the display. An enabled status means that the port-control value is set to auto or to force-unauthorized.

Examples

The following example shows that the authentication status of the client PC will be determined by the authentication process:

```
Router (config)# configure terminal
Router (config)# interface ethernet 0
Router (config-if)# dot1x port-control auto
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
  description switchport connect to a client
  !
interface FastEthernet1
  description switchport connect to a client
  !
interface FastEthernet2
  description switchport connect to a client
  !
interface FastEthernet3
  description switchport connect to a client
  !
```

```

interface FastEthernet4
  description Connect to the public network
  !
interface Vlan1
  description Apply 802.1x functionality on SVI
  dot1x pae authenticator
  dot1x port-control auto
  dot1x reauthentication

```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that a router or Ethernet switch network module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
dot1x re-authentication	Globally enables periodic reauthentication of the client on the 802.1X interface.
dot1x reauthentication (EtherSwitch)	Enables periodic reauthentication of the Ethernet switch network module client on the 802.1X interface.
dot1x timeout	Sets retry timeouts.
dot1x timeout (EtherSwitch)	Sets retry timeouts for the Ethernet switch network module.
show dot1x	Displays details for an identity profile.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

dot1x re-authenticate (privileged EXEC)

To manually initiate a reauthentication of the specified 802.1X-enabled ports, use the **dot1x re-authenticate** command in privileged EXEC mode.

dot1x re-authenticate [**interface** *interface-name interface-number*]

Syntax Description	interface (Optional) Interface on which reauthentication is to be initiated. <i>interface-name</i> <i>interface-number</i>
---------------------------	---

Command Default There is no default setting.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(11)AX	This command was introduced.
	12.3(2)XA	This command was integrated into Cisco IOS Release 12.3(2)XA.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
	12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.

Usage Guidelines You can use this command to reauthenticate a client without having to wait for the configured number of seconds between reauthentication attempts (re-authperiod) and automatic reauthentication.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples The following example shows how to manually reauthenticate the device that is connected to a port:

```
Router# dot1x re-authenticate interface gigabitethernet2/0/1
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
  description switchport connect to a client
!
interface FastEthernet1
  description switchport connect to a client
```

```
!  
interface FastEthernet2  
  description switchport connect to a client  
!  
interface FastEthernet3  
  description switchport connect to a client  
!  
interface FastEthernet4  
  description Connect to the public network  
!  
interface Vlan1  
  description Apply 802.1x functionality on SVI  
  dot1x pae authenticator  
  dot1x port-control auto  
  dot1x reauthentication
```

Related Commands

Command	Description
dot1x re-authentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
dot1x timeout	Sets retry timeouts.

dot1x reauthentication

To enable periodic reauthentication of the client PCs on the 802.1X interface, use the **dot1x reauthentication** command in interface configuration mode. To disable periodic reauthentication, use the **no** form of this command.

dot1x reauthentication

no dot1x reauthentication

Syntax Description This command has no arguments or keywords.

Defaults Periodic reauthentication is not set.

Command Modes Interface configuration

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.

Usage Guidelines The reauthentication period can be set using the **dot1x timeout** command.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows that reauthentication has been set for 1800 seconds:

```
Router (config)# configure terminal
Router (config)# interface ethernet 0
Router (config-if)# dot1x reauthentication
Router (config-if)# dot1x timeout reauth-period 1800
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)X

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
  description switchport connect to a client
  !
interface FastEthernet1
```

```
description switchport connect to a client
!
interface FastEthernet2
description switchport connect to a client
!
interface FastEthernet3
description switchport connect to a client
!
interface FastEthernet4
description Connect to the public network
!
interface Vlan1
description Apply 802.1x functionality on SVI
dot1x pae authenticator
dot1x port-control auto
dot1x reauthentication
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that a router can send an EAP request/identity frame to a client PC (assuming that a response is not received) before concluding that the client PC does not support 802.1X.
dot1x port-control	Sets an 802.1X port control value.
dot1x timeout	Sets retry timeouts.

dot1x system-auth-control

To globally enable 802.1X SystemAuthControl (port-based authentication), use the **dot1x system-auth-control** command in global configuration mode. To disable SystemAuthControl, use the **no** form of this command.

dot1x system-auth-control

no dot1x system-auth-control

Syntax Description This command has no arguments or keywords.

Defaults System authentication is set to disabled by default. If this command is disabled, all ports behave as if they are force authorized.

Command Modes Global configuration

Command History	Release	Modification
	12.3(2)XA	This command was introduced.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines The **no** form of the command removes any 802.1X-related configurations.

Examples The following example shows that system authentication has been enabled:

```
Router (config)# dot1x system-auth-control
```

Related Commands	Command	Description
	debug dot1x	Displays 802.1X debugging information.
	description	Specifies a description for an 802.1X profile.
	device	Statically authorizes or rejects individual devices.
	dot1x initialize	Initializes 802.1X state machines on all 802.1X-enabled interfaces.
	dot1x max-req	Sets the maximum number of times that a router or Ethernet switch network module can send an Extensible Authentication Protocol (EAP) request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
	dot1x port-control	Enables manual control of the authorized state of a controlled port.
	dot1x re-authenticate	Manually initiates a reauthentication of the specified 802.1X-enabled ports.
	dot1x reauthentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.

Command	Description
dot1x timeout	Sets retry timeouts.
identity profile	Creates an identity profile and enters identity profile configuration mode.
show dot1x	Shows details and statistics for an identity profile.
template	Specifies a virtual template from which commands may be cloned.

dot1x timeout

To set retry timeouts, use the **dot1x timeout** command in global configuration and interface configuration mode. To remove the retry timeouts, use the **no** form of this command.

```
dot1x timeout {auth-period seconds | held-period seconds | quiet-period seconds |
ratelimit-period seconds | reauth-period {seconds | server} | server-timeout seconds |
start-period seconds | supp-timeout seconds | tx-period seconds}
```

```
no dot1x timeout {auth-period seconds | held-period seconds | quiet-period seconds |
ratelimit-period seconds | reauth-period {seconds | server} | server-timeout seconds |
start-period seconds | supp-timeout seconds | tx-period seconds}
```

Syntax Description

auth-period <i>seconds</i>	Time the supplicant (client) waits for a response from an authenticator (for packets other than EAPOL-Start) before timing out. <ul style="list-style-type: none"> The value is from 1 to 65535 seconds. The default is 30 seconds.
held-period <i>seconds</i>	Time for which a supplicant will stay in the “HELD” state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt). <ul style="list-style-type: none"> The value is from 1 to 65535 seconds. The default is 60 seconds.
quiet-period <i>seconds</i>	Configures the number of seconds that the authenticator (server) remains quiet (in the HELD state) following a failed authentication exchange before trying to reauthenticate the client. The no prefix before this keyword and argument configures the default value of 60 seconds. <ul style="list-style-type: none"> The range is from 1 through 65535 seconds. The default is 120 seconds.
ratelimit-period <i>seconds</i>	Throttles the EAP-START packets that are sent from misbehaving client PCs (for example, PCs that send EAP-START packets that result in the wasting of router processing power). <ul style="list-style-type: none"> The authenticator ignores EAPOL-Start packets from clients that have successfully authenticated for the rate-limit period duration. The no prefix before this keyword and argument configures the rate-limit period to the default value of 0. The value is from 1 to 65535 seconds. By default, rate limiting is disabled.
reauth-period { <i>seconds</i> server }	Time after which an automatic reauthentication should be initiated. The no prefix before this keyword and argument configures the default value of 3600 seconds. <ul style="list-style-type: none"> The server keyword indicates that the reauthentication period value for the client should be obtained from the authentication, authorization, and accounting (AAA) server as Session-Timeout (RADIUS Attribute 27). If the server keyword is used, the action upon reauthentication is also decided by the server and sent as Termination-Action (RADIUS Attribute 29). The termination action could be either “terminate” or “reauthenticate.” If the server keyword is not used, the termination action is always “reauthenticate.” The value is from 1 to 65535 seconds. The default is 3600 seconds.

server-timeout <i>seconds</i>	Interval between two successive EAPOL-Start frames when they are being retransmitted. <ul style="list-style-type: none"> The value is from 1 to 65535 seconds. The default is 30 seconds. If an 802.1X packet is sent to the server and the server does not send a response, after the period specified by server-timeout value, the packet is sent again.
start-period <i>seconds</i>	Interval between two successive EAPOL-Start frames when they are being retransmitted. <ul style="list-style-type: none"> The value is from 1 to 65535 seconds. The default is 30 seconds.
supp-timeout <i>seconds</i>	Sets the authenticator-to-supplicant retransmission time for all EAP messages other than EAP Request ID. The no prefix before this keyword and argument configures the retransmission time to the default value of 30 seconds. <ul style="list-style-type: none"> The range is 1 to 65535.
tx-period <i>seconds</i>	Configures the number of seconds between retransmission of EAP request frames (assuming that no response is received) to the client. The no prefix before this keyword and argument configures the default value of 30 seconds. <ul style="list-style-type: none"> The value is from 1 to 65535 seconds. The default is 30 seconds. The value is applicable only to EAP Request ID packets. If an 802.1X packet is sent to the supplicant and the supplicant does not send a response after the retry period, the packet will be sent again.

Defaults

Periodic reauthentication and periodic rate-limiting are not done.

Command Modes

Global configuration
Interface configuration

Command History

A Release	Modification
12.1(11)AX	This command was introduced.
12.1(14)EA1	The supp-timeout and server-timeout keywords were added. The configuration mode for the command was changed to the interface configuration mode.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(2)X	This command was integrated into Cisco IOS Release 12.3(2)X.
12.3(11)T	The auth-period , held-period , and start-period keywords were added.
12.2(18)SE	Ranges for the server-timeout , supp-timeout , and tx-period keywords were changed.
12.2(25)SEC	The range for the tx-period keyword was changed, and the reauth-period and server-timeout keywords were added.

A Release	Modification
12.4(6)T	The supp-timeout keyword was added to the T-train.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.

Usage Guidelines

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows that various 802.1X retransmission and timeout periods have been set:

```
Router (config)# configure terminal
Router (config)# interface ethernet 0
Router (config-if)# dot1x port-control auto
Router (config-if)# dot1x reauthentication
Router (config-if)# dot1x timeout auth-period 2000
Router (config-if)# dot1x timeout held-period 2400
Router (config-if)# dot1x timeout reauth-period 1800
Router (config-if)# dot1x timeout quiet-period 600
Router (config-if)# dot1x timeout start-period 90
Router (config-if)# dot1x timeout supp-timeout 300
Router (config-if)# dot1x timeout tx-period 60
Router (config-if)# dot1x timeout server-timeout 60
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
  description switchport connect to a client
  !
interface FastEthernet1
  description switchport connect to a client
  !
interface FastEthernet2
  description switchport connect to a client
  !
interface FastEthernet3
  description switchport connect to a client
  !
interface FastEthernet4
  description Connect to the public network
  !
interface Vlan1
  description Apply 802.1x functionality on SVI
  dot1x pae authenticator
  dot1x port-control auto
  dot1x reauthentication
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that a router or Ethernet switch module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
dot1x port-control	Sets an 802.1X port control value.
dot1x re-authentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.

eap



Note

This command is removed effective with Cisco IOS Release 12.4(6)T.

To specify Extensible Authentication Protocol- (EAP-) specific parameters, use the **eap** command in identity profile configuration mode. To disable the parameters that were set, use the **no** form of this command.

```
eap {username name | password password}
```

```
no eap {username name | password password}
```

Syntax Description

username <i>name</i>	Username that will be sent to Request-Id packets.
password <i>password</i>	Password that should be used when replying to an Message Digest 5 (MD5) challenge.

Defaults

EAP parameters are not set.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.4(6)T	This command was removed.

Usage Guidelines

Use this command if your router is configured as a supplicant. This command provides the means for configuring the identity and the EAP MD5 password that will be used by 802.1X to authenticate.

Examples

The following example shows that the EAP username “user1” has been configured:

```
Router (config)# identity profile dot1x
Router (config-identity-prof)# eap username user1
```

Related Commands

Command	Description
identity profile	Creates an identity profile.

identity profile

To create an identity profile and to enter identity profile configuration mode, use the **identity profile** command in global configuration mode. To disable an identity profile, use the **no** form of this command.

```
identity profile { default | dot1x | eapoudp }
```

```
no identity profile { default | dot1x | eapoudp }
```

Syntax Description

default	Service type is default.
dot1x	Service type for 802.1X.
eapoudp	Service type for Extensible Authentication Protocol over UDP (EAPoUDP).

Defaults

An identity profile is not created.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	The eapoudp keyword was added.
12.4(6)T	The dot1x keyword was removed.

Usage Guidelines

The **identity profile** command and **default** keyword allow you to configure static MAC addresses of a client computer that does not support 802.1X and to authorize or unauthorize them statically. After you have issued the **identity profile** command and **default** keyword and are in identity profile configuration mode, you can specify the configuration of a template that can be used to create the virtual access interface to which unauthenticated supplicants (client computers) will be mapped.

The **identity profile** command and the **dot1x** keyword are used by the supplicant and authenticator. Using the **dot1x** keyword, you can set the username, password, or other identity-related information for an 802.1X authentication.

Using the **identity profile** command and the **eapoudp** keyword, you can statically authenticate or unauthenticate a device either on the basis of the device IP address or MAC address or on the type, and the corresponding network access policy can be specified using the **identity policy** command.

Examples

The following example shows that an identity profile and its description have been specified:

```
Router (config)# identity profile default  
Router (config-identity-prof)# description description_entered_here
```

The following example shows that an EAPoUDP identity profile has been created:

```
Router (config)# identity policy eapoudp
```

Related Commands	Command	Description
	debug dot1x	Displays 802.1X debugging information.
	description	Specifies a description for an 802.1X profile.
	device	Statically authorizes or rejects individual devices.
	dot1x initialize	Initializes 802.1X state machines on all 802.1X-enabled interfaces.
	dot1x max-req	Sets the maximum number of times that a router can send an EAP request/identity frame to a client PC.
	dot1x max-start	Sets the maximum number of times the authenticator sends an EAP request/identity frame (assuming that no response is received) to the client.
	dot1x pae	Sets the PAE type during 802.1X authentication.
	dot1x port-control	Enables manual control of the authorization state of a controlled port.
	dot1x re-authenticate	Manually initiates a reauthentication of the specified 802.1X-enabled ports.
	dot1x re-authentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
	dot1x system-auth-control	Enables 802.1X SystemAuthControl (port-based authentication).
	dot1x timeout	Sets retry timeouts.
	identity policy	Creates an identity policy.
	show dot1x	Displays details for an identity profile.
	template (identity profile)	Specifies a virtual template from which commands may be cloned.

macro global

To apply a macro to a router or switch or to apply and trace a macro configuration on a router or switch, use the **macro global** command in global configuration mode. To remove the macro, use the **no** form of this command.

```
macro global { apply | trace } macro-name [parameter { value }] [parameter { value } ...]
```

```
no macro global { apply | trace } macro-name [parameter { value }]
```

Syntax Description

apply	Applies a macro to a router or switch.
trace	Applies a macro to a router or switch and debugs the macro.
<i>macro-name</i>	Name of the macro.
parameter <i>value</i>	(Optional) Specifies unique parameter values that are specific to the router or switch. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value.

Command Default

A macro is not applied.

Command Modes

Global configuration

Command History

Release	Modification
12.2(20)SE	This command was introduced.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs).

Usage Guidelines

You can use the macro trace **macro name** command to apply and to show the macros that are running on a switch or to debug the macro to find any syntax or configuration errors.

If a command fails because of a syntax error or a configuration error when you apply a macro, the macro continues to apply the remaining commands to the switch.

When creating a macro that requires the assignment of unique values, use the **parameter** keyword to designate values that are specific to the switch.

Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a larger string, is considered a match and is replaced by the corresponding value.

Some macros might contain keywords that require a parameter value. You can use the **macro global** command to display a list of any required values in the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied.

There are Cisco-default Smartports macros embedded in the router and switch software. You can display these macros and the commands they contain by using the **show parser macro** command and **name** keyword.

Follow these guidelines when you apply a Cisco-default Smartports macro on a router or switch:

- Display all macros on the router or switch by using the **show parser macro** command. Display the contents of a specific macro by using the **show parser macro name** command.
- Keywords that begin with \$ mean that a unique parameter value is required. Append the Cisco-default macro with the required values by using the **parameter value** keyword and argument.

The Cisco-default macros use the \$ character to help identify required keywords. There is no restriction on using the \$ character to define keywords when you create a macro.

When you apply a macro to a router or switch, the macro name is automatically added to the switch. You can display the applied commands and macro names by using the **show running-config** command.

You can delete a global macro-applied configuration on a router or switch only by entering the **no** version of each command that is contained in the macro.

Examples

After you have created a new macro by using the **macro name** command, you can apply it to a router or switch. The following example shows how to see the “snmp” macro, how to apply the macro, and how to set the hostname to “test-server” and the IP precedence value to 7:

```
Router# show parser macro name snmp

Macro name : snmp
Macro type : customizable
# enable port security, linkup, and linkdown traps
snmp-server enable traps port-security
snmp-server enable traps linkup
snmp-server enable traps linkdown
# set snmp-server host
snmp-server host ADDRESS
# set SNMP trap notifications precedence
snmp-server ip precedence VALUE
-----

Router (config)# macro global apply snmp ADDRESS test-server VALUE 7
```

To debug a macro, use the **macro global** command with the **trace** keyword to find any syntax or configuration errors in the macro when it is applied to a switch. In the following example, the **ADDRESS** parameter value was not entered, causing the **snmp-server host** command to fail while the remainder of the macro is applied to the router or switch:

```
Router(config)# macro global trace snmp VALUE 7
Applying command...'snmp-server enable traps port-security'
Applying command...'snmp-server enable traps linkup'
Applying command...'snmp-server enable traps linkdown'
Applying command...'snmp-server host'
%Error Unknown error.
Applying command...'snmp-server ip precedence 7'
```

Related Commands

Command	Description
macro name	Creates a macro.

macro name

To create a configuration macro on a router or switch, use the **macro name** command in global configuration mode. To delete the macro definition, use the **no** form of this command.

macro name *macro-name*

no macro name *macro-name*

Syntax Description	<i>macro-name</i>	Name of the macro.
---------------------------	-------------------	--------------------

Command Default	A macro is not created.
------------------------	-------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.1(19)EA1	This command was introduced.
	12.2(20)SE	This command was integrated into Cisco IOS Release 12.2(20)SE, and the help string “# macro keywords” was added.
	12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs).

Usage Guidelines

A macro can contain up to 3000 characters. Enter one macro command per line. Use the @ character to end the macro. Use the # character at the beginning of a line to enter comment text within the macro. You can define mandatory keywords within a macro by using a help string to specify the keywords. Enter macro keywords to define the keywords that are available for use with the macro. You can enter up to three help string keywords separated by a space. If you enter more than three macro keywords, only the first three are shown.

Macro names are case sensitive. For example, the commands **macro name Sample-Macro** and **macro name sample-macro** will result in two separate macros.

When creating a macro, do not use the **exit** or **end** commands or change the command mode by using **interface interface-id**. This could cause commands that follow **exit**, **end**, or **interface interface-id** to execute in a different command mode.

The **no** form of this command only deletes the macro definition. It does not affect the configuration of those interfaces on which the macro is already applied. You can delete a macro-applied configuration on an interface by entering the default **interface interface-id** command.

Alternatively, you can create an anti-macro for an existing macro that contains the **no** form of all the corresponding commands in the original macro. Then apply the anti-macro to the interface.

You can modify a macro by creating a new macro with the same name as the existing macro. The newly created macro overwrites the existing macro but does not affect the configuration of those interfaces on which the original macro was applied.

Examples

The following example shows how to create a macro that defines the duplex mode and speed:

```
Router (config)# macro name duplex
Enter macro commands one per line. End with the character '@'.
duplex full
speed auto
@
```

The following example shows how create a macro with # macro keywords:

```
Router (config)# macro name test
switchport access vlan $VLANID
switchport port-security maximum $MAX
#macro keywords $VLANID $MAX
@
```

The following example shows how to display the mandatory keyword values before you apply the macro to an interface:

```
Router (config)# interface gigabitethernet1/0/1
Router (config-if)# macro apply test ?
WORD keyword to replace with a value e.g $VLANID,$MAX
<cr>
Router (config-if)# macro apply test $VLANID ?
WORD Value of first keyword to replace
Router (config-if)# macro apply test $VLANID 2
WORD keyword to replace with a value e.g $VLANID,$MAX
<cr>
Router (config-if)# macro apply test $VLANID 2 $MAX ?
WORD Value of second keyword to replace
```

Related Commands

Command	Description
macro global	Applies a macro to a router or switch or traces a macro configuration on a router or switch.

password (dot1x credentials)

To specify the password for an 802.1X credentials profile, use the **password** command in dot1x credentials configuration mode. To remove the password, use the **no** form of this command.

```
password [0 | 7] password
```

```
no password
```

Syntax Description		
	0	(Optional) A plain text password will follow. The default is 0.
	7	(Optional) An encrypted password will follow. The default is 0.
	<i>password</i>	The password.

Command Default A password is not specified.

Command Modes Dot1x credentials configuration

Command History	Release	Modification
	12.4(6)T	This command was introduced.

Usage Guidelines Before using this command, the **dot1x credentials** command must have been configured.

Examples The following example shows which credentials profile should be used when configuring a supplicant. The password is “secret.”

```
dot1x credentials basic-user
username router
password secret
description This credentials profile should be used for most configured ports
```

The credentials structure can be applied to an interface along with the **dot1x pae supplicant** command and keyword to enable supplicant functionality on that interface.

```
interface fastethernet 0/1
dot1x credentials basic-user
dot1x pae supplicant
```

Related Commands	Command	Description
	dot1x credentials	Specifies the 802.1X credentials profile to be used.

show dot1x

To display details for an identity profile, use the **show dot1x** command in privileged EXEC mode.

show dot1x [**all** | **interface** *interface-name* [**details** | **statistics**]] [**statistics**]

Syntax Description		
all	(Optional)	Displays 802.1X status for all ports.
interface <i>interface-name</i>	(Optional)	Displays 802.1X status for the specified port (including type, stack member, module, and port number).
interface <i>interface-name</i> details	(Optional)	Displays the interface configuration as well as the authenticator instances on the interface.
interface <i>interface-name</i> statistics	(Optional)	Displays the interface statistics.
statistics	(Optional)	Displays 802.1X statistics for all the interfaces.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(11)AX	This command was introduced.
	12.1(14)EA1	The all keyword was added.
	12.3(2)XA	This command was integrated into Cisco IOS Release 12.3(2)XA.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
	12.2(25)SED	The output display was expanded to include auth-fail-vlan information in the authorization state machine state and port status fields.
	12.2(25)SEE	The details and statistics keywords were added.
	12.3(11)T	The PAE, HeldPeriod, StartPeriod, and MaxStart fields were added to the show dot1x command output.

Usage Guidelines If you do not specify a port, global parameters and a summary appear. If you specify a port, details for that port appear in the output.

Examples The following is sample output for the **show dot1x** command:

```
Router# show dot1x

Sysauthcontrol = Disabled
Dot1x Version = 1

Dot1x Info for interface Ethernet0
-----
PortControl = AUTO
ReAuthentication = Disabled
ReAuthPeriod = 3600 Seconds
```

```

ServerTimeout      = 30 Seconds
SuppTimeout        = 30 Seconds
QuietWhile         = 120 Seconds
MaxReq             = 2

```

```
Dot1x Info for interface Ethernet1
```

```

-----
PortControl        = AUTO
ReAuthentication   = Disabled
ReAuthPeriod       = 3600 Seconds
ServerTimeout      = 30 Seconds
SuppTimeout        = 30 Seconds
QuietWhile         = 120 Seconds
MaxReq             = 2

```

The following is sample output for the **show dot1x** command using both the **interface** and **interface details** keywords. The clients are authenticated in this output example.

```
Router# show dot1x interface ethernet 0 details
```

```

PortControl        = AUTO
ReAuthentication   = Enabled
ReAuthPeriod       = 36000 Seconds
ServerTimeout      = 30 Seconds
SuppTimeout        = 30 Seconds
QuietWhile         = 120 Seconds
MaxReq             = 2

```

```
Dot1x Client List
```

```

-----
MAC Address        State
-----
0000.1111.0001    AUTHENTICATED
0000.1111.0002    UNAUTHENTICATED

```

The following **show dot1x** sample output shows information for all three possible interface configurations (that is, as an authenticator, as a supplicant, and as an authenticator and supplicant).

```
Router# show dot1x
```

```

Sysauthcontrol     = Enabled
Dot1x Version      = 1

```

```
Dot1x Information for interface Ethernet0
```

```

-----
PortControl        = AUTO
PAE                 = AUTHENTICATOR
ReAuthentication   = Enabled
ReAuthPeriod       = 60 Seconds
ServerTimeout      = 30 Seconds
SuppTimeout        = 30 Seconds
QuietWhile         = 120 Seconds
MaxReq             = 2

```

```
Dot1x Information for interface Ethernet1
```

```

-----
PortControl        = AUTO
PAE                 = SUPPLICANT
AuthPeriod         = 30
HeldPeriod         = 60 Seconds
StartPeriod        = 30 Seconds
MaxStart           = 2

```

```

Dot1x Information for interface Ethernet2
-----
PortControl          = AUTO
PAE                  = BOTH
ReAuthentication     = Enabled
ReAuthPeriod        = 60 Seconds
ServerTimeout       = 30 Seconds
SuppTimeout         = 30 Seconds
QuietWhile          = 120 Seconds
MaxReq               = 2
AuthPeriod          = 30
HeldPeriod           = 60 Seconds
StartPeriod         = 30 Seconds
MaxStart            = 2

```

The following is sample output for the **show dot1x** command using the **interface** and **details** keywords.

```

Router# show dot1x interface ethernet0

PortControl          = AUTO
PAE                  = AUTHENTICATOR
ReAuthentication     = Enabled
ReAuthPeriod        = 60 Seconds
ServerTimeout       = 30 Seconds
SuppTimeout         = 30 Seconds
QuietWhile          = 120 Seconds
MaxReq               = 2

Router# show dot1x interface ethernet0 details

PortControl          = AUTO
PAE                  = SUPPLICANT
ReAuthentication     = Enabled
ReAuthPeriod        = 60 Seconds
ServerTimeout       = 30 Seconds
SuppTimeout         = 30 Seconds
QuietWhile          = 120 Seconds
MaxReq               = 2

```

```

Dot1x Client List
-----
MAC Address          State
-----
0001.f380.87ce       AUTHENTICATED
0001.87ce.f380       AUTHENTICATING
0010.a7b4.97af       UNAUTHENTICATED

```

```

Dot1x List of Supplicant Instances
-----
MAC Address          State
-----
0180.c200.0003       AUTHORIZED

```

Table 1 describes the significant fields shown in the displays.

Table 1 *show dot1x Field Descriptions*

Field	Description
Sysauthcontrol	802.1X port-based authentication is enabled or disabled.
PortControl	Port control value. <ul style="list-style-type: none"> AUTO—the authentication status of the client PC is being determined by the authentication process. Force-authorize—all the client PCs on the interface are being authorized. Force-unauthorized—all the client PCs on the interface are being unauthorized.
PAE	Port Access Entity. Defines the role of an interface (as a supplicant, as an authenticator, or as an authenticator and supplicant).
ReAuthentication	Periodic reauthentication of client PCs on the interface has been enabled or disabled.
ReAuthPeriod	Time after which an automatic reauthentication will be initiated.
ServerTimeout	Timeout that has been set 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 number of seconds that are shown.
SuppTimeout	Time that has been set for supplicant (client PC) 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 number of seconds that are shown.
QuietWhile	After authentication fails for a client, the authentication gets restarted after the quiet period that is shown.
MaxReq	Maximum number of times that the router sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client PC before concluding that the client PC does not support 802.1X.
HeldPeriod	Interval for which the supplicant (client PC) will wait before trying to send its credentials after being unauthenticated by the authenticator.
StartPeriod	Interval between two successive Extensible Authentication Protocol over LAN- (EAPOL-) start messages (when they are being retransmitted).
MaxStart	Number of EAPOL-start messages that the supplicant (client PC) sends before the supplicant assumes that the other end is not 802.1X capable.

Table 1 *show dot1x Field Descriptions (continued)*

Field	Description
Dot1x Client List	Table providing information regarding MAC addresses and the state of the PCs. This list displays in the output if the interface is configured only as an authenticator or as an authenticator and a supplicant. If the interface is configured as a supplicant, a separate list is displayed.
Dot1x List of Supplicant Instances	Table providing information regarding MAC addresses and the state of the PCs. This list displays in the output if the interface is configured only as a supplicant.
MAC Address	List of MAC addresses (for example, the MAC address of the PC or of any 802.1X client).
State	The state of the PC can be authenticated or unauthenticated.

Related Commands

Command	Description
clear dot1x	Clears 802.1X interface information.
debug dot1x	Displays 802.1X debugging information.
dot1x default	Resets the global 802.1X parameters to their default values.
identity profile	Creates an identity profile.

show eap registrations

To display Extensible Authentication Protocol (EAP) registration information, use the **show eap registrations** command in privileged EXEC mode.

show eap registrations [method | transport]

Syntax Description	method	(Optional) Displays information about EAP method registrations only.
	transport	(Optional) Displays information about EAP transport registrations only.

Command Default If a keyword is not used, information is displayed for all lower layers used by EAP and for the methods that are registered with the EAP framework.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(25)SEE	This command was introduced.
	12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines This command is used to check which EAP methods are enabled on a router.

Examples The following is an example of output from the **show eap registrations** command:

```
Router# show eap registrations

Registered EAP Methods:
Method Type Name
4 Peer MD5
Registered EAP Lower Layers:
Handle Type Name
2 Authenticator Dot1x-Authenticator
1 Authenticator MAB
```

The following is an example of output from the **show eap registrations** command using the transport keyword:

```
Router# show eap registrations transport

Registered EAP Lower Layers:
Handle Type Name
2 Authenticator Dot1x-Authenticator
```

The output fields are self-explanatory.

■ show eap registrations

Related Commands

Command	Description
clear eap	Clears EAP session information for the switch or specified port.

show eap sessions

To display active Extensible Authentication Protocol (EAP) session information, use the **show eap sessions** command in privileged EXEC mode.

show eap sessions [**credentials** *credentials-name* | **interface** *interface-name* | **method** *method-name* | **transport** *transport-name*]

Syntax Description		
credentials <i>credentials-name</i>	(Optional)	Displays information about the specified credentials profile.
interface <i>interface-name</i>	(Optional)	Displays information, such as type, module, and port number, about sessions that are associated with the specified interface.
method <i>method-name</i>	(Optional)	Displays information about sessions that are associated with the specified EAP method.
transport <i>transport-name</i>	(Optional)	Displays information about sessions that are associated with the specified lower layer.

Command Default All active EAP sessions are displayed.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(25)SEE	This command was introduced.
	12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines The command output can be filtered using any of the optional keywords, singly or in combination.

Examples The following is an example of output from the **show eap sessions** command:

```
Router# show eap sessions

Role: Authenticator Decision: Fail
Lower layer: Dot1x-AuthenticaInterface: Gi1/0/1
Current method: None Method state: Uninitialised
Retransmission count: 0 (max: 2) Timer: Authenticator
ReqId Retransmit (timeout: 30s, remaining: 2s)
EAP handle: 0x5200000A Credentials profile: None
Lower layer context ID: 0x93000004 Eap profile name: None
Method context ID: 0x00000000 Peer Identity: None
Start timeout (s): 1 Retransmit timeout (s): 30 (30)
Current ID: 2 Available local methods: None
Role: Authenticator Decision: Fail
Lower layer: Dot1x-AuthenticaInterface: Gi1/0/2
Current method: None Method state: Uninitialised
Retransmission count: 0 (max: 2) Timer: Authenticator
```

■ show eap sessions

```
ReqId Retransmit (timeout: 30s, remaining: 2s)
EAP handle: 0xA800000B Credentials profile: None
Lower layer context ID: 0x0D000005 Eap profile name: None
Method context ID: 0x00000000 Peer Identity: None
Start timeout (s): 1 Retransmit timeout (s): 30 (30)
Current ID: 2 Available local methods: None
.
.
.
```

The following is an example of output from the **show eap sessions interface** command:

```
Router# show eap sessions interface gigabitethernet1/0/1
```

```
Role: Authenticator Decision: Fail
Lower layer: Dot1x-AuthenticataInterface: Gi1/0/1
Current method: None Method state: Uninitialised
Retransmission count: 1 (max: 2) Timer: Authenticator
ReqId Retransmit (timeout: 30s, remaining: 13s)
EAP handle: 0x5200000A Credentials profile: None
Lower layer context ID: 0x93000004 Eap profile name: None
Method context ID: 0x00000000 Peer Identity: None
Start timeout (s): 1 Retransmit timeout (s): 30 (30)
```

The fields in the above output are self-explanatory.

Related Commands

Command	Description
clear eap sessions	Clears EAP session information for the switch or for the specified port.

show ip igmp snooping

To display the Internet Group Management Protocol (IGMP) snooping configuration of a device, use the **show ip igmp snooping** command in privileged EXEC mode.

```
show ip igmp snooping [groups] [mrouter] [querier] [vlan vlan-id]
```

Syntax Description	groups	(Optional) Displays group information.
	mrouter	(Optional) Displays information about dynamically learned and manually configured multicast router ports.
	querier	(Optional) Displays IGMP querier information.
	vlan <i>vlan-id</i>	(Optional) Specifies a VLAN. Valid values are 1 to 1001. If this keyword is not configured, information is displayed for all VLANs.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.
	12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
	12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC on Cisco 870 series Integrated Services Routers (ISRs). The groups and querier keywords were added.

Usage Guidelines You can also use the **show mac-address-table multicast** command to display entries in the MAC address table for a VLAN that has IGMP snooping enabled.

Examples The following is sample output from the **show ip igmp snooping** command:

```
Router# show ip igmp snooping

Global IGMP Snooping configuration:
-----
IGMP snooping                : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Last Member Query Interval   : 1000

Vlan 1:
-----
IGMP snooping                : Enabled
```

show ip igmp snooping

```
IGMPv2 immediate leave      : Enabled
Explicit host tracking      : Enabled
Multicast router learning mode : pim-dvmrp
Last Member Query Interval  : 1000
CGMP interoperability mode  : IGMP_ONLY
```

Vlan 11:

```
-----
IGMP snooping              : Enabled
IGMPv2 immediate leave     : Disabled
Explicit host tracking      : Enabled
Multicast router learning mode : pim-dvmrp
Last Member Query Interval  : 1000
CGMP interoperability mode  : IGMP_ONLY
```

The following is sample output from the **show ip igmp snooping** command using the **vlan** keyword:

```
Router# show ip igmp snooping vlan 1
```

```
vlan 1
-----
IGMP snooping is globally enabled
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is enabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
```

The following is sample output from the **show ip igmp snooping** command using the **mrouter** keyword:



Note

In this example, Fa0/3 is a dynamically learned router port, and Fa0/2 is a configured static router port.

```
Router# show ip igmp snooping mrouter vlan 1
```

```
Vlan   ports
----   -
1      Fa0/2(static), Fa0/3(dynamic)
```

The following is sample output from the **show ip igmp snooping** command using the **groups** keyword:

```
Router #show ip igmp snooping groups
Vlan   Group          Version  Port List
-----
1      192.168.1.2      v2      Fa0/1/0
11     192.168.1.2      v2      Fa0/1/1
```

The information in the output display is self-explanatory.

Related Commands

Command	Description
ip igmp snooping	Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN.
ip igmp snooping vlan	Enables IGMP snooping on the VLAN interface.
ip igmp snooping vlan immediate-leave	Enables IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
show mac-address-table multicast	Displays the Layer 2 multicast entries for a VLAN.

template (identity profile)

To specify a virtual template from which commands may be cloned, use the **template** command in identity profile configuration mode. To disable the virtual template, use the **no** form of this command.

template *virtual-template*

no template *virtual-template*

Syntax Description	<i>virtual-template</i>	Specifies the virtual template interface that will serve as the configuration clone source for the virtual interface that is dynamically created for authenticated users.
---------------------------	-------------------------	---

Defaults A virtual template from which commands may be cloned is not specified.

Command Modes Identity profile configuration

Command History	Release	Modification
	12.3(2)XA	This command was introduced.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines The **identity profile** command and **default** keyword must be entered in global configuration mode before the **template** command can be used.

Examples The following example shows that a default identity profile and a template have been specified:

```
Router (config)# identity profile default
Router (config-identity-prof)# template virtualtemplate1
```

Related Commands	Command	Description
	description	Enters an identity profile description.
	device	Statically authorizes or rejects individual devices.
	identity profile	Creates an identity profile.

username (dot1x credentials)

To specify the username for an 802.1X credentials profile, use the **username** command in dot1x credentials configuration mode. To remove the username, use the **no** form of this command.

username *name*

no username

Syntax Description	<i>name</i>	Name of the credentials profile.
---------------------------	-------------	----------------------------------

Command Default	A username is not specified.	
------------------------	------------------------------	--

Command Modes	Dot1x credentials configuration	
----------------------	---------------------------------	--

Command History	Release	Modification
	12.4(6)T	This command was introduced.

Usage Guidelines	Before using this command, the dot1x credentials command must have been configured.	
-------------------------	--	--

Examples	The following example shows which credentials profile should be used when configuring a supplicant:	
-----------------	---	--

```
dot1x credentials basic-user
username router
password secret
description This credentials profile should be used for most configured ports
```

The credentials structure can be applied to an interface, along with the **dot1x pae supplicant** command and keyword, to enable supplicant functionality on that interface.

```
interface fastethernet 0/1
dot1x credentials basic-user
dot1x pae supplicant
```

Related Commands	Command	Description
	dot1x credentials	Specifies an 802.1X credentials profile to be used.

Glossary

authenticator—Entity at one end of a point-to-point LAN segment that enforces host authentication. The authenticator is independent of the actual authentication method and functions only as a pass-through for the authentication exchange. It communicates with the host, submits the information from the host to the authentication server, and authorizes the host when instructed to do so by the authentication server.

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



Note

Refer to *Internetworking Terms and Acronyms* for terms not included in this glossary.

Feature Information for VPN Access Control Using 802.1X Authentication

Table 2 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 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.

Table 2 Feature Information for VPN Access Control Using 802.1X Authentication

Feature Name	Releases	Feature Information
Converged 802.1X Authenticator and Converged 802.1X Supplicant Support	12.4(6)T	<p>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.)</p> <p>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</p>
VPN Access Control Using 802.1X Authentication	12.4(4)XC	<p>Various 802.1X commands were integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.</p> <p>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</p>

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

© 2003 – 2006 Cisco Systems, Inc. All rights reserved.