CHAPTER 46

Configuring 802.1X Port-Based Authentication

This chapter describes how to configure IEEE 802.1X port-based authentication on the Catalyst 4500 series switch to prevent unauthorized client devices from gaining access to the network.

This chapter includes the following major sections:

Note For complete syntax and usage information for the switch commands used in this chapter, see the *Cisco Catalyst 4500 Series Switch Command Reference* and related publications at this location: http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html

If a command is not in the *Catalyst 4500 Series Switch Command Reference*, you can locate it in the Cisco IOS library. See related publications at this location: http://www.cisco.com/en/US/products/ps6350/index.html

About 802.1X Port-Based Authentication

802.1X defines 802.1X port-based authentication as a client-server based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. An authentication server validates each supplicant (client) connected to an authenticator (network access switch) port before making available any services offered by the switch or the LAN.

Note 802.1X support requires an authentication server that is configured for Remote Authentication Dial-In User Service (RADIUS). 802.1X authentication does not work unless the network access switch can route packets to the configured RADIUS server. To verify that the switch can route packets, you must ping the server from the switch.

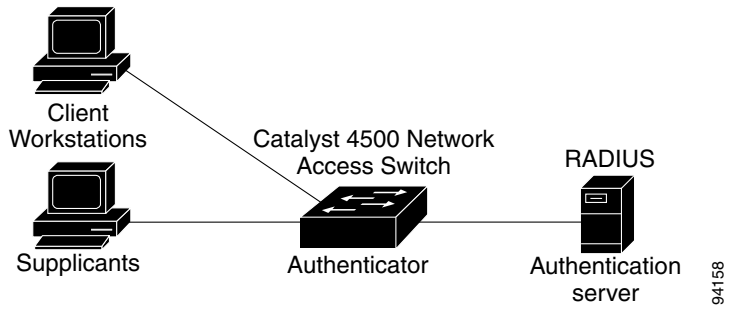
Until a client is authenticated, only Extensible Authentication Protocol over LAN (EAPOL) traffic is allowed using the port to which the client is connected. After authentication succeeds, normal traffic can pass using the port.

To configure 802.1X port-based authentication, you need to understand the concepts in these sections:

Device Roles

With 802.1X port-based authentication, network devices have specific roles. Figure 46-1 shows the role of each device, which is described below.

Figure 46-1 802.1X Device Roles



- Client—The workstation that requests access to the LAN, and responds to requests from the switch. The workstation must be running 802.1X-compliant client software.
- Authenticator—Controls physical access to the network based on the authentication status of the client. The Catalyst 4500 series switch acts as an intermediary between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch encapsulates and decapsulates the Extensible Authentication Protocol (EAP) frames and interacts with the RADIUS authentication server.

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

Note The Catalyst 4500 series switches must be running software that supports the RADIUS client and 802.1X.

- Authentication server—Performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch that the client is authorized to access the LAN and switch services. (The only supported authentication server is the RADIUS authentication server with EAP extensions; it is available in Cisco Secure Access Control Server version 3.2 and later releases.)

802.1X and Network Access Control

Network Access Control is a feature that allows port access policies to be influenced by the antivirus posture of the authenticating device.

Antivirus posture includes such elements as the operating system running on the device, the operating system version, whether antivirus software is installed and what version of antivirus signatures is available. If the authenticating device has a NAC-aware 802.1X supplicant and the authentication server is configured to support NAC using 802.1X, antivirus posture information is automatically included as part of the 802.1X authentication exchange.

For information on NAC, refer to the URL:

http://www.cisco.com/en/US/products/ps6128/index.html

Authentication Initiation and Message Exchange

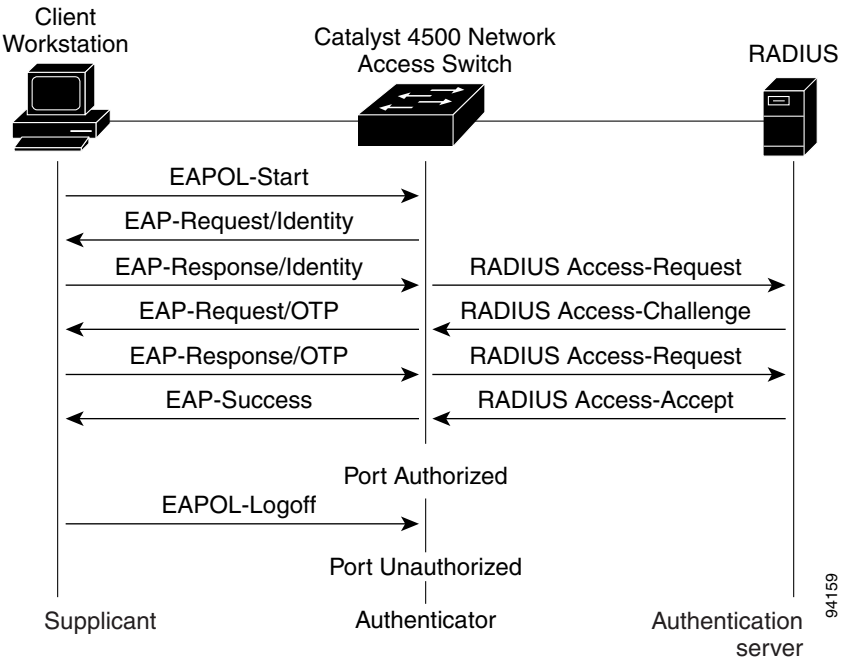
The switch or the client can initiate authentication. If you enable authentication on a port by using the **authentication port-control auto** interface configuration command (**dot1x port-control auto** command in Cisco IOS Release 12.2(46)SG and earlier releases), the switch must initiate authentication when it determines that the port link state has changed. It then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.

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

If 802.1X is not enabled or supported on the network access switch, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state. A port in the authorized state means that the client was successfully authenticated. When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized.

The specific exchange of EAP frames depends on the authentication method being used. Figure 46-2 shows a message exchange that is initiated by the client using the One-Time Password (OTP) authentication method with an authentication server.

Figure 46-2 Message Exchange



Ports in Authorized and Unauthorized States

The switch port state determines whether the client is granted access to the network. The port starts in the unauthorized state. While in this state, the port disallows all ingress and egress traffic except for 802.1X protocol packets. When a client is successfully authenticated, the port transitions to the authorized state, allowing all traffic for the client to flow normally.

If a non-802.1X capable client is connected to an unauthorized 802.1X port, the switch requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network. If a guest VLAN is configured on a port that connects to a client that does not support 802.1X, the port is placed in the configured guest VLAN and in the authorized state. For more information, see the "Using 802.1X for Guest VLANs" section on page 46-11.

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

You can control the port authorization state by using the **authentication port-control** interface configuration command (**dot1x port-control auto** command in Cisco IOS Release 12.2(46)SG and earlier releases) and these keywords:

- **force-authorized**—Disables 802.1X authentication and causes the port to transition to the authorized state without requiring authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. This setting is the default.
- **force-unauthorized**—Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client using the interface.
- **auto**—Allows 802.1X authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received using the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. The switch can uniquely identify each client attempting to access the network by the client's MAC address.

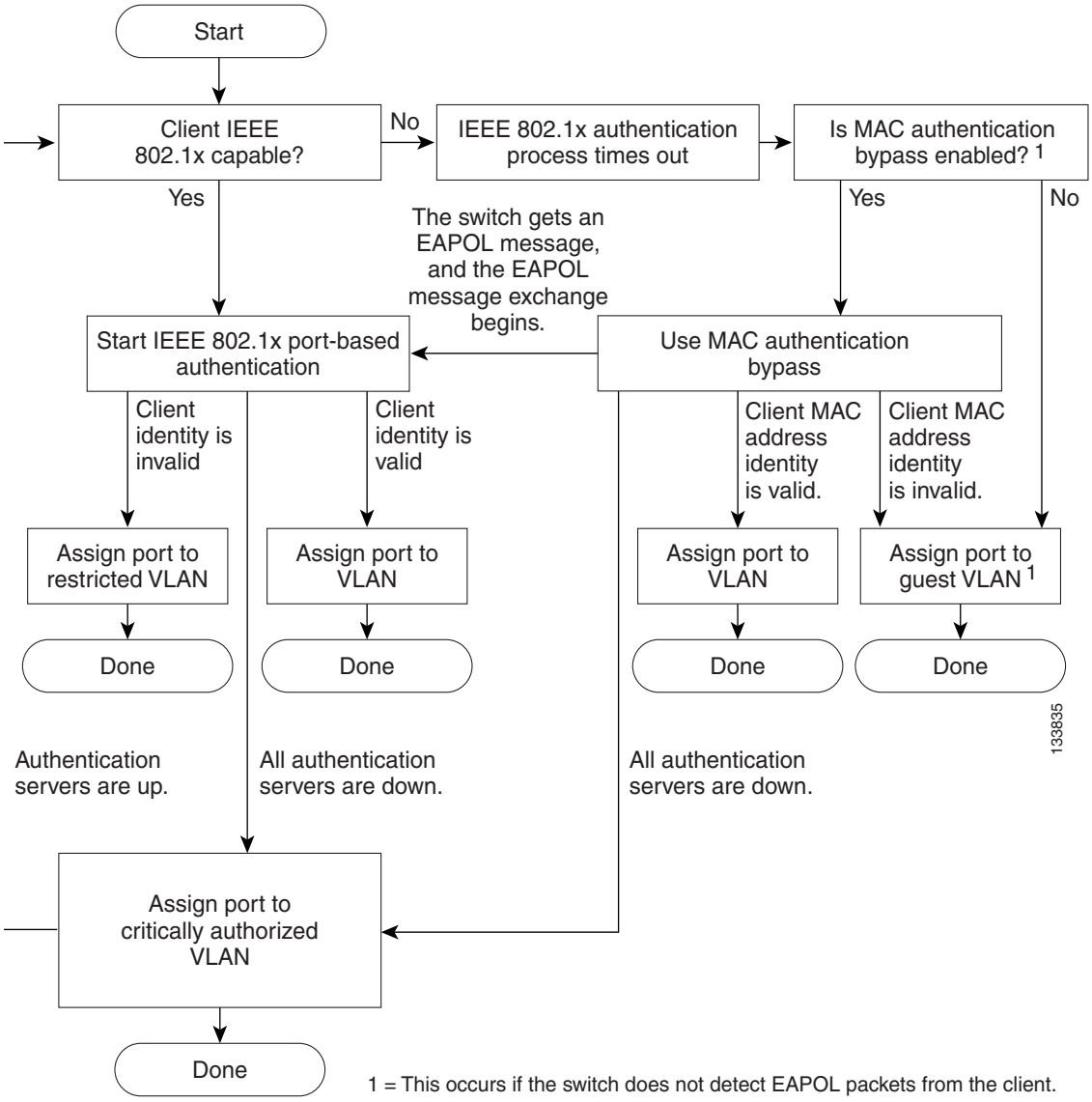
If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed using the port. If authentication fails, the port remains in the unauthorized state, but authentication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

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

If Multidomain Authentication (MDA) is enabled on a port, this flow can be used with some exceptions that are applicable to voice authorization. For more information on MDA, see the "Using Multiple Domain Authentication and Multiple Authentication" section on page 46-22.

Figure 46-3 shows the authentication process.

Figure 46-3 Authentication Flowchart



802.1X Host Mode

The 802.1X port's host mode determines whether more than one client can be authenticated on the port and how authentication is enforced. You can configure an 802.1X port to use any of the five host modes described in the following sections. In addition, each mode can be modified to allow preauthentication open access:

- Single-Host Mode, page 46-7
- Multiple-Hosts Mode, page 46-7
- Multidomain Authentication Mode, page 46-7
- Multiauthentication Mode, page 46-8

- Pre-Authentication Open Access, page 46-8

Single-Host Mode

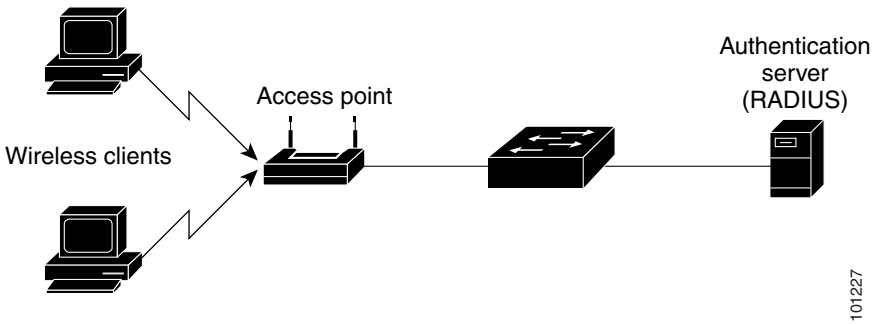
You can configure an 802.1X port for single-host or multiple-hosts mode. In single-host mode (see Figure 46-1 on page 46-3), only one client can be connected to the 802.1X-enabled switch port. The switch detects the client by sending an EAPOL frame when the port link state changes to the up state. If a client leaves or is replaced with another client, the switch changes the port link state to down, and the port returns to the unauthorized state.

Multiple-Hosts Mode

In multiple-hosts mode, you can attach multiple hosts to a single 802.1X-enabled port. Figure 46-4 on page 46-7 shows 802.1X port-based authentication in a wireless LAN. In this mode, only one of the attached clients must be authorized for all clients to be granted network access. If the port becomes unauthorized (reauthentication fails or an EAPOL-logoff message is received), the switch denies network access to all of the attached clients. In this topology, the wireless access point is responsible for authenticating the clients attached to it, and it also acts as a client to the switch.

Note Wired guest access does not work on Supervisor Engine 8-E, in multiple-host mode or in multi-authentication mode.

Figure 46-4 Multiple Host Mode Example



Multidomain Authentication Mode

Beginning with Cisco IOS Release 12.2(37)SG, Catalyst 4500 series switches support Multidomain Authentication (MDA), which allows an IP phone (Cisco or third-party) and a single host behind the IP phone to authenticate independently, using 802.1X, MAC authentication bypass (MAB) or (for the host only) web-based authentication. In this application, *multidomain* refers to two domains — data and voice — and only two MAC addresses are allowed per-port. A switch can place the host in the data VLAN and the IP phone in the voice VLAN, even though they appear on the same switch port. The data VLAN and the voice VLAN can be specified in the CLI configuration. The devices are identified as either data or voice depending on the vendor-specific-attributes (VSAs) received from the authentication, authorization, and accounting (AAA) server. The data and voice VLANs can also be obtained from the VSAs received from the (AAA) server during authentication.

Figure 46-5 Multidomain Authentication Mode Example

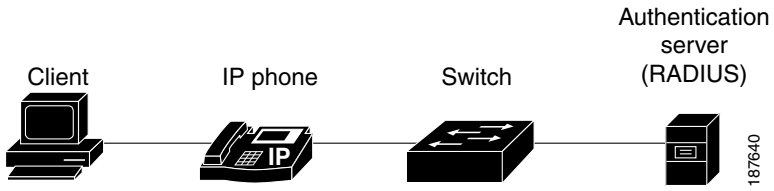


Figure 46-5 shows a typical MDA application with a single host behind an IP phone connected to the 802.1X-enabled port. Because the client is not directly connected to the switch, the switch cannot detect a loss of port link if the client is disconnected. To prevent another device from using the established authentication of the disconnected client later, Cisco IP phones send a Cisco Discovery Protocol (CDP) host presence type length value (TLV) to notify the switch of changes in the attached client's port link state.

For details on how to configure MDA, see the "Using Multiple Domain Authentication and Multiple Authentication" section on page 46-22.

Multiauthentication Mode

Available starting in Cisco IOS Release 12.2(50)SG, multiauthentication mode allows one client on the voice VLAN and multiple authenticated clients on the data VLAN. When a hub or access point is connected to an 802.1X port, multiauthentication mode provides enhanced security over multiple-hosts mode by requiring authentication of each connected client. For non-802.1X devices, you can use MAB or web-based authentication as the fallback method for individual host authentications, allowing you to authenticate different hosts through different methods on a single port.

Multiauthentication also supports MDA functionality on the voice VLAN by assigning authenticated devices to either a data or voice VLAN depending on the VSAs received from the authentication server.

Note When a port is in multiauthentication mode, Guest VLAN and Authentication Failed VLAN will not activate for data devices.

Pre-Authentication Open Access

Beginning with Cisco IOS Release 12.2(50)SG, any of the four host modes can be additionally configured to allow a device to gain network access before authentication. This preauthentication open access is useful in an application such as the Pre-boot eXecution Environment (PXE), where a device must access the network to download a bootable image containing an authentication client.

Enable preauthentication open access by entering the **authentication open** command after host mode configuration. It acts as an extension to the configured host mode. For example, if preauthentication open access is enabled with single-host mode, then the port allows only one MAC address. When preauthentication open access is enabled, initial traffic on the port is restricted only by whatever other access restriction, independent of 802.1X, is configured on the port. If no access restriction other than 802.1X is configured on the port, then a client device has full access on the configured VLAN.

802.1X Violation Mode

You can use the **authentication violation** interface configuration command to configure the violation mode: restrict, shutdown, and replace.

In single-host mode, a security violation is triggered when more than one device are detected on the data vlan. In multidomain authentication mode, a security violation is triggered when more than one device are detected on the data or voice VLAN.

Security violation cannot be triggered in multiple-host mode or multiauthentication mode.

When security violation occurs, the port is protected depending on the configured violation action:

Shutdown—Errdisables the port; the default behavior on a port.

Restrict—The port state is unaffected. However the platform is notified to restrict the traffic from offending MAC-address.

Replace—Replaces existing host with the new host, instead of error-disabling or restricting the port.

For more information see "Configuring Violation Action" section on page 46-55.

Using MAC Move

Hosts should be able to move across ports within a switch on the same or different VLAN without restriction, as if they had moved to a port on another switch.

Prior to Cisco IOS Release 12.2(54)SG, when a MAC address is authenticated on one switch port, that address is not allowed on another 802.1X switch port. If the switch detects that same MAC address on another 802.1X port, the address is not allowed.

Beginning with Cisco IOS Release 12.2(54)SG, you can move a MAC address to another port on the same switch. it is not pertinent for directly connected hosts or for hosts behind Cisco phones, where a port-down event or proxy EAPoL-Logoff/CDP TLV is received when the initial host disconnects. It is pertinent for hosts that disconnect from behind a hub, third party phone, or legacy Cisco phone, causing the session to remain up. With MAC move you can disconnect the host from such a device and connect it directly to another port on the same switch.

You can globally enable MAC move so that the device is reauthenticated on the new port. When a host moves to a second port, the session on the first port is deleted, and the host is reauthenticated on the new port.

MAC move is supported on all host modes. (The authenticated host can move to any port on the switch, for any host mode enabled on that port.)

For more information see "Configuring MAC Move" section on page 46-54.

Using MAC Replace

Beginning with Cisco IOS Release 12.2(54)SG, you can allow new hosts to connect to abandoned ports. If the configured violation action is *replace*, the existing host is replaced by the new host, instead of err-disabling or restricting the port (as happens for single-host and MDA modes).

it is not an issue for directly connected hosts or for hosts behind Cisco phones, where a port-down event or proxy EAPoL-Logoff/CDP TLV is received when the initial host disconnects. It is an issue where a host disconnects from behind a hub, third party phone, or legacy Cisco phone, causing the session to remain up. New hosts connecting to this port violate the host-mode, triggering a violation. When the violation action is *replace*, the NAD (switch) terminates the initial session and resets the authentication sequence based on the new MAC. This applies to single-host and MDA host modes. In multiple- auth mode, no attempt is made to remove an existing session on the same port.

For more information see the "Configuring MAC Replace" section on page 46-54.

Using 802.1X with VLAN Assignment

You can use the VLAN assignment to limit network access for certain users. With the VLAN assignment, 802.1X-authenticated ports are assigned to a VLAN based on the username of the client connected to that port. The RADIUS server database maintains the username-to-VLAN mappings. After successful 802.1X authentication of the port, the RADIUS server sends the VLAN assignment to the switch. The VLAN can be a standard VLAN or a PVLAN.

On platforms that support PVLANs, you can isolate hosts by assigning ports into PVLANs.

When configured on the switch and the RADIUS server, 802.1X with VLAN assignment has these characteristics:

- If no VLAN is supplied by the RADIUS server, the port is configured in its access VLAN or isolated PVLAN when authentication succeeds.
- If the authentication server provides invalid VLAN information, the port remains unauthorized. This situation prevents ports from appearing unexpectedly in an inappropriate VLAN due to a configuration error.
- Starting with Cisco IOS Release 15.0(2)SG, if multi-authentication mode is enabled on an 802.1X port, VLAN Assignment occurs successfully for the first authenticated host. Subsequent authorized (based on user credentials) data hosts, are considered successfully authenticated, provided either they have no VLAN assignment or have a VLAN assignment matching the first successfully authenticated host on the port. This ensures that all successfully authenticated hosts on a port are members of the same VLAN. Flexibility of VLAN assignment is only provided to the first authenticated host.
- If the authentication server provides valid VLAN information, the port is authorized and placed in the specified VLAN when authentication succeeds.
- If the multiple-hosts mode is enabled, all hosts are in the same VLAN as the first authenticated user.
- If 802.1X is disabled on the port, the port is returned to the configured access VLAN.
- A port must be configured as an access port (which can be assigned only into “regular” VLANs), or as a PVLAN host port (which can be assigned only into PVLANs). Configuring a port as a PVLAN host port implies that all hosts on the port are assigned into PVLANs, whether their posture is compliant or non-compliant. If the type of the VLAN named in the Access-Accept does not match the type of VLAN expected to be assigned to the port (regular VLAN to access port, secondary PVLAN to PVLAN host port), the VLAN assignment fails.
- If a guest VLAN is configured to handle non-responsive hosts, the type of VLAN configured as the guest VLAN must match the port type (that is, guest VLANs configured on access ports must be standard VLANs, and guest VLANs configured on PVLAN host ports must be PVLANs). If the guest VLAN’s type does not match the port type, non-responsive hosts are treated as if no guest VLAN is configured (that is, they are denied network access).
- To assign a port into a PVLAN, the named VLAN must be a secondary PVLAN. The switch determines the implied primary VLAN from the locally configured secondary-primary association.

Note If you change the access VLAN or PVLAN host VLAN mapping on a port that is already authorized in a RADIUS assigned VLAN, the port remains in the RADIUS assigned VLAN.

To configure VLAN assignment you need to perform these tasks:

- Enable AAA authorization by using the **network** keyword to allow interface configuration from the RADIUS server. For an illustration of how to apply the **aaa authorization network group radius** command, refer to the section "Enabling 802.1X Authentication" on page 28.
- Enable 802.1X. (The VLAN assignment feature is automatically enabled when you configure 802.1X on an access port.)
- Assign vendor-specific tunnel attributes in the RADIUS server. To ensure proper VLAN assignment, the RADIUS server must return these attributes to the switch:
  - Tunnel-Type = VLAN
  - Tunnel-Medium-Type = 802
  - Tunnel-Private-Group-ID = VLAN NAME

Using 802.1X for Guest VLANs

You can use guest VLANs to enable non-802.1X-capable hosts to access networks that use 802.1X authentication. For example, you can use guest VLANs while you are upgrading your system to support 802.1X authentication.

Guest VLANs are supported on a per-port basis, and you can use any VLAN as a guest VLAN as long as its type matches the type of the port. If a port is already forwarding on the guest VLAN and you enable 802.1X support on the network interface of the host, the port is immediately moved out of the guest VLAN and the authenticator waits for authentication to occur.

Enabling 802.1X authentication on a port starts the 802.1X protocol. If the host fails to respond to packets from the authenticator within a certain amount of time, the authenticator brings the port up in the configured guest VLAN.

If the port is configured as a PVLAN host port, the guest VLAN must be a secondary PVLAN. If the port is configured as an access port, the guest VLAN must be a regular VLAN. If the guest VLAN configured on a port is not appropriate for the type of the port, the switch behaves as if no guest VLAN is configured (that is, non-responsive hosts are denied network access).

For details on how to configure guest VLANs, see the "Configuring 802.1X with Guest VLANs" section on page 46-56.

Usage Guidelines for Using 802.1X Authentication with Guest VLANs

When using 802.1X authentication with guest VLANs, consider these guidelines:

- When you reconfigure a guest VLAN to a different VLAN, any authentication failed ports are also moved and the ports stay in their current authorized state.
- When you shut down or remove a guest VLAN from the VLAN database, any authentication failed ports are immediately moved to an unauthorized state and the authentication process is restarted.

Note No periodic reauthentication is allowed with guest VLANs.

Usage Guidelines for Using 802.1X Authentication with Guest VLANs on Windows-XP Hosts

When using 802.1X authentication with guest VLANs on Windows-XP hosts, consider these guidelines:

- If the host fails to respond to the authenticator, the port attempts to connect three times (with a 30 second timeout between each attempt). After this time, the login/password window does not appear on the host, so you must unplug and reconnect the network interface cable.
- Hosts responding with an incorrect login/password fail authentication. Hosts failing authentication are not put in the guest VLAN. The first time that a host fails authentication, the quiet-period timer starts, and no activity occurs for the duration of the quiet-period timer. When the quiet-period timer expires, the host is presented with the login and password window. If the host fails authentication for the second time, the quiet-period timer starts again, and no activity occurs for the duration of the quiet-period timer. The host is presented with the login and password window a third time. If the host fails authentication the third time, the port is placed in the unauthorized state, and you must disconnect and reconnect the network interface cable.

Using 802.1X with MAC Authentication Bypass

The 802.1X protocol has 3 entities: client (supplicant), authenticator, and authentication server. Typically, the host PC runs the supplicant software and tries to authenticate itself by sending its credentials to the authenticator which in turn relays that info to the authentication server for authentication.

However, not all hosts may have supplicant functionality. Devices that cannot authenticate themselves using 802.1X but still need network access can use MAC Authentication Bypass (MAB), which uses the connecting device's MAC address to grant or deny network access.

Typically, you use this feature on ports where devices such as printers are connected. Such devices do not have 802.1X supplicant functionality.

In a typical deployment, the RADIUS server maintains a database of MAC addresses that require access. When this feature detects a new MAC address on a port, it generates a RADIUS request with both username and password as the device's MAC address. After authorization succeeds, the port is accessible to the particular device using the same code path that 802.1X authentication would take when processing an 802.1X supplicant. If authentication fails, the port moves to the guest VLAN if configured, or it remains unauthorized.

The Catalyst 4500 series switch also supports reauthentication of MACs on a per-port level. Be aware that the reauthentication functionality is provided by 802.1X and is not MAB specific. In the reauthentication mode, a port stays in the previous RADIUS-sent VLAN and tries to re-authenticate itself. If the reauthentication succeeds, the port stays in the RADIUS-sent VLAN. Otherwise, the port becomes unauthorized and moves to the guest VLAN if one is configured.

For details on how to configure MAB, see the "Configuring 802.1X with MAC Authentication Bypass" section on page 46-59.

Feature Interaction

This section lists feature interactions and restrictions when MAB is enabled. If a feature is not listed, assume that it interacts seamlessly with MAB (such as Unidirectional Controlled Port).

- MAB can only be enabled if 802.1X is configured on a port. MAB functions as a fall back mechanism for authorizing MACs. If you configure both MAB and 802.1X on a port, the port attempts to authenticate using 802.1X. If the host fails to respond to EAPOL requests and MAB is configured, the 802.1X port is opened up to listen to packets and to grab a MAC address, rather than attempt to authenticate endlessly.

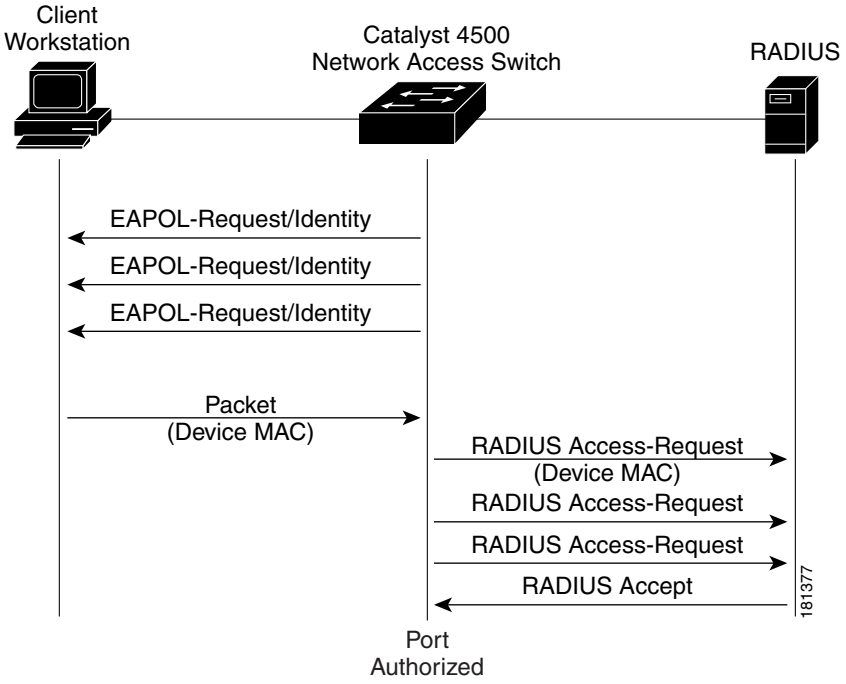
  Based on the default 802.1X timer values, the transition between mechanisms takes approximately 90 seconds. You can shorten the time by reducing the value of the transmission period time, which affects the frequency of EAPOL transmission. A smaller timer value results in sending EAPOLs during a shorter time interval. With MAB enabled, after 802.1X performs one full set of EAPOLs, the learned MAC address is forwarded to the authentication server for processing.

  The MAB module performs authorization for the first MAC address detected on the wire. The port is considered authorized once a valid MAC address is received that RADIUS approves of.

  802.1X authentication can re-start if an EAPOL packet is received on a port that was initially authorized as a result of MAB.

  Figure 46-6 shows the message exchange during MAB.

Figure 46-6 Message Exchange during MAC Authentication Bypass



- The authentication-failed VLAN is used only with dot1x-authentication-failed users. MAB is not attempted with dot1x-authentication-failed users. If 802.1X authentication fails, a port moves to the authentication-failed VLAN (if configured) whether MAB is configured or not.

- When both MAB and guest VLAN are configured and no EAPOL packets are received on a port, the 802.1X state-machine is moved to a MAB state where it opens the port to listen to traffic and grab MAC addresses. The port remains in this state forever waiting to see a MAC on the port. A detected MAC address that fails authorization causes the port to be moved to the guest VLAN if configured.

  While in a guest VLAN, a port is open to all traffic on the specified guest VLAN. Non-802.1X supplicants that normally would be authorized but are in guest VLAN due to the earlier detection of a device that failed authorization, would remain in the guest VLAN indefinitely. However, loss of link or the detection of an EAPOL on the wire causes a transition out of the guest VLAN and back to the default 802.1X mode.
- Catalyst 4500 series switch supports MAB with VVID, with the restriction that the MAC address appears on a port data VLAN only. All IP phone MACs learned using CDP are allowed on voice VLANs.
- MAB and VMPS are mutually exclusive because their functionality overlaps.

Using 802.1X with Web-Based Authentication

The web-based authentication feature, known as Web Authentication Proxy, allows you to authenticate end users on host systems that do not run the IEEE 802.1X supplicant.

When configuring web-based authentication, consider these guidelines:

- Fallback to web-based authentication is configured on switch ports in access mode. Ports in trunk mode are not supported.
- Fallback to web-based authentication is not supported on EtherChannels or EtherChannel members.
- Although fallback to web-based authentication is an interface-specific configuration, the web-based authentication fallback behavior is defined in a global fallback profile. If the global fallback configuration changes, the new profile is not used until the next instance of authentication fallback.

For detailed information on configuring web-based authentication, see Chapter 48, “Configuring Web-Based Authentication.”

Using 802.1X with Inaccessible Authentication Bypass

When a switch cannot reach the configured RADIUS servers and clients (supplicants) cannot be authenticated, you can configure a switch to allow network access to hosts connected to *critical* ports that are enabled for Inaccessible Authentication Bypass.

When Inaccessible Authentication Bypass is enabled, a switch monitors the status of the configured RADIUS servers. If no RADIUS servers are available, clients that fail authentication due to server unavailability are authorized. Inaccessible Authentication Bypass can be enabled for data clients and voice clients. For data clients, you can specify an Inaccessible Authentication Bypass VLAN on a per-port basis. For voice clients they are authorized in the configured voice vlan. Inaccessible Authentication Bypass for voice clients can activate in Multiple Domain Authentication and Multiple Authentication modes, in which authentication is enforced for voice devices.

Note Inaccessible Authentication Bypass allows a voice client to access configured voice VLAN when RADIUS becomes unavailable. For the voice device to operate properly, it must learn the voice VLAN ID through other protocols such as CDP, LLDP, or DHCP, wherever appropriate. When a RADIUS server is unavailable, it may not be possible for a switch to recognize a MAC address as that of a voice device.

Therefore, when Inaccessible Authentication Bypass is configured for voice devices, it should also be configured for data. Voice devices may be authorized on both critical data and voice VLANs. If port security is enabled, this may affect the maximum port security entries enforced on the port.

By default, data clients that were already authorized when RADIUS becomes unavailable are unaffected by Inaccessible Authentication Bypass. To reauthenticate all authorized data clients on the port when RADIUS becomes unavailable, use the **authentication server dead action reinitialize vlan** interface configuration command. This command is intended for multiauthentication mode and is mutually exclusive with the **authentication server dead action authorize vlan** command.

Note In multiauthentication mode, you cannot use the **authentication server dead action authorize vlan** command to enable Inaccessible Authentication Bypass for data clients; it has no effect. Instead, use the **authentication server dead action reinitialize vlan** *vlan-id* command.

When RADIUS becomes available, critically authorized ports can be configured to automatically reauthenticate themselves.

Note To properly detect RADIUS server availability, the **test username** *name* option should be enabled in the **radius-server host** command. For details on how to configure RADIUS server, see the "Configuring Switch-to-RADIUS-Server Communication" section on page 46-31.

Inaccessible Authentication Bypass cannot activate after a port falls back to Web-based authentication. For details on how to configure Web-based authentication, see Chapter 48, "Configuring Web-Based Authentication."

For details on how to configure Inaccessible Authentication Bypass, see Chapter 48, "Configuring Web-Based Authentication".

Using 802.1X with Unidirectional Controlled Port

Unidirectional Controlled Port is a combined hardware and software feature that allows dormant PCs to be powered on based on the receipt of a specific Ethernet frame, known as the *magic packet*. Generally, Unidirectional Controlled Port is used in environments where administrators plan to manage remote systems during off-hours, when the systems usually have been powered down.

Use of Unidirectional Controlled Port with hosts attached through 802.1X ports presents a unique problem: when the host powers down, a 802.1X port becomes unauthorized. In this state, the port allows the receipt and transmission of EAPoL packets only. The Unidirectional Controlled Port magic packet cannot reach the host; without powering up, the PC cannot authenticate and open the port.

Unidirectional Controlled Port solves this problem by allowing packets to be transmitted on unauthorized 802.1X ports.

Note Unidirectional Controlled Port only works when Spanning Tree PortFast is enabled on the port.

For details on how to configure 802.1X with Unidirectional Controlled Port, see the "Configuring 802.1X with Unidirectional Controlled Port" section on page 46-65.

Unidirectional State

A unidirectional controlled port is typically configured when a connected host might enter a sleeping mode or power-down state. When either occurs, the host does not exchange traffic with other devices in the network. A host connected to the unidirectional port cannot send traffic to the network; it can only receive traffic from other devices in the network.

When you configure a port as unidirectional (with the **authentication control-direction in** interface configuration command), the port will receive traffic in VLANs on that port, but it is not put into a spanning-tree forwarding state. If a VLAN contains only unauthenticated ports, any SVI on that VLAN will be in a down state, during which packets will not be routed into the VLAN. For the SVI to be up, and so enable packets to be routed into the VLAN, at least one port in the VLAN must either be authenticated or in the spanning-tree forwarding state.

Bidirectional State

When you configure a port as bidirectional by using the **authentication control-direction both** interface configuration command (or the **dot1x control-direction both** interface configuration command for Cisco IOS Release 12.2(46) or earlier), the port is access-controlled in both directions. In this state, except for EAPOL packets, a switch port does not receive or send packets.

Using 802.1X with VLAN User Distribution

An alternative to dynamically assigning a VLAN ID or a VLAN name is to assign a VLAN group name. The 802.1X VLAN User Distribution feature allows you to distribute users belonging to the same group (and characterized by a common VLAN group name) across multiple VLANs. You usually do this to avoid creating an overly large broadcast domain.

For example, with this feature, you can download a common VLAN group name (similar to ENG-Group, for all the users belonging to the engineering organization) from the authentication server to all the access-layer switches. The VLAN group name is then individually mapped to a different VLAN on each access-layer switch. The same VLAN number need not be spanned across separate switches. Similarly, the VLANs does not need to be renamed at the edge devices.

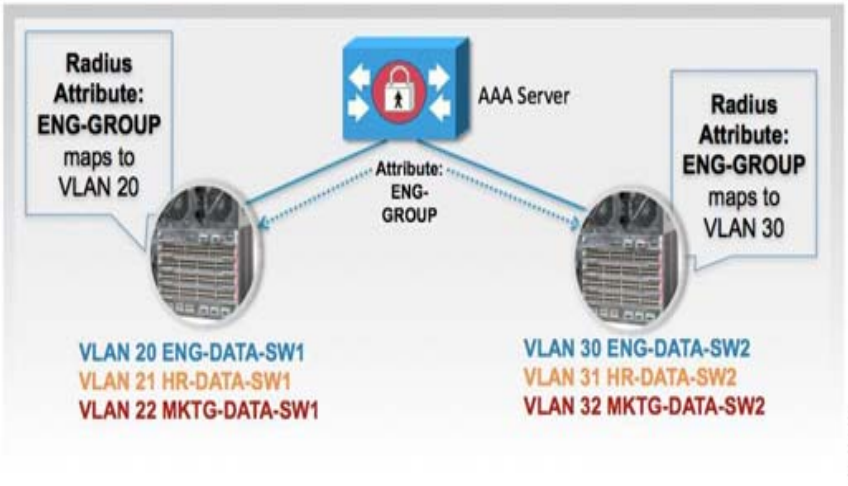
When the authentication server returns more than one VLAN group name or VLANs, this feature attempts to distribute users evenly across those groups. It internally maintains the count of users assigned to each VLAN on that switch by authentication or port security. Based on this information, this feature assigns a newly authenticated user to the least loaded VLAN on that switch among all the VLANs or VLAN group names obtained from the RADIUS server.

This VLAN distribution considers the load of all the valid VLANs only during initial user authentication, and not during reassignment. When some of the existing authenticated users are removed, the feature does not attempt to redistribute the remaining authenticated users. Group distribution does not guarantee perfect load distribution all the time.

Deployment Example

In a large campus LAN design, you might want to design the VLAN infrastructure without large Layer 2 domain. For the same employee VLAN, customers might have different VLANs at different campus access switches. When you deploy 802.1X with VLAN assignment, it does not assign one employee VLAN to all employees. You have to know the real VLANs configured on the switch. User distribution allows you to send a list of VLAN or VLAN group name(s) to the switch. Your switch can then do a local mapping to the corresponding VLAN. (Figure 46-7).

Figure 46-7 802.1X with VLAN User Distribution



For details on how to configure VLAN User Distribution, see the "Configuring 802.1X with VLAN User Distribution" section on page 46-67.

Using 802.1X with Authentication Failed VLAN Assignment

You can use authentication-failed VLAN assignment on a per-port basis to provide access for authentication failed users. Authentication failed users are end hosts that are 802.1X- capable but do not have valid credentials in an authentication server or end hosts that do not give any username and password combination in the authentication pop-up window on the user side.

If a user fails the authentication process, that port is placed in the authentication-failed VLAN. The port remains in the authentication-failed VLAN until the reauthentication timer expires. When the reauthentication timer expires the switch starts sending the port reauthentication requests. If the port fails reauthentication it remains in the authentication-failed VLAN. If the port is successfully reauthenticated, the port is moved either to the VLAN sent by RADIUS server or to the newly authenticated ports configured VLAN; the location depends on whether RADIUS is configured to send VLAN information.

Note When enabling periodic reauthentication (see the "Enabling Periodic Reauthentication" section on page 46-80), only local reauthentication timer values are allowed. You cannot use a RADIUS server to assign the reauthentication timer value.

You can set the maximum number of authentication attempts that the authenticator sends before moving a port into the authentication-failed VLAN. The authenticator keeps a count of the failed authentication attempts for each port. A failed authentication attempt is either an empty response or an EAP failure. The authenticator tracks any mix of failed authentication attempts towards the authentication attempt count. After the maximum number of attempts is reached the port is placed in the authentication-failed VLAN until the reauthentication timer expires again.

Note RADIUS can send a response without an EAP packet in it when it does not support EAP, and sometimes third-party RADIUS servers also send empty responses. When this behavior occurs, the authentication attempt counter is incremented.

For details on how to configure Authentication Failed VLAN Assignment, see the "Configuring 802.1X with Authentication Failed" section on page 46-69.

Usage Guidelines for Using Authentication Failed VLAN Assignment

Usage guidelines include the following:

- You should enable reauthentication. The ports in authentication-failed VLANs do not receive reauthentication attempts if reauthentication is disabled. To start the reauthentication process the authentication-failed VLAN must receive a link-down event or an EAP logoff event from the port. If the host is behind a hub, you may never get a link-down event and may not detect the new host until the next reauthentication occurs.
- EAP failure messages are not sent to the user. If the user failures authentication the port is moved to an authentication-failed VLAN and a EAP success message is sent to the user. Because the user is not notified of the authentication failure there may be confusion as to why there is restricted access to the network. A EAP Success message is sent for the following reasons:
  - If the EAP Success message is not sent, the user tries to authenticate every 60 seconds (by default) by sending an EAP-start message.
  - In some cases, users have configured DHCP to EAP-Success and unless the user sees a success, DHCP does not work on the port.
- Sometimes a user caches an incorrect username and password combination after receiving a EAP success message from the authenticator and reuses that information in every reauthentication. Until the user passes the correct username and password combination the port remains in the authentication-failed VLAN.
- When an authentication failed port is moved to an unauthorized state the authentication process is restarted. If you should fail the authentication process again the authenticator waits in the held state. After you have correctly reauthenticated all 802.1X ports are reinitialized and treated as normal 802.1X ports.
- When you reconfigure an authentication-failed VLAN to a different VLAN, any authentication failed ports are also moved and the ports stay in their current authorized state.
- When you shut down or remove an authentication-failed VLAN from the VLAN database, any authentication failed ports are immediately moved to an unauthorized state and the authentication process is restarted. The authenticator does not wait in a held state because the authentication-failed VLAN configuration still exists. While the authentication-failed VLAN is inactive, all authentication attempts are counted, and as soon as the VLAN becomes active the port is placed in the authentication-failed VLAN.
- If you reconfigure the maximum number of authentication failures allowed by the VLAN, the change takes affect after the reauthentication timer expires.
- Internal VLANs that are used for Layer 3 ports cannot be configured as authentication-failed VLANs.
- The authentication-failed VLAN is supported only in single-host mode (the default port mode).
- When a port is placed in an authentication-failed VLAN the user's MAC address is added to the mac-address-table. If a new MAC address appears on the port, it is treated as a security violation.
- When an authentication failed port is moved to an authentication-failed VLAN, the Catalyst 4500 series switch does not transmit a RADIUS-Account Start Message as it does for standard 802.1X authentication.

Using 802.1X with Port Security

We do not recommend enabling port security when IEEE 802.1x is enabled. IEEE 802.1x enforces a single MAC address per port (or per VLAN when MDA is configured for IP telephony). Therefore port security is redundant and in some cases may interfere with the expected IEEE 802.1x operations.

Using 802.1X Authentication with ACL Assignments and Redirect URLs

Beginning with Cisco IOS Release 12.2(50)SG, you can download per-host policies such as ACLs and redirect URLs to the switch from the RADIUS server during 802.1X or MAB authentication of the host. ACL download is also supported with web authentication after a fallback from 802.1X or MAB.

When the 802.1X host mode of the port is either single-host, MDA, or multiple authentication, the downloaded ACLs (DACLs) are modified to use the authenticated hosts' IP address as the source address. When the host mode is multiple-hosts, the source address is configured as ANY, and the downloaded ACLs or redirects apply to all devices on the port.

If no ACLs are provided during the authentication of a host, the static default ACL configured on the port is applied to the host. On a voice VLAN port, only the static default ACL of the port is applied to the phone.

This section includes these topics:

For details on how to configure downloadable ACL and URL redirect, refer to the "Configuring 802.1X Authentication with ACL Assignments and Redirect URLs" section on page 46-37.

Cisco Secure ACS and AV Pairs for URL-Redirect

When downloadable ACL is enabled, Cisco Secure ACS provides AAA services through RADIUS.

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

- CiscoSecure-Defined-ACL specifies the names of the DACLs on the Cisco Secure ACS. The switch receives the ACL name using the CiscoSecure-Defined-ACL AV pair in the format:

  #ACL#-IP-*name-number*

  name is the ACL name and *number* is the version number (similar to 3f783768).

  The Auth-Manager code verifies whether the access control entries (ACEs) of the specified downloadable ACL were previously downloaded. If not, the Auth-Manager code sends an AAA request with the downloadable ACL name as the username so that the ACEs are downloaded. The downloadable ACL is then created as a named ACL on the switch. This ACL has ACEs with a source address of any and does not have an implicit deny statement at the end. When the downloadable ACL is applied to an interface after authentication completes, the source address changes from any to the host source IP address depending on the host mode of the interface. The ACEs are prepended to the downloadable ACL applied to the switch interface to which the endpoint device is connected. If traffic matches the CiscoSecure-Defined-ACL ACEs, the appropriate actions are taken.
- url-redirect and url-redirect-acl specify the local URL policy on the switch. The switches use these cisco-av-pair VSAs as follows:

- url-redirect = <HTTP or HTTPS URL>
- url-redirect-acl = switch ACL name or number

These AV pairs enable the switch to intercept an HTTP or HTTPS request from the endpoint device and forward the client web browser to the specified redirect address from which the latest antivirus files can be downloaded. The url-redirect AV pair on the Cisco Secure ACS contains the URL to which the web browser is redirected. The url-redirect-acl AV pair contains the name or number of an ACL that specifies the HTTP or HTTPS traffic to be redirected. Traffic that matches a permit entry in the redirect ACL is redirected.

Note The redirect or default ACL must be defined on the switch.

When redirect ACLs are used, we recommend that you configure a dynamic ACL that has an explicit permit statement for the IP address to which the traffic should be redirected.

ACLs

If downloadable ACL is configured for a particular client on the authentication server, you must configure a default port ACL on a client-facing switch port.

If the default ACL is configured on the switch and the Cisco Secure ACS sends a host access policy to the switch, it applies the policy to traffic from the host connected to a switch port. If the policy does not apply, the switch applies the default ACL. If the Cisco Secure ACS sends the switch a downloadable ACL, this ACL takes precedence over the default ACL already configured on the switch port. However, if the switch receives a host access policy from the Cisco Secure ACS, but the default ACL is not configured, the authorization failure is declared.

For details on how to configure a downloadable policy, refer to the "Configuring a Downloadable Policy" section on page 46-43.

Using 802.1X with RADIUS-Provided Session Timeouts

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

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

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

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

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

For details on how to configure RADIUS-provided session timeouts, see the "Configuring RADIUS-Provided Session Timeouts" section on page 46-52.

Using 802.1X with Voice VLAN Ports

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

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

Each port that you configure for a voice VLAN is associated with a VVID and a PVID. This configuration allows voice traffic and data traffic to be separated onto different VLANs.

A voice VLAN port becomes active when a link exists whether the port is AUTHORIZED or UNAUTHORIZED. All traffic exiting the voice VLAN is obtained correctly and appears in the MAC address table. Cisco IP phones do not relay CDP messages from other devices. If several Cisco IP phones are connected in a series, the switch recognizes only the one directly connected to it. When 802.1X is enabled on a voice VLAN port, the switch drops packets from unrecognized Cisco IP phones more than one hop away.

When 802.1X is enabled on a port, you cannot configure a PVID that is equal to a VVID. For more information about voice VLANs, see Chapter 43, "Configuring Voice Interfaces."

Observe the following feature interactions:

- 802.1X VLAN assignment cannot assign to the port the same VLAN as the voice VLAN; otherwise, the 802.1X authentication fails. The same holds true for dynamic VLAN assignment.
- 802.1X guest VLAN works with the 802.1X voice VLAN port feature. However, the guest VLAN cannot be the same as the voice VLAN.
- You cannot use the 802.1X voice VLAN port feature with 802.1X port security's sticky MAC address configuration and statically configured MAC address configuration.
- 802.1X accounting is unaffected by the 802.1X voice VLAN port feature.
- When 802.1X is configured on a port, you cannot connect multiple IP phones to a Catalyst 4500 series switch through a hub.
- Because voice VLANs cannot be configured as PVLAN host ports, and because only PVLANs can be assigned to PVLAN host ports, VLAN assignment cannot assign a PVLAN to a port with a voice VLAN configured.

For details on how to configure 802.1X with voice VLANs, see the "Configuring 802.1X with Voice VLAN" section on page 46-71.

Using Voice Aware 802.1x Security

You use the voice aware 802.1x security feature to configure the switch to disable only the VLAN on which a security violation occurs, whether it is a data or voice VLAN. In previous releases, when an attempt to authenticate the data client caused a security violation, the entire port shut down, resulting in a complete loss of connectivity.

You can use this feature in IP phone deployments where a PC is connected to the IP phone. A security violation found on the data VLAN results in the shutdown of only the data VLAN. The traffic on the voice VLAN flows through the switch without interruption.

For information on configuring voice aware 802.1x security, see the "Configuring Voice Aware 802.1x Security" section on page 46-72

Using Multiple Domain Authentication and Multiple Authentication

Multiple Domain Authentication (MDA) allows both a data device and a voice device, such as an IP phone (Cisco or third party non-Cisco), to authenticate on the same switch port, which is divided into a data domain and a voice domain.

Multi Auth allows multiple data devices and a voice device. When a voice VLAN is configured on a multiple- authentication port, the port can perform authentication in the voice domain as on an MDA port.

MDA does not enforce the order of device authentication. For best results, however, you should authenticate a voice device before you authenticate a data device on an MDA-enabled port.

When configuring MDA, consider the following guidelines.

Note The same guidelines also apply for Multiple Authentication when voice VLAN is configured.

- We recommend that you enable CoPP on an MDA-enabled port to protect against a DoS attack. Refer to Chapter 52, "Configuring Control Plane Policing and Layer 2 Control Packet QoS."
- To configure a switch port for MDA or Multiple Authentication, see the "Configuring Multiple Domain Authentication and Multiple Authorization" section on page 46-33.
- You must configure the voice VLAN for the IP phone when the host mode is set to multidomain. For more information, see Chapter 43, "Configuring Voice Interfaces."
- To authorize a voice device, the AAA server must be configured to send a Cisco Attribute-Value (AV) pair attribute with a value of device-traffic-class=voice. Without this value, the switch treats the voice device as a data device.
- You must configure the attribute device-traffic-class=voice on all authenticated phones. If not configured, authenticated phones may not work correctly.
- The guest VLAN and restricted VLAN features only apply to the data devices on an MDA-enabled port. The switch treats a voice device that fails authorization as a data device.
- If more than one device attempts authorization on either the voice or the data domain of a port, it is error-disabled.
- Until a device is authorized, the port drops its traffic. Non-Cisco IP phones or voice devices are allowed into both the data and voice VLANs. The data VLAN allows the voice device to contact a DHCP server to obtain an IP address and acquire the voice VLAN information. After the voice device starts sending on the voice VLAN, its access to the data VLAN is blocked. A security violation may occur in MDA if the voice device continues to send traffic on the data VLAN.
- MDA can use MAC authentication bypass as a fallback mechanism to allow the switch port to connect to devices that do not support 802.1X authentication. it is especially useful for third party phones without 802.1X supplicant. For more information, see the "Using 802.1X with MAC Authentication Bypass" section on page 46-12.
- When a data or a **voice** device is detected on a port, its MAC address is blocked until authorization succeeds. If the authorization fails, the MAC address remains blocked for 5 minutes.
- If more than one device is detected on the data VLAN or more than one voice device is detected on the voice VLAN while a port is unauthorized, the port is error-disabled.

- When a port host mode is changed from single- or multihost to multidomain mode, an authorized data device remains authorized on the port. However, a Cisco IP phone that was allowed on the port in the voice VLAN is automatically removed and must be reauthenticated on that port.
- Active fallback mechanisms such as guest VLAN and restricted VLAN remain configured after a port changes from single- or multihost mode to multidomain mode.
- Switching a port host mode from multidomain to single- or multihost mode removes all authorized devices from the port.
- If a data domain is authorized first and placed in the guest VLAN, non-802.1X-capable voice devices need to tag their packets on the voice VLAN to trigger authentication.
- We do not recommend per-user ACLs with an MDA-enabled port. An authorized device with a per-user ACL policy might impact traffic on both the voice and data VLANs of the port. If used, only one device on the port should enforce per-user ACLs.

Note Multi-Authentication per user VLAN is not supported on Catalyst 4500 Series Switch.

802.1X Supplicant and Authenticator Switches with Network Edge Access Topology

The Network Edge Access Topology (NEAT) feature extends identity to areas outside the wiring closet (such as conference rooms).

You can enable any authentication host mode on the authenticator switch interface that connects to a supplicant switch. Once the supplicant switch authenticates successfully, the port mode changes from access to trunk. To ensure that NEAT works on all host modes, use the **dot1x supplicant force-multicast** global configuration command on the supplicant switch. If the access VLAN is configured on the authenticator switch, it becomes the native VLAN for the trunk port after successful authentication.

Note MAB is not supported or recommended for use with NEAT. Only use 802.1X to authenticate the supplicant switch.

Note The Catalyst 4500 series switch only supports authenticator ports.

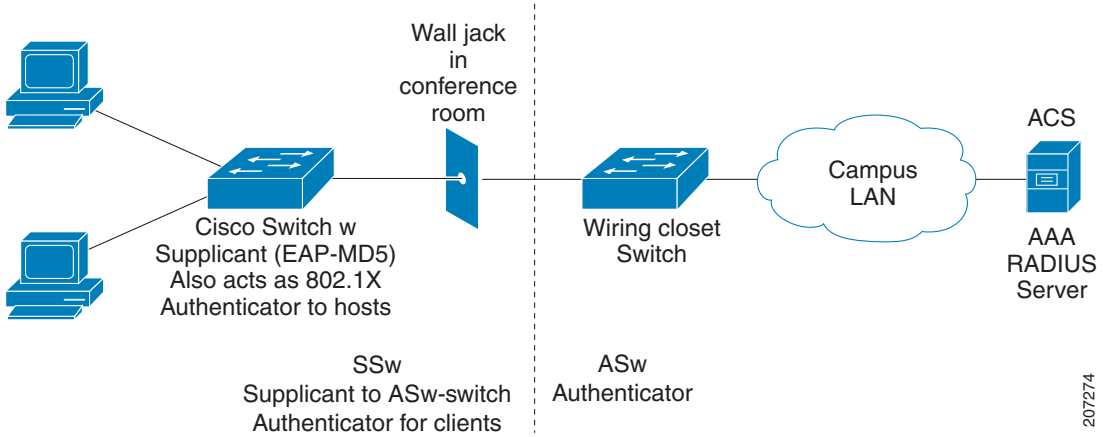
Deployment

NEAT is intended for deployment scenarios where a switch acting as 802.1X authenticator to end-hosts (PC or Cisco IP-phones) is placed in an unsecured location (outside wiring closet).

Because of this topology, the authenticator switch cannot always be trusted. For example, compact switches (8-port Catalyst 3560 and Catalyst 2960) are generally deployed outside the wiring closet. This enables hacker devices to swamp them to gain access to the network, compromising security. An edge switch must be able to authenticate itself against another switch, referred to as Network Edge Authentication Topology (NEAT).

Figure 46-8 illustrates a typical NEAT topology.

Figure 46-8 Typical NEAT Topology



NEAT facilitates the following functionality in such scenarios:

Host Authorization— Ensures that only traffic from authorized hosts (connecting to the switch with a supplicant) is allowed on the network. The switches use Client Information Signalling Protocol (CISP) to send the MAC addresses connecting the supplicant switch to the authenticator switch.

Auto enablement—Automatically enables trunk configuration on the authenticator switch, allowing user traffic from multiple VLANs arising from supplicant switches. At the ACS, you must configure the Cisco AV pair as device-traffic-class=switch. For details on how to do this, see the "Configuring an Authenticator and a Supplicant Switch with NEAT" section on page 46-86.

How 802.1X Fails on a Port

802.1X may fail on a port in three ways: timeout, explicit failure, and protocol timeout.

Timeout—A switch attempts 802.1X at link up but the attached endpoint is not 802.1X-capable. After the configured number of retries and timeouts, the switch attempts the next authentication method if one is configured (like MAB). If MAB fails, the switch deploys the Guest VLAN (also called the no-response VLAN), if configured. The Guest VLAN is configured with the **authentication event no-response** interface command.

Explicit Failure—A switch and the endpoint perform the entire 802.1X authentication sequence and the result is an explicit failure (usually indicated by an Access-Reject from the RADIUS server to the switch and an EAP-Failure sent from the switch to the endpoint). In this case, the switch attempts MAB (if "authentication event failure action next-method" is configured) or deploy the AuthFail VLAN (if "authentication event failure action authorize vlan" is configured).

Protocol Timeout—A switch and the endpoint start the 802.1X authentication process but do not complete it. For example, the endpoint may send an 802.1X EAPoL-Start message and then stop responding to the switch (perhaps, because the endpoint lacks a credential or because it is waiting for end user to enter some information). In this case, the switch knows that the connected device is EAPoL-capable, so it will not deploy the Guest VLAN after timing out. Instead, it restarts authentication after a timeout. The switch continues to label the port as EAPoL-capable until a physical link down event is detected. To force the switch to deploy the Guest VLAN in the case of a protocol timeout, configure **dot1x guest-vlan supplicant** globally. If the port is configured for hostmode multi-domain authentication, the switch behaves as if **dot1x guest-vlan supplicant** is configured.

Supported Topologies

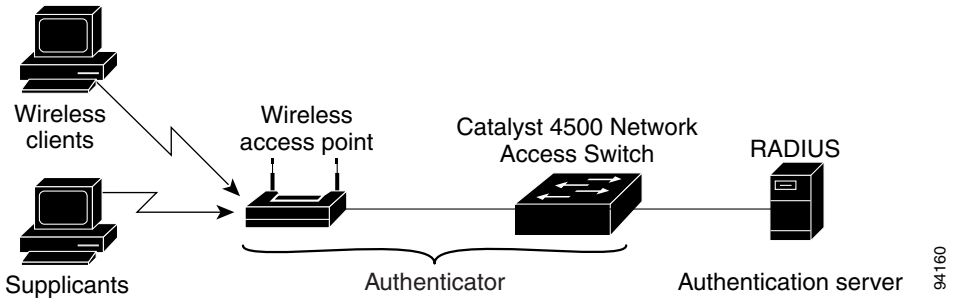
The 802.1X port-based authentication supports two topologies:

- Point-to-point
- Wireless LAN

In a point-to-point configuration (see Figure 46-1 on page 46-3), only one client can be connected to the 802.1X-enabled switch port when the multiple- host mode is not enabled (the default). The switch detects the client when the port link state changes to the up state. If a client leaves or is replaced with another client, the switch changes the port link state to down, and the port returns to the unauthorized state.

For 802.1X port-based authentication in a wireless LAN (Figure 46-9), you must configure the 802.1X port as a multiple-host port that is authorized as a wireless access point once the client is authenticated. (See the "Resetting the 802.1X Configuration to the Default Values" section on page 46-93.) When the port is authorized, all other hosts that are indirectly attached to the port are granted access to the network. If the port becomes unauthorized (reauthentication fails or an EAPOL-logoff message is received), the switch denies access to the network for all wireless access point-attached clients. In this topology, the wireless access point is responsible for authenticating clients attached to it, and the wireless access point acts as a client to the switch.

Figure 46-9 Wireless LAN Example



Configuring 802.1X Port-Based Authentication

To configure 802.1X, follow this procedure:

Step 1 Enable 802.1X authentication. See the "Enabling 802.1X Authentication" section on page 46-28.

Step 2 Configure switch to RADIUS server communication. See the "Configuring Switch-to-RADIUS-Server Communication" section on page 46-31.

Step 3 Adjust the 802.1X timer values. See the "Changing the Quiet Period" section on page 46-83.

Step 4 Configure optional features. See the "Configuring RADIUS-Provided Session Timeouts" section on page 46-52.

These sections describe how to configure 802.1X:

Default 802.1X Configuration

Table 46-1 shows the default 802.1X configuration.

Table 46-1 Default 802.1X Configuration

Feature	Default Setting
Authentication, authorization, and accounting (AAA)	Disabled
RADIUS server • IP address • UDP authentication port • Key	 • None specified • 1645 • None specified
Per-interface 802.1X protocol enable state	Force-authorized The port transmits and receives normal traffic without 802.1X-based authentication of the client.
Periodic reauthentication	Disabled
Time between reauthentication attempts	3600 sec
Quiet period	60 sec Number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.
Retransmission time	30 sec Number of seconds that the switch should wait for a response to an EAP request/identity frame from the client before retransmitting the request.
Maximum retransmission number	2 Number of times that the switch sends an EAP-request/identity frame before restarting the authentication process.
Multiple host support	Disabled
Client timeout period	30 sec When relaying a request from the authentication server to the client, the amount of time that the switch waits for a response before retransmitting the request to the client.
Authentication server timeout period	30 sec When relaying a response from the client to the authentication server, the amount of time that the switch waits for a reply before retransmitting the response to the server. This setting is not configurable.

802.1X Configuration Guidelines

Guidelines for configuring 802.1X authentication include the following:

- The 802.1X protocol is supported only on Layer 2 static access, PVLAN host ports, and Layer 3 routed ports. You cannot configure 802.1X for any other port modes.
- If you are planning to use VLAN assignment, be aware that the features use general AAA commands. For information on how to configure AAA, refer to the "Enabling 802.1X Authentication" section on page 46-28. Alternatively, you can refer to the Cisco IOS security documentation at this location:

  http://www.cisco.com/en/US/products/ps6586/products_ios_technology_home.html

Enabling 802.1X Authentication

To enable 802.1X port-based authentication, you first must enable 802.1X globally on your switch, then enable AAA and specify the authentication method list. A method list describes the sequence and authentication methods that must be queried to authenticate a user.

The software uses the first method listed in the method list to authenticate users; if that method fails to respond, the software selects the next authentication method in the list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle, the authentication process stops, and no other authentication methods are attempted.

Note To allow VLAN assignment, you must enable AAA authorization to configure the switch for all network-related service requests.

To configure 802.1X port-based authentication, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# dot1x system-auth-control`	Enables 802.1X on your switch. To disable 802.1X globally on the switch, use the **no dot1x system-auth-control** command.
Step 3	`Switch(config)# aaa new-model`	Enables AAA. To disable AAA, use the **no aaa new-model** command.

	Command	Purpose
Step 4	`Switch(config)# aaa authentication dot1x {default} method1 [method2...]`	Creates an 802.1X AAA authentication method list. To create a default list that is used when a named list is not specified in the **authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. Enter at least one of these keywords: • **group radius**—Use the list of all RADIUS servers for authentication. • **none**—Use no authentication. The client is automatically authenticated by the switch without using the information supplied by the client. To disable 802.1X AAA authentication, use the **no aaa authentication dot1x** {**default** | *list-name*} *method1* [*method2*...] global configuration command.
Step 5	`Switch(config)# aaa authorization network {default} group radius`	(Optional) Configures the switch for user RADIUS authorization for all network-related service requests, such as VLAN assignment.
Step 6	`Switch(config)# interface interface-id`	Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.
Step 7	`Switch(config-if)# switchport mode access`	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
Step 8	`Switch(config-if)# dot1x pae authenticator`	Enables 802.1X authentication on the port with default parameters. Refer to the "Default 802.1X Configuration" section on page 46-26.

Step 9	Cisco IOS Release 12.2(50)SG and later
	`Switch(config-if)# authentication port-control auto`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x port-control auto`
		Enables 802.1X authentication on the interface.

Step 10	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 11	`Switch # show dot1x interface interface-id details`	Verifies your entries. Check the PortControl row in the 802.1X port summary section of this display. The PortControl value is set to **auto**.
Step 12	`Switch# show running-config`	Verifies your entries.
Step 13	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Note Enabling Spanning Tree PortFast ensures that a port comes up immediately after authorization.

Note Whenever you configure any 802.1X parameter on a port, a dot1x authenticator is automatically created on the port. As a result, **dot1x pae authenticator** appears in the configuration, ensuring that dot1x authentication still works on legacy configurations without manual intervention.

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

Cisco IOS Release 12.2(50)SG and later

```
Switch# configure terminal
Switch(config)# dot1x system-auth-control
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# interface fastethernet2/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication port-control auto
Switch(config-if)# end

Switch# show authentication sessions interface f9/2
            Interface:  FastEthernet9/2
          MAC Address:  0007.e95d.83c4
           IP Address:  Unknown
               Status:  Running
               Domain:  UNKNOWN
       Oper host mode:  single-host
     Oper control dir:  both
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A050B160000009505106398
      Acct Session ID:  0x0000009B
               Handle:  0x0D000095

Runnable methods list:
       Method   State
       dot1x    Running
       mab      Not run
```

Cisco IOS Release 12.2(46)SG or earlier

```
Switch# configure terminal
Switch(config)# dot1x system-auth-control
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# interface fastethernet2/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end

Switch# show dot1x interface f9/2 details

Dot1x Info for FastEthernet9/2
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

```
Dot1x Authenticator Client List
-------------------------------
Supplicant                = 0007.e95d.83c4
Session ID                = 0A050B160000009505106398
    Auth SM State         = AUTHENTICATING
    Auth BEND SM State    = REQUEST
Port Status               = UNAUTHORIZED
```

The following example illustrates when a port is authorized:

```
Switch# show authentication sessions int G4/5
           Interface:  GigabitEthernet4/5
         MAC Address:  0015.e981.0531
          IP Address:  Unknown
           User-Name:  ctssxp
              Status:  Authz Success
              Domain:  DATA
      Oper host mode:  single-host
     Oper control dir:  both
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A053F0F00000004041E6B0C
      Acct Session ID:  0x00000021
              Handle:  0x2C000004

Runnable methods list:
       Method   State
       dot1x    Authc Success

Switch# show dot1x interface G4/5 details

Dot1x Info for GigabitEthernet4/5
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Dot1x Authenticator Client List
-------------------------------
Supplicant                = 0015.e981.0531
Session ID                = 0A053F0F00000004041E6B0C
    Auth SM State         = AUTHENTICATED
    Auth BEND SM State    = IDLE
Port Status               = AUTHORIZED
```

Configuring Switch-to-RADIUS-Server Communication

A RADIUS security server is identified by its host name or IP address, host name and specific UDP port number, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, which enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service (for example, authentication), the second host entry configured acts as the failover backup to the first one. The RADIUS host entries are tried in the order they were configured.

To configure the RADIUS server parameters on the switch, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# radius-server host {hostname | ip-address} auth-port port-number [acct-port port-number] [test username name] [ignore-auth-port] [ignore-acct-port] [idle-time min] key string`	Configures the RADIUS server parameters on the switch. For *hostname* | *ip-address,* specify the hostname or IP address of the remote RADIUS server. To delete the specified RADIUS server, use the **no radius-server host** {*hostname* | *ip-address*} global configuration command. **auth-port** *port-number*—Specifies the UDP destination port for authentication requests. The default is 1645. **acct-port** *port-number*—Specifies the UDP destination port for accounting requests. The default is 1646. Use **test username** *name* to enable automated RADIUS server testing, and to detect the RADIUS server going up and down. The **name** parameter is the username used in the test access request sent to the RADIUS server; it does not need to be a valid user configured on the server. The **ignore-auth-port** and **ignore-acct-port** options disable testing on the authentication and accounting ports respectively. The **idle-time** *min* parameter specifies the number of minutes before an idle RADIUS server is tested to verify that it is still up. The default is 60 minutes. The **key** *string* specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server. **Note** Always configure the key as the last item in the **radius-server host** command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon. If you want to use multiple RADIUS servers, use this command multiple times.
Step 3	`Switch(config)# radius-server deadtime min`	(Optional) Configures the number of minutes before a dead RADIUS server is tested to check whether it has come back up. The default is 1 minute.
Step 4	`Switch(config)# radius-server dead-criteria time seconds tries num`	(Optional) Configures the criteria used to decide whether a RADIUS server is dead. The **time** parameter specifies the number of seconds after which a request to the server is unanswered before it is considered dead. The **tries** parameter specifies the number of times a request to the server is unanswered before it is considered dead. The recommended values for these parameters are **tries** equal to **radius-server retransmit** and **time** equal to **radius-server retransmit** x **radius-server timeout**.

	Command	Purpose
Step 5	`Switch(config)# ip radius source-interface m/p`	Establishes the IP address to be used as the source address for all outgoing RADIUS packets.
Step 6	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	`Switch# show running-config`	Verifies your entries.
Step 8	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

This example shows how to specify the server with IP address 172.120.39.46 as the RADIUS server. The first command specifies port 1612 as the authorization port, sets the encryption key to rad123.

The second command dictates that key matches are performed on the RADIUS server:

```
Switch# configure terminal
Switch(config)# radius-server host 172.120.39.46 auth-port 1612 key rad123
Switch(config)# ip radius source-interface g3/2
Switch(config)# end
Switch#
```

You can globally configure the timeout, retransmission, and encryption key values for all RADIUS servers by using the **radius-server host** global configuration command. If you want to configure these options on a per-server basis, use the **radius-server timeout**, **radius-server retransmit**, and the **radius-server key** global configuration commands.

You also need to create a AAA client setting on the RADIUS server. These settings include the IP address of the switch and the key string to be shared by both the server and the switch.

Configuring Multiple Domain Authentication and Multiple Authorization

Note Multiple Authorization requires Cisco IOS Release 12.2(50)SG and later releases.

To configure Multiple Domain Authentication (MDA) and Multiple Authorization, perform this task.

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# radius-server vsa send authentication`	Configures the network access server to recognize and use vendor-specific attributes (VSAs).
Step 3	`Switch(config)# interface` *`interface-id`*	Specifies the port to which multiple hosts are indirectly attached, and enters interface configuration mode.

	Command	Purpose

Step 4	Cisco IOS Release 12.2(50)SG and later
	`Switch(config-if)# [no] authentication host-mode {single-host | multi-host | multi-domain} | multi-auth}`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# [no] dot1x host-mode {single-host | multi-host | multi-domain}`
		The keywords allow the following:
		• **single-host—**Single-host (client) on an IEEE 802.1X-authorized port.
		• **multi-host**—Multiple-hosts on an 802.1X-authorized port after a authenticating a single host.
		• **multi-domain—**Both a host and a voice device (such as an IP phone, Cisco or non-Cisco), to authenticate on an IEEE 802.1X-authorized port.
		Note You must configure a voice VLAN for an IP phone when the host mode is set to **multi-domain**. For more information, see Chapter 43, "Configuring Voice Interfaces."
		• **multi-auth—**Allows multiple hosts and a voice device, such as an IP phone (Cisco or non-Cisco), to be authenticated on an IEEE 802.1x-authorized port. This keyword requires Cisco IOS Release 12.2(50)SG or a later release.
		Ensure that the **dot1x port-control** interface configuration command is set to **auto** for the specified interface.
		To disable multiple hosts on the port, use the **no authentication host-mode {multi-host | multi-domain | multi-auth}** interface configuration command (for earlier releases, use the **no dot1x host-mode** {**multi-host | multi-domain**} interface configuration command).

Step 5	`Switch(config-if)# switchport voice vlan` *vlan-id*	(Optional) Configures the voice VLAN.
Step 6	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 7	`Switch# show dot1x interface` *interface-id* `[detail]`	Verifies your entries.
Step 8	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

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

Cisco IOS Release 12.2(50)SG and later

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

Cisco IOS Release 12.2(46)SG or earlier

```
Switch(config)# interface gigabitethernet2/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
Switch(config-if)# end
```

This example shows how to enable MDA and to allow both a host and a 802.1X voice device (a Cisco or third-party phone with 802.1X supplicant) on the port:

Cisco IOS Release 12.2(50)SG and later

```
Switch# conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface FastEthernet3/1
Switch(config-if)# shut
Switch(config-if)# switchport access vlan 12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 10
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication host-mode multi-domain
Switch(config-if)# no shut
Switch(config-if)# end
```

Cisco IOS Release 12.2(46)SG or earlier

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface FastEthernet3/1
Switch(config-if)# shut
Switch(config-if)# switchport access vlan 12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 10
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
Switch(config-if)# no shut
Switch(config-if)# end
```

This example shows how to enable MDA and to allow both a host and a non-802.1X voice device on the port:

Cisco IOS Release 12.2(50)SG and later

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface FastEthernet3/1
Switch(config-if)# shut
Switch(config-if)# switchport access vlan 12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 10
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication host-mode multi-domain
Switch(config-if)# mab eap
Switch(config-if)# no shut
Switch(config-if)# end
```

Cisco IOS Release 12.2(46)SG or earlier

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface FastEthernet3/1
Switch(config-if)# shut
Switch(config-if)# switchport access vlan 12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 10
Switch(config-if)# dot1x pae authenticator
```

```
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
Switch(config-if)# dot1x mac-auth-bypass
Switch(config-if)# no shut
Switch(config-if)# end
```

This example shows how to verify the dot1x MDA settings on interface FastEthernet3/1:

```
Switch# show dot1x interface FastEthernet3/1 detail

Dot1x Info for FastEthernet3/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_DOMAIN
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0

Dot1x Authenticator Client List
-------------------------------
Domain                    = DATA
Supplicant                = 0000.0000.ab01
        Auth SM State     = AUTHENTICATED
        Auth BEND SM Stat = IDLE
Port Status               = AUTHORIZED
Authentication Method     = Dot1x
Authorized By             = Authentication Server
Vlan Policy               = 12

Domain                    = VOICE
Supplicant                = 0060.b057.4687
        Auth SM State     = AUTHENTICATED
        Auth BEND SM Stat = IDLE
Port Status               = AUTHORIZED
Authentication Method     = Dot1x
Authorized By             = Authentication Server

Switch#
```

This example shows how to enable MDA and to authentication of multiple hosts and a voice device on an IEEE 802.1x-authorized port:

Note This example applies to Cisco IOS Release 12.2(50)SG and later releases.

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface FastEthernet3/1
Switch(config-if)# shut
Switch(config-if)# switchport access vlan 12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 10
Switch(config-if)# dot1x pae authenticator
```

```
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication host-mode multi-auth
Switch(config-if)# map eap
Switch(config-if)# no shut
Switch(config-if)# end
```

Configuring 802.1X Authentication with ACL Assignments and Redirect URLs

This section includes these topics:

Downloadable ACL

The downloadable ACL (DACL) feature allows you to download device specific authorization policies from the authentication server. These policies activate after authentication succeeds for the respective client and the client's IP address was populated in the IP device tracking table. (Downloadable ACL is applied on the port, once the port is authenticated and the IP device tracking table has the host IP address entry).

The following sections describe the configuration that is necessary to complement the related authentication (802.1X or MAB) configuration. (No unique configuration is required on the switch. All of the configuration is on the ACS.) After authentication succeeds, enter the **show ip access-list** command to display the downloadable ACLs.

Configuring the Switch for Downloadable ACL

To configure the switch for downloadable ACL, follow these steps:

Step 1 Configure the IP device tracking table.

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

Step 2 Configure RADIUS VSA to forward authentication.

```
Switch(config)# radius-server vsa send authentication
```

Step 3 Configure static ACL for the interface.

```
Switch(config)# int g2/9
Switch(config-if)# ip access-group pacl-4 in
```

Interface Configuration Example

```
Switch# show running-configuration interface g2/9
Building configuration...

Current configuration : 617 bytes
!
interface GigabitEthernet2/9
 switchport
 switchport access vlan 29
 switchport mode access
```

```
 switchport voice vlan 1234
 access-group mode prefer port
 ip access-group pacl-4 in
 speed 100
 duplex full
 authentication event fail action authorize vlan 111
 authentication event server dead action authorize vlan 333
 authentication event server alive action reinitialize
 authentication host-mode multi-auth
 authentication order dot1x
 authentication port-control auto
 authentication timer restart 100
 authentication timer reauthenticate 20
 authentication timer inactivity 200
 mab eap
 dot1x pae authenticator
end

Switch#
Switch# show ip access-list pacl-4
    10 permit ip host 1.1.1.1 host 2.2.2.2
    20 permit icmp host 1.1.1.1 host 2.2.2.2
Switch#
```

Debug Commands for DACL

The IP device tracking table contains the host IP address learned through ARP or DHCP.

The following command displays the constraints on the IP device tracking table:

```
Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------
  IP Address     MAC Address       Interface          STATE
-----------------------------------------------------------------
50.0.0.12       0015.60a4.5e84 GigabitEthernet2/9     ACTIVE
```

The following **show authentication sessions** command displays the authentication sessions that contains the downloadable ACL obtained from ACS:

Note The **show epm** command will be deprecated, displaying a warning message when used. Use the **show authentication sessions** command instead.

```
Switch-2033# show authentication sessions interface g2/9 details
            Interface:  GigabitEthernet2/9
          MAC Address:  2c54.2d6a.0345
         IPv6 Address:  Unknown
         IPv4 Address:  8.8.8.11
            User-Name:  2C-54-2D-6A-03-45
               Status:  Authorized
               Domain:  DATA
      Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  0404040400000610081AA183
      Acct Session ID:  0x000006F2
               Handle:  0x760005B9
       Current Policy:  POLICY_Gi2/9
```

```
Server Policies:
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51de4498

Method status list:
       Method           State
       mab              Authc Success
```

The **show authentication sessions interface** *interface-name* **policy** displays session information in the form of Local Policies(features defined locally on the box), Server policies(features downloaded from radius) and Resultant Policies(the one with higher precedence when both local and server policies are present). By default, server policies have higher precedence than those defined locally.

```
AUTH# show authentication sessions interface e0/0 policy
            Interface:  Ethernet0/0
          MAC Address:  aabb.cc01.ff00
         IPv6 Address:  Unknown
         IPv4 Address:  Unknown
            User-Name:  gupn
               Status:  Authorized
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-host
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  0D0102330000000D0003329A
      Acct Session ID:  Unknown
               Handle:  0x6F000002
       Current Policy:  POLICY_Et0/0

Local Policies:
        Template: SVC_1 (priority 10)
         Idle timeout:  500 sec
                  TAG:  blue
         URL Redirect:  www.a.com
     URL Redirect ACL:  a

        Template: SVC_3 (priority 20)
         Idle timeout:  300 sec
                  TAG:  red
         URL_Redirect:  www.b.com
     URL-Redirect ACL:  b

Server Policies:
         Idle timeout:  800 sec


Resultant policies:
         Idle timeout:  500 sec
                  TAG:  blue
         URL Redirect:  www.a.com
     URL Redirect ACL:  a
                  TAG:  red

Method status list:
       Method           State
       dot1x            Authc Success
```

The following command displays the contents of the downloadable ACL:

```
Switch# show ip access-lists xACSACLx-IP-auth-48b79b6e
Extended IP access list xACSACLx-IP-auth-48b79b6e (per-user)
    10 permit udp any any
Switch(config)#
```

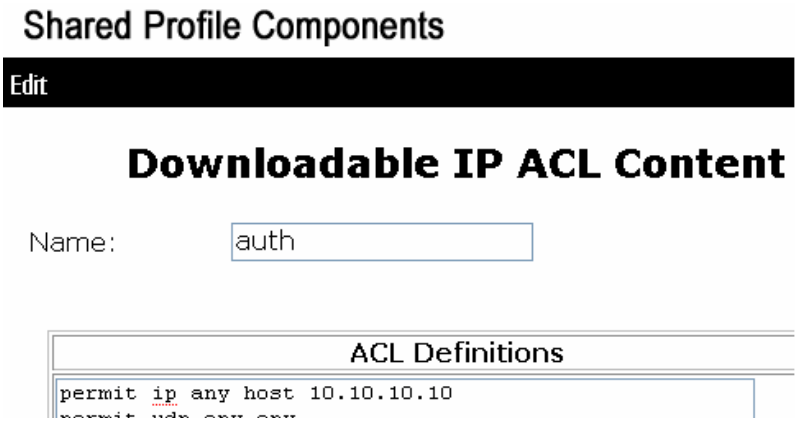
Cisco ACS Configuration for DACL

Note Only Cisco ACS supports DACL.

To ensure correct functioning of the ACS configuration required for DACL, follow these steps:

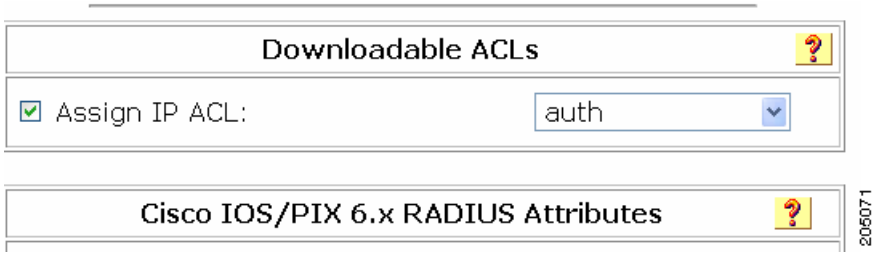
Step 1 Configure a downloadable IP ACL on the window that appears when you select **Radius Shared Profile > Downloadable IP ACL Content** (Figure 46-10).

Figure 46-10 Shared Profile Components



Step 2 Attach this downloadable ACL with the USER on the window that appears when you select **User > DACLs** (Figure 46-11).

Figure 46-11 Downloadable ACLs



URL-Redirect

To configure URL-direct, you need to configure it on the ACS, and on the switch.

Configuring ACS

To configure two Cisco-AV pairs, add the following statements under the user or group Cisco IOS/PIX 6x RADIUS attributes:

```
url-redirect-acl=urlacl
url-redirect=http://www.cisco.com
```

Note A default port ACL must be configured on the interface.

Configuring the Switch

To configure the switch for URL redirect, follow these steps:

Step 1 Configure the IP device tracking table.

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

Step 2 Configure RADIUS by using the **send authentication** command.

```
Switch(config)# radius-server vsa send authentication
```

Step 3 Configure the URL redirect ACL (URLACL).

```
Switch# ip access-list urlacl
    10 permit tcp any any
Switch#
```

Step 4 Configure static ACL (PACL) for the interface.

```
Switch(config)# int g2/9
Switch(config-if)# ip access-group pacl-4 in
```

Interface Configuration Example

```
Switch# show running-configuration int g2/9
Building configuration...

Current configuration : 617 bytes
!
interface GigabitEthernet2/9
 switchport
 switchport access vlan 29
 switchport mode access
 switchport voice vlan 1234
 access-group mode prefer port
 ip access-group pacl-4 in
 speed 100
 duplex full
 authentication event fail action authorize vlan 111
 authentication event server dead action authorize vlan 333
 authentication event server alive action reinitialize
 authentication host-mode multi-auth
 authentication order dot1x
 authentication port-control auto
 authentication timer restart 100
 authentication timer reauthenticate 20
 authentication timer inactivity 200
 mab
```

```
 dot1x pae authenticator
end

Switch#

Switch# show access-list pacl-4
    10 permit ip host 1.1.1.1 host 2.2.2.2
    20 permit icmp host 1.1.1.1 host 2.2.2.2
Switch#
```

Verify URL-redirect by using the following commands.

The **show ip device tracking** command displays the constraints on the IP device tracking table:

```
Switch(config)# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------
  IP Address     MAC Address       Interface          STATE
-----------------------------------------------------------
50.0.0.12       0015.60a4.5e84 GigabitEthernet2/9     ACTIVE
```

The **show authentication sessions interface details** command displays the URL-redirect-acl and URL-redirect URL information that downloads from the ACS:

```
Switch-2033# show authentication sessions int G1/0/7 details
            Interface:  GigabitEthernet1/0/7
          MAC Address:  2c54.2d6a.0344
         IPv6 Address:  Unknown
         IPv4 Address:  7.7.7.17
            User-Name:  2C-54-2D-6A-03-44
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  0A4046D50000009502F03C4B
      Acct Session ID:  0x000000D9
               Handle:  0x0700005A
       Current Policy:  POLICY_Et0/0

Local Policies:

Server Policies:
         URL Redirect:  www.cisco.com
     URL Redirect ACL:  urlacl

Method status list:

       Method           State
       mab              Authc Success
```

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

Guideline for DACL and URL Redirect

For downloadable ACL or URL redirect, the ACL source must be ANY (permit TCP ANY host 1.1.1.1 eq 80 or permit TCP ANY host 1.1.1.1 eq 443).

Configuring a Downloadable Policy

To configure downloadable policies, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# access-list` *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]	Defines the default port ACL through a source address and wildcard. The *access-list-number* is a decimal from 1 to 99 or 1300 to 1999. Enter **deny** or **permit** to specify whether to deny or permit access if conditions match. *source* is the address of the network or host from which the packet is sent, specified as follows: • The 32-bit quantity in dotted-decimal format • The keyword any as an abbreviation for source and source-wildcard value of 0.0.0.0 255.255.255.255 You do not need a source-wildcard value. • The keyword host as an abbreviation for source and source-wildcard of source 0.0.0.0. (Optional) Applies the source-wildcard wildcard bits to the source. (Optional) Enters log to cause an informational logging message about the packet that matches the entry to be sent to the console.
Step 3	`Switch(config-if)# interface` *interface-id*	Enters interface configuration mode.
Step 4	`Switch(config-if)# ip access-group` {*access-list-number* | *name*} **in**	Controls access to the specified interface. This step is mandatory for a functioning downloaded policy.
Step 5	`Switch(config)# exit`	Returns to global configuration mode.
Step 6	`Switch(config)# aaa new-model`	Enables AAA.
Step 7	`Switch(config)# aaa authorization network default local`	Sets the authorization method to local. To remove the authorization method, use the **no aaa authorization network default local** command.
Step 8	`Switch(config)# ip device tracking`	Enables the IP device tracking table. To disable the IP device tracking table, use the **no ip device tracking** global configuration commands.
Step 9	`Switch(config)# ip device tracking` [**probe** {**count** *count* | **interval** *interval*}]	(Optional) Configures these parameters for the IP device tracking table: • **count—**Number of times that the switch sends the ARP probe. The range is 1 to 5. The default is 3. • **interval—**Number of seconds that the switch waits for a response before resending the ARP probe. The range is 30 to 300 seconds. The default is 30 seconds.
Step 10	`Switch(config)# ip device tracking` [**probe** {*delay interval*}]	(Optional) Configures the optional probe delay parameter for the IP device tracking table: • **interval**—Number of seconds that the switch delays sending an ARP probe, triggered by link-up and ARP probe generation by the tracked device. The range is 1 to 120 seconds. The default is 0 seconds.

	Command	Purpose
Step 11	`Switch(config)# radius-server vsa send authentication`	Configures the network access server to recognize and use vendor-specific attributes. **Note** The downloadable ACL must be operational.
Step 12	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 13	`Switch# show ip device tracking {all | interface interface-id | ip ip-address | mac mac-address}`	Displays information about the entries in the IP device tracking table.
Step 14	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

The following example illustrates how to configure a switch for downloadable policy:

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default local
Switch(config)# ip device tracking
Switch(config)# ip access-list extended default_acl
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# radius-server vsa send authentication
Switch(config)# int fastEthernet 2/13
Switch(config-if)# ip access-group default_acl in
Switch(config-if)# exit
```

Configuring 802.1X Authentication with Per-User ACL and Filter-ID ACL

This section includes the following topics:

Per-User ACL and Filter-ID ACL

Prior to Cisco IOS Release 12.2(52)SG, the Catalyst 4500 platform only supported downloadable ACLs, which work with the Cisco ACS server but not with third-party AAA servers. With Cisco IOS Release 12.2(52)SG, the Catalyst 4500 switch offers the Filter-ID/Per-user-acl enhancement, which allows ACL policy enforcement using a third-party AAA server.

The Filter-ID feature provides the following capabilities:

Filter-ID option allows an administrator to define the ACL name on the AAA server using IETF standard RADIUS attribute. The ACL itself must be preconfigured locally on the switch.

The Per-user-acl feature provides the following capabilities:

Per-user ACL allows an administrator to define the per-user ACL on the AAA server using Cisco RADIUS AV pairs. This action allows a third-party AAA server to interoperate by loading the Cisco RADIUS dictionary, which has Cisco Radius AV pairs configured as a VSA.

Note The RADIUS vendor-specific attributes (VSAs) allow vendors to support their own proprietary RADIUS attributes that are not included in standard RADIUS attributes.

Configuring the Switch

To configure the switch for per-user ACL and filter-ID ACL:

Step 1 Configure the IP device tracking table.

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

Step 2 Configure static ACL for the interface.

```
Switch(config)# int g2/9
Switch(config-if)# ip access-group pacl-4 in
```

Interface Configuration Example

```
Switch# show running-configuration interface g2/9
Building configuration...

Current configuration : 617 bytes
!
interface GigabitEthernet2/9
 switchport
 switchport access vlan 29
 switchport mode access
 switchport voice vlan 1234
 access-group mode prefer port
 ip access-group pacl-4 in
 speed 100
 duplex full
 authentication event fail action authorize vlan 111
 authentication event server dead action authorize vlan 333
 authentication event server alive action reinitialize
 authentication host-mode multi-auth
 authentication order dot1x
 authentication port-control auto
 authentication timer restart 100
 authentication timer reauthenticate 20
 authentication timer inactivity 200
 mab eap
 dot1x pae authenticator
end

Switch#
Switch# show ip access-list pacl-4
    10 permit ip host 1.1.1.1 host 2.2.2.2
    20 permit icmp host 1.1.1.1 host 2.2.2.2
Switch#
```

Per-User ACL Configuration in ACS

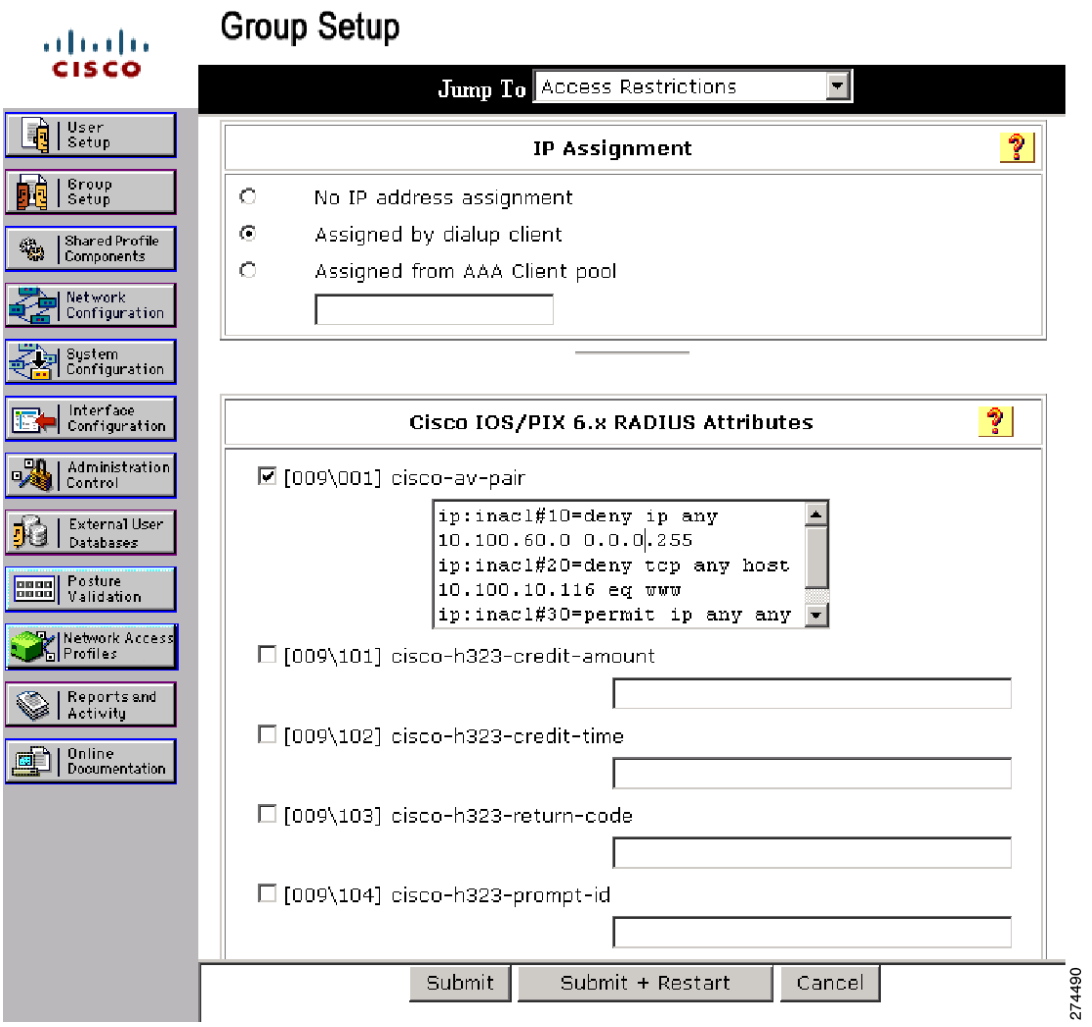
In the Group/User Setting page, scroll down to the Cisco IOS/PIX 6.x RADIUS Attributes section. Select the box next to [009\001 cisco-av-pair] and enter the elements of the per-user ACL. Per-user ACLS take this format:

```
protocol_#:inacl# sequence number=ACE
```

protocol Either ip (for IP-based ACLs) or mac (for MAC-based ACLs)

Figure 46-12 shows how members of the group you are configuring are denied all access to the 10.100.60.0 subnet, are denied HTTP access to the server at 10.100.10.116, and are permitted everywhere else.

Figure 46-12 Define the ACEs for the Per-User ACL



Note Outbound ACLs (OUTACL) are not supported.

Filter-Id Configuration in ACS

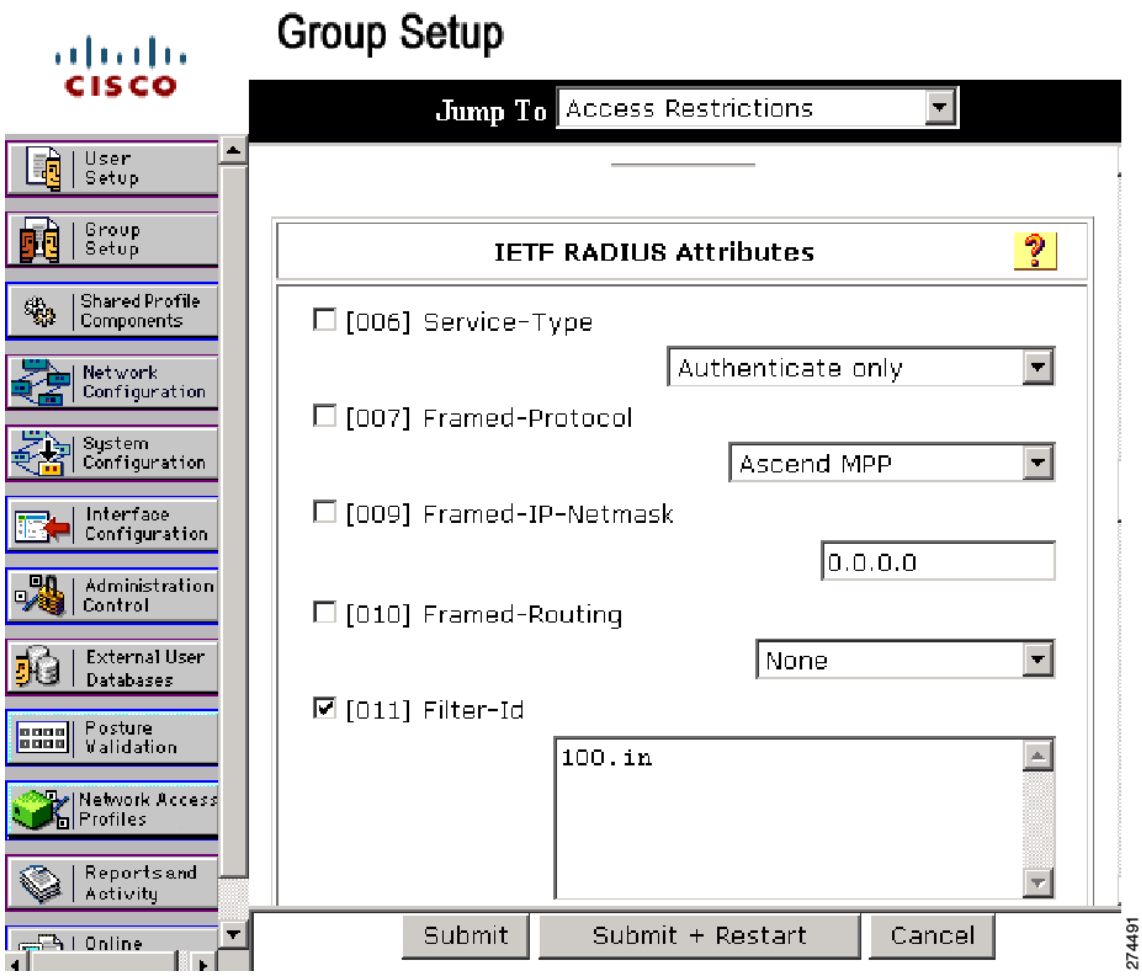
In the Group/User Setting page, scroll down to the IETF RADIUS Attributes section. Select the box next to Filter-Id and enter the ACL to apply for members of this group (Figure 46-13).

The Filter-Id ia in this format:

`ACL_#.in`

ACL Number of the ACL that was previously configured on the switch

Figure 46-13 Configuring the Filter-ID Attribute



Note Outbound ACLs (for example, 100.out) are not supported.

Debug Commands for Per-User ACL and Filter-ID ACL

The IP device tracking table contains the host IP address learned through ARP or DHCP. The following command displays the constraints on the IP device tracking table:

```
Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------
IP Address MAC Address Interface STATE
-----------------------------------------------------------
50.0.0.12 0015.60a4.5e84 GigabitEthernet2/9 ACTIVE
```

The following command shows authentication sessions that contains the Filter-Id 100:

```
Switch-2033# show authentication sessions interface G2/9 details
            Interface:  GigabitEthernet2/9
          MAC Address:  2c54.2d6a.0344
```

```
         IPv6 Address:  Unknown
         IPv4 Address:  7.7.7.19
            User-Name:  2C-54-2D-6A-03-44
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  0A4046D50000009C0310AB47
      Acct Session ID:  0x000000E7
               Handle:  0xF3000061
       Current Policy:  POLICY_Gi2/9

Server Policies:
              URL Redirect ACL:  testacl
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51def075
              Filter-ID:  100

Method status list:
       Method           State
       mab              Authc Success
```

The following command displays the contents of the per-user-acl (note that per-user-acl are shown above as the default port ACL configured on the interface, 151 is the default port ACL in the following example):

```
Switch# show access-list
151

     deny ip host 20.20.0.3 host 20.20.10.10

    10 permit ip any any (57 estimate matches)
```

The following command displays the number of sessions:

```
RouterRP# show authentication sessions

Interface    MAC Address    Method  Domain  Status Fg Session ID
Gi2/9        aabb.cc00.5600 mab     VOICE   Auth      0D0102340000000CEDF12589

Session count = 1

Key to Session Events Status Flags:

  A - Applying Policy (multi-line status for details)
  D - Awaiting Deletion
  F - Final Removal in progress
  I - Awaiting IIF ID allocation
  P - Pushed Session (non-transient state)
  R - Removing User Profile (multi-line status for details)
  U - Applying User Profile (multi-line status for details)
  X - Unknown Blocker
```

The following command displays authentication sessions that contains the per-user-acl:

```
S2049# show authentication sessions int gi 2/9 det
           Interface:  GigabitEthernet2/9
         MAC Address:  ccdd.aabb.0001
        IPv6 Address:  Unknown
        IPv4 Address:  6.6.65.66
           User-Name:  ccddaabb0001
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  multi-auth
```

```
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  0D0202010000003D04147B45
      Acct Session ID:  0x0000004A
               Handle:  0x7900002A
       Current Policy:  POLICY_Gi2/9

Local Policies:
    arp-probe-timeout:  yes

Server Policies:
         Per-User ACL:  GigabitEthernet1/0/23#v4#7C1C4AC
                     :  permit ip any host 1.1.1.20


Method status list:
       Method           State
       mab              Authc Success
```

The following command displays the contents of the per-user-acl (note that per-user-acl are shown above as the default port ACL configured on the interface, 151 is the default port ACL in the preceding example below):

```
Switch# show access-list
151

     deny ip host 20.20.0.3 host 20.20.10.10

    10 permit ip any any (57 estimate matches)
..
..
..(check for the mac access-list created)..
..
Extended MAC access list PerUser_MAC_ACL-589079192 (per-user)
    deny   any host 0000.aaaa.aaaa
..
```

The following command shows that the Policy Enforced Module (EPM) session contains the Filter-Id 155 from ACS:

Note The 156 IP extended ACL is to be preconfigured on the switch, so that the policy enforcement can happen.

```
Switch# show ip access-list 156
Extended IP access list 156
    10 deny ip any host 155.155.155.156
    20 deny ip any 156.100.60.0 0.0.0.255
    30 deny tcp any host 156.100.10.116 eq www
```

The following command shows authentication sessions that contains the Filter-Id TEST-ACL. TEST-ACL has been defined locally:

```
Switch-2033# show authentication sessions interface Gi2/9 details
            Interface:  GigabitEthernet2/9
          MAC Address:  2c54.2d6a.0344
         IPv6 Address:  Unknown
         IPv4 Address:  7.7.7.19
            User-Name:  2C-54-2D-6A-03-44
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
```

```
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  0A4046D50000009C0310AB47
      Acct Session ID:  0x000000E7
               Handle:  0xF3000061
       Current Policy:  POLICY_Gi2/9

Local Policies:
        Template: MYACL (priority 150)
            Filter-ID:  TEST-ACL

Server Policies:
              URL Redirect ACL:  testacl
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51def075


Method status list:
       Method           State
       mab              Authc Success
```

The following command displays the contents of the Filter-Id applied on the interface:

```
Switch# show ip access-list interface gi6/3
     deny ip host 20.20.0.2 host 155.155.155.156
     deny ip host 20.20.0.2 156.100.60.0 0.0.0.255
     deny tcp host 20.20.0.2 host 156.100.10.116 eq www
```

Guidelines for Per-User ACL and Filter-ID ACL

For per user ACL and Filter-ID ACL, the ACL source must be ANY (permit TCP ANY host 1.1.1.1 eq 80 or permit TCP ANY host 1.1.1.1 eq 443).

Configuring a Per-User ACL and Filter-ID ACL

To configure per-user ACL and Filter-ID ACL, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# access-list` *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]	Defines the default port ACL through a source address and wildcard. The *access-list-number* is a decimal from 1 to 99 or 1300 to 1999. Enter **deny** or **permit** to specify whether to deny or permit access if conditions match. *source* is the address of the network or host from which the packet is sent, specified as follows: • The 32-bit quantity in dotted-decimal format • The keyword any as an abbreviation for source and source-wildcard value of 0.0.0.0 255.255.255.255 You do not need a source-wildcard value. • The keyword host as an abbreviation for source and source-wildcard of source 0.0.0.0. (Optional) Applies the source-wildcard wildcard bits to the source. (Optional) Enters log to cause an informational logging message about the packet that matches the entry to be sent to the console.
Step 3	`Switch(config-if)# interface` *interface-id*	Enters interface configuration mode.
Step 4	`Switch(config-if)# ip access-group` {*access-list-number* | *name*} **in**	Controls access to the specified interface. This step is mandatory for a functioning downloaded policy.
Step 5	`Switch(config)# exit`	Returns to global configuration mode.
Step 6	`Switch(config)# aaa new-model`	Enables AAA.
Step 7	`Switch(config)# aaa authorization network default local`	Sets the authorization method to local. To remove the authorization method, use the **no aaa authorization network default local** command.
Step 8	`Switch(config)# ip device tracking`	Enables the IP device tracking table. To disable the IP device tracking table, use the **no ip device tracking** global configuration commands.
Step 9	`Switch(config)# ip device tracking` [**probe** {**count** *count* | interval *interval*}]	(Optional) Configures these parameters for the IP device tracking table: • **count—**Number of times that the switch sends the ARP probe. The range is 1 to 5. The default is 3. • **interval—**Number of seconds that the switch waits for a response before resending the ARP probe. The range is 30 to 300 seconds. The default is 30 seconds.
Step 10	`Switch(config)# ip device tracking` [**probe** {*delay interval*}]	(Optional) Configures the optional probe delay parameter for the IP device tracking table: • **interval**—Number of seconds that the switch delays sending an ARP probe, triggered by link-up and ARP probe generation by the tracked device. The range is 1 to 120 seconds. The default is 0 seconds.

	Command	Purpose
Step 11	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 12	`Switch# show ip device tracking {all | interface interface-id | ip ip-address | mac mac-address}`	Displays information about the entries in the IP device tracking table.
Step 13	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

The following example illustrates how to configure a switch for downloadable policy:

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default local
Switch(config)# ip device tracking
Switch(config)# ip access-list extended default_acl
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# int fastEthernet 2/13
Switch(config-if)# ip access-group default_acl in
Switch(config-if)# exit
```

Configuring RADIUS-Provided Session Timeouts

You can configure the Catalyst 4500 series switch to use a RADIUS-provided reauthentication timeout.

To configure RADIUS-provided timeouts, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface interface-id`	Enters interface configuration mode.
Step 3	`Switch(config-if)# switchport mode access`	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
Step 4	`Switch(config-if)# dot1x pae authenticator`	Enables 802.1X authentication on the port with default parameters. Refer to the "Default 802.1X Configuration" section on page 46-26.

Step 5	Cisco IOS Release 12.2(50)SG and later
	`Switch(config-if)# authentication timer reauthenticate {interface | server}`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x timeout reauth-attempts {interface | server}`
		Sets the reauthentication period (seconds).

Step 6	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 7	`Switch# show dot1x interface interface-id details`	Verifies your entries.
Step 8	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

This example shows how to configure a switch to derive the reauthentication period from the server and to verify the configuration:

Cisco IOS Release 12.2(50):

```
Switch# configure terminal
Switch(config)# interface f7/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication timer reauthenticate server
Switch(config-if)# end
Switch# show dot1x interface f7/1 det

Dot1x Info for FastEthernet7/11
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = FORCE_AUTHORIZED
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = (From Authentication Server)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0

Dot1x Authenticator Client List Empty

Port Status               = AUTHORIZED

Switch#
```

Cisco IOS Release 12.2(46) or earlier

```
Switch# configure terminal
Switch(config)# interface f7/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x timeout reauth-attempts server
Switch(config-if)# end
Switch# show dot1x interface f7/1 det

Dot1x Info for FastEthernet7/11
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = FORCE_AUTHORIZED
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = (From Authentication Server)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
```

```
Dot1x Authenticator Client List Empty

Port Status                = AUTHORIZED

Switch#
```

Configuring MAC Move

MAC move allows an authenticated host to move from one switch port to another.

Note You should remove port security before configuring MAC move.

To globally enable MAC move on the switch, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# authentication mac-move permit`	Enable MAC move globally.
Step 3	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 4	`Switch# show run`	Verifies your entries.
Step 5	`Switch # copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

This example shows how to globally enable MAC move on a switch:

```
Switch# configure terminal
Switch(config)# authentication mac-move permit
```

The following syslog messages displays when MAC-move happens:

```
%AUTHMGR-5-SECUREMACMOVE: <mac-addr> moved from <interface-name> to <interface-name>
```

Configuring MAC Replace

MAC replace allows new users to connect to abandoned ports.

If a user disconnects but the switch has not received the EAPoL-Logoff, the session will remain up. For single or multiple- domain modes, no new hosts can connect to that port. If a new host tries to connect, a violation is triggered on the port. Where the violation action is configured as replace, the desired behavior is for the NAD (switch) to terminate the initial session and reset the authentication sequence based on the new MAC.

To enable MAC replace on a switch, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface interface-id`	Enters interface configuration mode.

	Command	Purpose
Step 3	`Switch(config-if)# authentication violation [restrict | shutdown | replace]`	Tears down the old session and authenticates the new host, when a new host is seen in single or multiple- domain modes.
Step 4	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 5	`Switch# show run`	Verifies your entries.
Step 6	`Switch # copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

This example shows how to globally enable MAC replace on a switch:

```
Switch# configure terminal
Switch(config)# interface f7/1
Switch(config-if)# authentication violation replace
```

The following syslog messages displays when MAC-replace occurs:

```
%AUTHMGR-5-SECUREMACREPLACE: <mac-addr> replaced <mac-addr> on <interface-name>
```

Configuring Violation Action

You can configure 802.1X security violation behavior as either shutdown, restrict, or replace mode, based on the response to the violation.

To configure the violation action, performing the following task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface interface-id`	Enters interface configuration mode.
Step 3	`Switch(config-if)# authentication violation [restrict | shutdown | replace]`	(Optional) Configures the disposition of the port if a security violation occurs. The default action is to shut down the port. If the **restrict** keyword is configured, the port does not shut down. When a new host is seen in single or multiple- domain modes, **replace** mode tears down the old session and authenticates the new host.
Step 4	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 5	`Switch# show run`	Verifies your entries.
Step 6	`Switch # copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

This example shows how to configure the violation mode shutdown on a switch:

```
Switch# configure terminal
Switch(config)# authentication violation shutdown
```

A port is error-disabled when a security violation triggers on shutdown mode. The following syslog messages displays:

```
%AUTHMGR-5-SECURITY_VIOLATION: Security violation on the interface <interface name>, new
MAC address <mac-address> is seen.
```

```
%PM-4-ERR_DISABLE: security-violation error detected on <interface name>, putting
<interface name> in err-disable state
```

Configuring 802.1X with Guest VLANs

You can configure a guest VLAN for each 802.1X port on the Catalyst 4500 series switch to provide limited services to clients, such as downloading the 802.1X client. These clients might be upgrading their system 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 Catalyst 4500 series switch assigns clients to a guest VLAN, provided one of the following apply:

- The authentication server does not receive a response to its EAPOL request or identity frame.
- The EAPOL packets are not sent by the client.

Beginning with Cisco IOS Release 12.2(25)EWA, the Catalyst 4500 series switch maintains the EAPOL packet history. If another EAPOL packet is detected on the interface during the lifetime of the link, network access is denied. The EAPOL history is reset upon loss of the link.

Any number of 802.1X-incapable clients are allowed access when the 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.

Note When a port is put into a guest VLAN, it is automatically placed into multihost mode, and an unlimited number of hosts can connect using the port. Changing the multihost configuration does not effect a port in a guest VLAN.

Note Except for an RSPAN VLAN or a voice VLAN, you can configure any active VLAN as an 802.1X guest VLAN.

To configure 802.1X with guest VLAN on a port, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface` *interface-id*	Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.

Step 3	`Switch(config-if)# switchport mode access`
	or
	`Switch(config-if)# switchport mode private-vlan host`
		Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
		
		Specifies that the ports with a valid PVLAN trunk association become active host PVLAN trunk ports.

Step 4	`Switch(config-if)# dot1x pae authenticator`	Enables 802.1X authentication on the port with default parameters. Refer to the "Default 802.1X Configuration" section on page 46-26.

	Command	Purpose
Step 5	Cisco IOS Release 12.2(50)SG and later `Switch(config-if)# authentication event no-response action authorize vlan` *vlan-id* Cisco IOS Release 12.2(46)SG or earlier releases `Switch(config-if)# dot1x guest-vlan` *vlan-id*	Enables a guest VLAN on a particular interface. To disable the guest VLAN feature on a particular port, use the **no authentication event no-response action authorize vlan** interface configuration command (for earlier releases, use the **no dot1x guest-vlan** interface configuration command).

Step 6	Cisco IOS Release 12.2(50)SG and later
	`Switch(config-if)# authentication port-control auto`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x port-control auto`
		Enables 802.1X authentication on the interface.

Step 7	`Switch(config-if)# end`	Returns to configuration mode.
Step 8	`Switch(config)# end`	Returns to privileged EXEC mode.

This example shows how to enable regular VLAN 50 on Fast Ethernet 4/3 as a guest VLAN on a static access port:

Cisco IOS Release 12.2(50)SG and later

```
Switch# configure terminal
Switch(config)# interface fa4/3
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication event no-response action authorize vlan 50
Switch(config-if)# authentication port-control auto
Switch(config-if)# end
Switch#
```

Cisco IOS Release 12.2(46)SG or earlier

```
Switch# configure terminal
Switch(config)# interface fa4/3
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x guest-vlan 50
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

This example shows how to enable a secondary PVLAN 100 as a guest VLAN on a PVLAN host port:

Cisco IOS Release 12.2(50)SG and later

```
Switch# configure terminal
Switch(config)# interface fa4/3
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication event no-response action authorize vlan 100
Switch(config-if)# end
Switch#
```

Cisco IOS Release 12.2(46)SG or earlier

```
Switch# configure terminal
Switch(config)# interface fa4/3
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x guest-vlan 100
Switch(config-if)# end
Switch#
```

To allow supplicants into a guest VLAN on a switch, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch# dot1x guest-vlan supplicant`	(Optional) Enables supplicants to be allowed into the guest VLANs globally on the switch. **Note** Although not visible in the CLI for Cisco IOS Release 12.3(31)SG, legacy configurations that include the **dot1x guest-vlan supplicant** command still work. We do not recommend that you use this command. However, because the authentication failed VLAN option makes it unnecessary. To disable the supplicant guest VLAN feature on a switch, use the **no dot1x guest-vlan supplicant** global configuration command.
Step 3	`Switch(config)# interface` *interface-id*	Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.

Step 4	`Switch(config-if)# switchport mode access`
	or
	`Switch(config-if)# switchport mode private-vlan host`
		Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
		Specifies that the ports with a valid PVLAN trunk association become active host PVLAN trunk ports.

Step 5	`Switch(config-if)# dot1x pae authenticator`	Enables 802.1X authentication on the port with default parameters. Refer to the "Default 802.1X Configuration" section on page 46-26.
Step 6	`Switch(config-if)# dot1x guest-vlan` *vlan-id*	Specifies an active VLAN as an 802.1X guest VLAN. The range is 1 to 4094.

Step 7	Cisco IOS Release 12.2(50)SG and later
	`Switch(config-if)# authentication port-control auto`
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x port-control auto`
		Enables 802.1X authentication on the interface.

Step 8	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 9	`Switch# show dot1x interface` *interface-id*	Verifies your entries.
Step 10	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

This example shows how to enable the guest VLAN feature and to specify VLAN 5 as a guest VLAN:

Cisco IOS Release 12.2(50)SG and later

```
Switch# configure terminal
Switch(config)# dot1x guest-vlan supplicant
Switch(config)# interface gigabitethernet5/9
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication event no-response action authorize vlan 5
Switch(config-if)# authentication port-control auto
Switch(config-if)# end
Switch#
```

Cisco IOS Release 12.2(46)SG or earlier

```
Switch# configure terminal
Switch(config)# dot1x guest-vlan supplicant
Switch(config)# interface gigabitethernet5/9
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x guest-vlan 5
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

Configuring 802.1X with MAC Authentication Bypass

To enable MAC Authentication Bypass (MAB), perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface` *interface-id*	Specifies the port to be configured, and enters interface configuration mode.

Step 3	`Switch(config-if)# switchport mode access`
	or
	`Switch(config-if)# switchport mode private-vlan host`
		Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
		
		Specifies that the ports with a valid PVLAN trunk association become active host PVLAN trunk ports.

Step 4	`Switch(config-if)# dot1x pae authenticator`	Enables 802.1X authentication on the port with default parameters. Refer to the "Default 802.1X Configuration" section on page 46-26.

Step 5	Cisco IOS Release 12.2(50)SG and later
	`Switch(config-if)# authentication port-control auto`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x port-control auto`
		Enables 802.1X authentication on the interface.

Step 6	Cisco IOS Release 12.2(50)SG and later
	`Switch(config-if)# mab [eap]`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x mac-auth-bypass [eap]`
		Enables MAB on a switch.
		The **eap** option specifies that a complete EAP conversation should be used, as opposed to standard RADIUS Access-Request, Access-Accept conversation. By default, the **eap** option is not enabled for MAB.

	Command	Purpose
Step 7	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 8	`Switch# show mab interface` *interface-id* `details`	(Optional) Verifies your entries.
Step 9	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Note Removing a 802.1X MAB configuration from a port does not impact the authorized or authenticated state of the port. If the port is in an unauthenticated state, it remains in that state. If the port is in an authenticated state because of MAB, the switch reverts to the 802.1X Authenticator. If the port was already authorized with a MAC address and the MAB configuration was removed, the port remains in an authorized state until reauthentication occurs. At that time, if an 802.1X supplicant is detected on the wire, the MAC address is removed.

This example shows how to enable MAB on Gigabit Ethernet interface 3/3 and to verify the configuration:

Cisco IOS Release 12.2(50)SG and later

```
Switch# configure terminal
Switch(config)# interface gigabitethernet3/3
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication port-control auto
Switch(config-if)# mab
Switch(config-if)# end
Switch# show mab int g3/3 details
MAB details for GigabitEthernet3/3
--------------------------------------
Mac-Auth-Bypass           = Enabled

MAB Client List
---------------
Client MAC                = 0001.0001.0001
Session ID                = C0A8016F0000002304175914
MAB SM state              = TERMINATE
Auth Status               = AUTHORIZED
```

Cisco IOS Release 12.2(46)SG or earlier

```
Switch# configure terminal
Switch(config)# interface gigabitethernet3/3
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x mac-auth-bypass
Switch(config-if)# end
Switch# show dot1x int g3/3 details
Dot1x Info for GigabitEthernet3/3
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
```

```
QuietPeriod                = 60
ServerTimeout              = 30
SuppTimeout                = 30
ReAuthPeriod               = 3600 (Locally configured)
ReAuthMax                  = 2
MaxReq                     = 2
TxPeriod                   = 1
RateLimitPeriod            = 0
Mac-Auth-Bypass            = Enabled

Dot1x Authenticator Client List
-------------------------------
Supplicant                 = 0000.0000.0001
 Auth SM State      = AUTHENTICATED
 Auth BEND SM Stat = IDLE
Port Status                = AUTHORIZED
Authentication Method      = MAB
Authorized By              = Authentication Server
Vlan Policy                = N/A

Switch#
```

Configuring 802.1X with Inaccessible Authentication Bypass

Caution You must configure the switch to monitor the state of the RADIUS server as described in the section Configuring Switch-to-RADIUS-Server Communication, page 46-31 for Inaccessible Authentication Bypass to work properly. Specifically, you must configure the RADIUS test username, idle-time, deadtime and dead-criteria. Failure to do so results in the switch failing to detect that the RADIUS server has gone down, or prematurely marking a dead RADIUS server as alive again.

To configure a port as a critical port and to enable the Inaccessible Authentication Bypass feature, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# dot1x critical eapol`	(Optional) Configures whether to send an EAPOL-Success packet when a port is critically authorized partway through an EAP exchange. **Note** Some supplicants require this. The default is not to send EAPOL-Success packets when a port is critically authorized partway through an EAP exchange. If there is no ongoing EAP exchange at the time when a port is critically authorized, EAPOL-Success packet is always sent out regardless of this option.

	Command	Purpose

Step 3	[Catalyst 4900M, Catalyst 4948E, Catalyst 4948E-F, Catalyst 4948E-F, Supervisor Engine 6-E, and Supervisor Engine 6L-E] Cisco IOS Release 12.2(50)SG and later
	[Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E)]
	Cisco IOS Release 15.0(1)X and later
	`Switch(config)# authentication critical recovery delay msec`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config)# dot1x critical recovery delay msec`
		(Optional) Specifies a throttle rate for the reinitialization of critically authorized ports when the RADIUS server becomes available. The default throttle rate is 100 milliseconds. This means that 10 ports reinitialize per second.

Step 4	`Switch(config)# interface interface-id`	Specifies the port to be configured and enters interface configuration mode.

Step 5	`Switch(config-if)# switchport mode access`
	or
	`Switch(config-if)# switchport mode private-vlan host`
		Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
		
		Specifies that the ports with a valid PVLAN trunk association become active host PVLAN trunk ports.

Step 6	`Switch(config-if)# dot1x pae authenticator`	Enables 802.1X authentication on the port with default parameters. Refer to the "Default 802.1X Configuration" section on page 46-26.
Step 7	`Switch(config-if)# authentication port-control auto`	Enables 802.1X authentication on the interface.

Step 8	[Catalyst 4900M, Catalyst 4948E, Catalyst 4948E-F, Supervisor Engine 6-E, and Supervisor Engine 6L-E]
	Cisco IOS Release 12.2(50)SG and later
	[Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E)]
	Cisco IOS Release 15.0(1)XO and later
	`Switch(config-if)# authentication event server dead action authorize [vlan vlan-id]`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x critical`
	
	or
	[Catalyst 4900M, Catalyst 4948E, Catalyst 4948E-F, Supervisor Engine 6-E, and Supervisor Engine 6L-E]
	Cisco IOS Release 15.0(2)SG and later
	[Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E)]
	Cisco IOS Release XE 3.2.0SG and later
	`Switch(config-if)# [no] authentication event server dead action reinitialize [vlan vlan-id]`
		Enables the Inaccessible Authentication Bypass feature for data clients on the port and specifies a VLAN into which data clients are assigned. If no VLAN is specified, data clients are assigned into the configured data VLAN on the port.
		To disable the feature, use the **no authentication event server dead action authorize vlan** interface configuration command (for earlier releases, use the **no dot1x critical** interface configuration command).
		
		Alternatively, starting with Cisco IOS Release 15.0(2)SG you can enable Inaccessible Authentication Bypass for data clients using the **authentication event server dead action reinitialize vlan** interface configuration command which forces all authorized data clients to be reauthenticated when RADIUS becomes unavailable and a client attempts to authenticate. This only applies to data devices. Voice devices are unaffected.
		To disable it, use the **no authentication event server dead action reinitialize vlan** interface configuration command.

	Command	Purpose
Step 9	[Catalyst 4900M, Catalyst 4948E, Catalyst 4948E-F, Supervisor Engine 6-E, and Supervisor Engine 6L-E] Cisco IOS Release 15.0(2)SG and later [Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E)] Cisco IOS Release XE 3.2.0SG and later `Switch(config-if)# authentication event server dead action authorize voice`	(Optional) Enables Inaccessible Authentication Bypass for voice clients on the port. This command applies to Multiple Domain Authentication and Multiple Authentication modes. To disable the feature, use the **no authentication event server dead action authorize voice** interface configuration command.

Step 10	[Catalyst 4900M, Catalyst 4948E, Catalyst 4948E-F, Supervisor Engine 6-E, and Supervisor Engine 6L-E]
	Cisco IOS Release 12.2(50)SG and later [Supervisor Engine 7-E, Supervisor Engine 7L-E, Supervisor Engine 8-E)]
	Cisco IOS Release 15.0(1)XO and later
	`Switch(config-if)# authentication event server alive action reinitialize`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x critical recovery action reinitialize`
		(Optional) Specifies that the port should be reinitialized if it is critically authorized and RADIUS becomes available.
		The default is not to reinitialize the port.

Step 11	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 12	`Switch# show dot1x interface` *interface-id* **details**	(Optional) Verifies your entries.
Step 13	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

The following example shows a full configuration of 802.1X with Inaccessible Authentication Bypass, including required AAA and RADIUS configuration as specified in the "Enabling 802.1X Authentication" section on page 46-28 and "Configuring Switch-to-RADIUS-Server Communication" section on page 46-31.

The RADIUS server configured is at IP address 10.1.2.3, using port 1645 for authentication and 1646 for accounting. The RADIUS secret key is mykey. The username used for the test server probes is randomizes. The test probes for both living and dead servers are generated once per minute. The interface FastEthernet 3/1 is configured to critically authenticate into VLAN 17 when AAA becomes unresponsive, and to reinitialize automatically when AAA becomes available again.

Cisco IOS Release 12.2(50)SG and later

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# dot1x system-auth-control
Switch(config)# radius-server host 10.1.2.3 auth-port 1645 acct-port 1646 test username
randomuser idle-time 1 key mykey
Switch(config)# radius-server deadtime 1
Switch(config)# radius-server dead-criteria time 15 tries 3
Switch(config)# interface f3/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication event server dead action authorize vlan 17
Switch(config-if)# end
```

```
Switch# show dot1x int fastethernet 3/1 details

Dot1x Info for FastEthernet3/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Critical-Auth             = Enabled
Critical Recovery Action  = Reinitialize
Critical-Auth VLAN        = 17

Dot1x Authenticator Client List
-------------------------------
Supplicant                = 0000.0000.0001

Auth SM State     = AUTHENTICATING
Auth BEND SM Stat = RESPONSE
Port Status               = AUTHORIZED
Authentication Method     = Dot1x
Authorized By             = Critical-Auth
Operational HostMode      = SINGLE_HOST
Vlan Policy               = 17

Switch#
```

Cisco IOS Release 12.2(46)SG or earlier

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# dot1x system-auth-control
Switch(config)# radius-server host 10.1.2.3 auth-port 1645 acct-port 1646 test username
randomuser idle-time 1 key mykey
Switch(config)# radius-server deadtime 1
Switch(config)# radius-server dead-criteria time 15 tries 3
Switch(config)# interface f3/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x critical
Switch(config-if)# dot1x critical vlan 17
Switch(config-if)# dot1x critical recovery action reinitialize
Switch(config-if)# end
Switch# show dot1x int fastethernet 3/1 details

Dot1x Info for FastEthernet3/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
```

```
SuppTimeout                = 30
ReAuthPeriod               = 3600 (Locally configured)
ReAuthMax                  = 2
MaxReq                     = 2
TxPeriod                   = 30
RateLimitPeriod            = 0
Critical-Auth              = Enabled
Critical Recovery Action   = Reinitialize
Critical-Auth VLAN         = 17

Dot1x Authenticator Client List
-------------------------------
Supplicant                 = 0000.0000.0001

Auth SM State      = AUTHENTICATING
Auth BEND SM Stat = RESPONSE
Port Status                = AUTHORIZED
Authentication Method      = Dot1x
Authorized By              = Critical-Auth
Operational HostMode       = SINGLE_HOST
Vlan Policy                = 17

Switch#
```

Configuring 802.1X with Unidirectional Controlled Port

To configure unidirectional controlled port, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface interface-id`	Specifies the port to be configured and enters interface configuration mode.

Step 3	`Switch(config-if)# switchport mode access`
	or
	`Switch(config-if)# switchport mode private-vlan host`
		Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
		
		Specifies that the ports with a valid PVLAN trunk association become active host PVLAN trunk ports.

Step 4	`Switch(config-if)# dot1x pae authenticator`	Enables 802.1X authentication on the port with default parameters. Refer to the "Default 802.1X Configuration" section on page 46-26.
Step 5	`Switch(config-if)# authentication port-control auto`	Enables 802.1X authentication on the interface.

Step 6	Cisco IOS Release 12.2(50)SG and later
	`Switch(config-if)# authentication control-direction {in | both}`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x control-direction {in | both}`
		Enables unidirectional port control on each port.

Step 7	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 8	`Switch# show dot1x interface interface-id details`	(Optional) Verifies your entries.
Step 9	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Note Unidirectional controlled port only works when Spanning Tree PortFast is enabled on the port. Unidirectional controlled port and Spanning Tree PortFast should be configured on a switch port that connects to a host. If two such ports are connected together with an Ethernet cable, high CPU utilization may result because host learning will be flapping between the two ports.

This example shows how to enable unidirectional port control:

Cisco IOS Release 12.2(50)SG and later

```
Switch# configure terminal
Switch(config)# interface gigabitethernet3/3
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication control-direction in
Switch(config-if)# end
Switch# show dot1x int g3/3
Dot1x Info for GigabitEthernet3/3
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = In
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0

Switch#
```

Cisco IOS Release 12.2(46)SG or earlier

```
Switch# configure terminal
Switch(config)# interface gigabitethernet3/3
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x control-direction in
Switch(config-if)# end
Switch# show dot1x int g3/3
Dot1x Info for GigabitEthernet3/3
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = In
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0

Switch#
```

Configuring 802.1X with VLAN User Distribution

You will need to configure the switch and ACS to configure 802.1X with VLAN user distribution.

Configuring the Switch

To configure the switch, follow these steps:

Step 1 Create a VLAN group on the switch.

Enter the following commands to create a VLAN group and assign some VLANs to the VLAN group. The following example creates the VLAN group **eng-group** and maps VLANs 20 to 24 to that group:

```
Switch# configure terminal
Switch(config)# vlan group eng-group vlan-list 20-24
Switch(config)# end
Switch# show vlan group group-name eng-group
Group Name VLANs Mapped
---------------- --------------------
eng-group        20-24
```

Note Ensure that the VLANs you specify as part of the VLAN group are enabled on the switch. Only specified VLANs are considered for assignment.

Step 2 Configure the individual ports for multidomain, single-host or multiple- host.

For details, refer to the "Enabling 802.1X Authentication" section on page 46-28.

show commands

Use the following **show** commands to display the member VLANs in a VLAN group:

show command	Purpose
show vlan group all	Displays the member VLANs for all the VLAN groups configured on the device.
show vlan group group-name *vlan-group-name*	Displays the member VLANs in a VLAN group with the given VLAN group name.
show vlan group group-name *vlan-group-name* **user-count**	Displays the user count for each of the member VLANs of the specified VLAN group This feature counts only authenticated users and MAC addresses added through port security for distribution. It does not consider other learned MAC addresses. As of Cisco IOS Release 12.2(54)SG, the user count for a VLAN is incremented when a host is learned through port security, 802.1X, MAB, or fallback authentication on that VLAN.

The following examples show outputs of the **show vlan group** command:

```
Switch# show vlan group all
Group Name VLANs Mapped
---------------- --------------------
eng-dept         3-4

Switch# show vlan group group-name my_group user-count
     VLAN :   Count
   -------------------
     3          : 1
     4          : 0
     5          : 2
     7          : 0
     9          : 0
Switch#
```

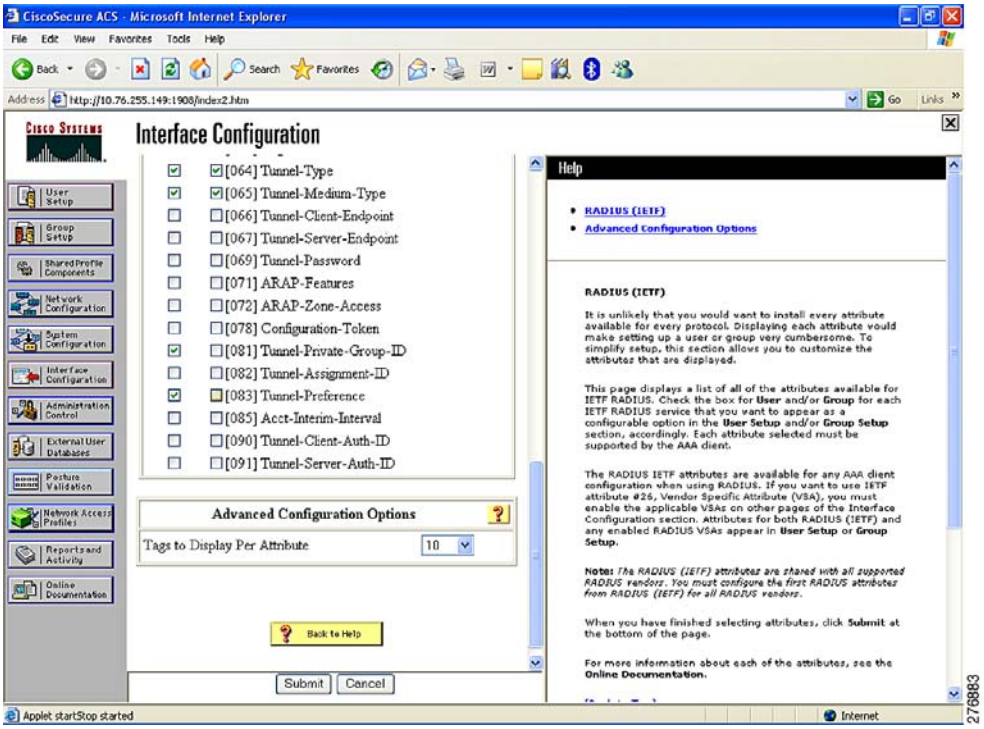
In this example, VLANs 3,4, 5, 7, and 9 are members of the VLAN group *my group*.

ACS Configuration

After configuring the switch, you must provide the VLAN group name in the ACS configuration.

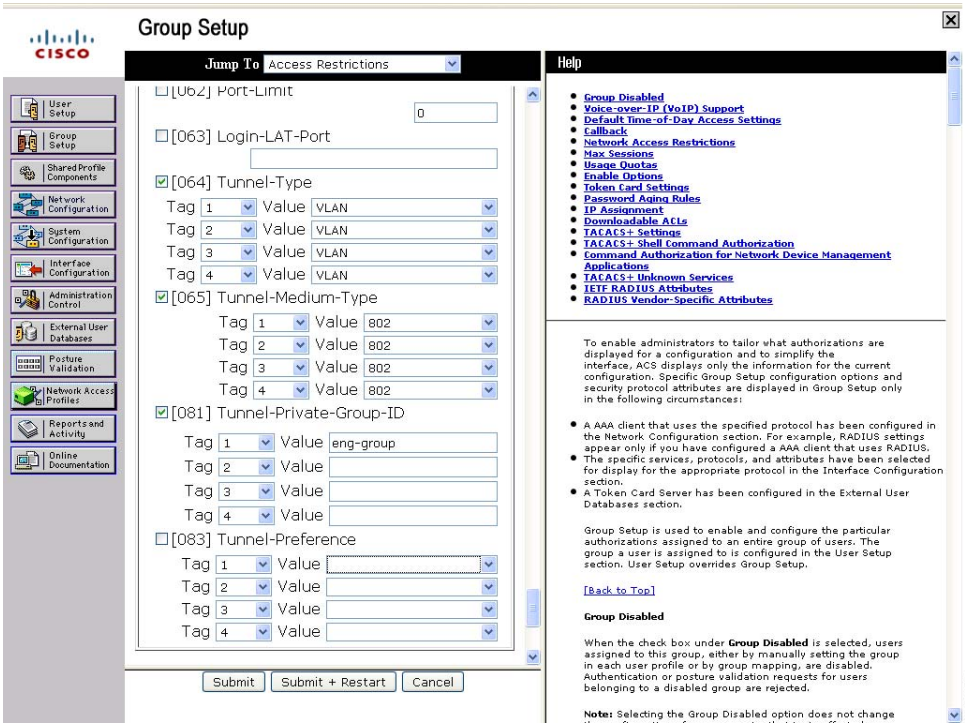
By default, ACS sends only one VLAN name or group per user. However, you can configure ACS to send more than one tag per attribute. To do this, you must modify the configuration in ACS for user or group. (See the example shown in Figure 46-14.)

Figure 46-14 VLAN User Distribution on ACS: Interface Configuration to Modify Tags per Attribute



After you add the number of tags required per attribute, the user or group set up presents multiple fields to be filled with values from the RADIUS server (Figure 46-15).

Figure 46-15 VLAN User Distribution on ACS: Multiple VLAN Numbers Configured per User



After you complete these two tasks and receive authorization, ACS sends the configured VLAN group to the switch. The switch is alerted to the list of VLANs configured under the VLAN group, and the least loaded valid VLAN in the group is assigned to the port.

Configuring 802.1X with Authentication Failed

By configuring authentication-failed VLAN alignment on any Layer 2 port on the Catalyst 4500 series switch, you can provide limited network services to clients that fail the authentication process.

Note You can use authentication-failed VLAN assignment with other security features, such as Dynamic ARP Inspection (DAI), Dynamic Host Configuration Protocol (DHCP) snooping, and IP Source Guard. Each of these features can be enabled and disabled independently on the authentication-failed VLAN.

To configure 802.1X with authentication-failed VLAN assignment, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface` *interface-id*	Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.
Step 3	`Switch(config-if)# switchport mode access`	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
Step 4	`Switch(config-if)# authentication port-control auto`	Enables 802.1X authentication on the interface.

	Command	Purpose

Step 5	Cisco IOS Release 12.2(50)SG and later
	`Switch(config-if)# authentication event fail action authorize vlan vlan-id`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x auth-fail vlan vlan-id`
		Enables authentication-failed VLAN on a particular interface.
		To disable the authentication-failed VLAN feature on a particular port, use the **no authentication event fail action authorize vlan** interface configuration command.

Step 6	Cisco IOS Release 12.2(50)SG and later
	`Switch(config-if)# authentication event fail retry max-attempts action [authorize vlan vlan-id | next-method]`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x auth-fail max-attempts max-attempts`
		Configure a maximum number of attempts before the port is moved to authentication-failed VLAN.
		Default is 3 attempts.

Step 7	`Switch(config-if)# end`	Returns to configuration mode.
Step 8	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 9	`Switch# show dot1x interface interface-id details`	(Optional) Verifies your entries.
Step 10	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

This example shows how to enable a regular VLAN 40 on Fast Ethernet 4/3 as a authentication-failed VLAN on a static access port:

Cisco IOS Release 12.2(50)SG and later

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet3/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication event fail retry 5 action authorize vlan 40
Switch(config-if)# end
Switch# show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            2

Dot1x Info for GigabitEthernet3/1
----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
Switch#
```

Cisco IOS Release 12.2(46)SG or earlier

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet3/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x auth-fail vlan 40
Switch(config-if)# dot1x auth-fail max-attempts 3
Switch# show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            2
Critical Recovery Delay         100
Critical EAPOL              Disabled

Dot1x Info for GigabitEthernet3/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 5
RateLimitPeriod           = 0
Auth-Fail-Vlan            = 40
Auth-Fail-Max-attempts    = 3
Switch#
```

Configuring 802.1X with Voice VLAN

Note You must configure 802.1X and voice VLAN simultaneously.

Note You cannot configure an authentication-failed VLAN and a voice VLAN on the same port. When you try to configure these two features on the same port, a syslog message appears.

To enable 802.1X with voice VLAN, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface` *interface-id*	Enters interface configuration mode.
Step 3	`Switch(config-if)# switchport access vlan` *vlan-id*	Sets the VLAN for a switched interface in access mode.
Step 4	`Switch(config-if)# switchport mode access`	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
Step 5	`Switch(config-if)# switchport voice vlan` *vlan-id*	Sets the voice VLAN for the interface.

	Command	Purpose
Step 6	`Switch(config-if)# dot1x pae authenticator`	Enables 802.1X authentication on the port with default parameters. Refer to the "Default 802.1X Configuration" section on page 46-26.

Step 7	Cisco IOS Release 12.2(50)SG and later
	`Switch(config-if)# authentication port-control auto`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x port-control auto`
		Enables 802.1X authentication on the interface.

Step 8	`Switch(config-if)# end`	Returns to configuration mode.
Step 9	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 10	`Switch# show dot1x interface` *interface-id* `details`	(Optional) Verifies your entries.
Step 11	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

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

Cisco IOS Release 12.2(50)SG and later

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

Cisco IOS Release 12.2(46)SG or earlier

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

Configuring Voice Aware 802.1x Security

You use the voice aware 802.1x security feature on the switch to disable only the VLAN on which a security violation occurs, whether it is a data or voice VLAN. You can use this feature in IP phone deployments where a PC is connected to the IP phone. A security violation found on the data VLAN results in the shutdown of only the data VLAN. The traffic on the voice VLAN flows through the switch without interruption.

Follow these guidelines to configure voice aware 802.1x voice security on the switch:

- You enable voice aware 802.1x security by entering the **errdisable detect cause security-violation shutdown vlan** global configuration command. You disable voice aware 802.1x security by entering the **no** version of this command. This command applies to all 802.1x-configured ports in the switch.

Note If you do not include the **shutdown vlan** keywords, the entire port is shut down when it enters the error-disabled state.

- If you use the **errdisable recovery cause security-violation** global configuration command to configure error-disabled recovery, the port is automatically re-enabled. If error-disabled recovery is not configured for the port, you re-enable it with the **shutdown** and **no-shutdown** interface configuration commands.
- You can re-enable individual VLANs with the **clear errdisable interface** *interface-id* **vlan** [*vlan-list*] privileged EXEC command. If you do not specify a range, all VLANs on the port are enabled.

To enable voice aware 802.1x security, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# errdisable detect cause security-violation shutdown vlan`	Shuts down any VLAN on which a security violation error occurs. **Note** If the **shutdown vlan** keywords are not included, the entire port enters the error-disabled state and shuts down.
Step 3	`Switch(config)# errdisable recovery cause security-violation`	(Optional) Enables automatic per-VLAN error recovery.
Step 4	`Switch(config)# errdisable recovery interval` *interval*	(Optional) Sets a recovery interval (in sec). The *interval* range is 30 to 86400. The default is 300 sec.
Step 5	`Switch(config)# end`	Enters exec mode.
Step 6	`Switch# clear errdisable interface` *interface-id* **vlan** [*vlan-list*]	(Optional) Reenables individual VLANs that have been error disabled. • For *interface-id* specify the port on which to reenable individual VLANs. • (Optional) For *vlan-list* specify a list of VLANs to be re-enabled. If *vlan-list* is not specified, all VLANs are re-enabled.
Step 7	`Switch(config)# interface` *interface-id*	Enters interface configuration mode.
Step 8	`Switch(config-if)# shutdown no-shutdown`	(Optional) Re-enables an error-disabled VLAN, and clears all error-disable indications.
Step 9	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 10	`Switch# show errdisable detect`	Verifies your settings.
Step 11	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

```
Switch# configure terminal
Switch(config)# errdisable detect cause security-violation shutdown vlan
Switch(config)# errdisable recovery cause security-violation
Switch(config)# errdisable recovery interval interval
Switch(config)# end
```

```
Switch# clear errdisable interface interface-id vlan [vlan-list]
Switch(config)# interface interface-id
Switch(config-if)# shutdown
Switch(config-if)# end
Switch# show errdisable detect
Switch# copy running-config startup-config
```

This example shows how to configure the switch to shut down any VLAN on which a security violation error occurs:

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

This example shows how to re-enable all VLANs that were error disabled on port Gi4/0/2:

```
Switch# clear errdisable interface GigabitEthernet4/0/2 vlan
```

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

Configuring 802.1X with VLAN Assignment

For enabling dynamic VLAN assignment, no additional configuration is required in the switch. For information on configuring Multiple- authentication (MDA), refer to the "Configuring Multiple Domain Authentication and Multiple Authorization" section on page 46-33. To enable VLAN assignment, you must configure the Cisco ACS server.

Note 802.1x authentication with VLAN assignment is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN Membership Policy Server (VMPS).

To enable 802.1X with VLAN assignment, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface interface-id`	Enters interface configuration mode.
Step 3	`Switch(config-if)# switchport access vlan-id`	Sets the VLAN for a switched interface in access mode.
Step 4	`Switch(config-if)# switchport mode access`	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
Step 5	`Switch(config-if)# switchport voice vlan vlan-id`	Sets the voice VLAN for the interface.
Step 6	`Switch(config-if)# authentication host-mode multi-domain`	Enables MDA on the interface.
Step 7	`Switch(config-if)# authentication port-control auto`	Enables 802.1X authentication on the interface.
Step 8	`Switch(config-if)# dot1x pae authenticator`	Enables 802.1X authentication on the port with default parameters. Refer to the "Default 802.1X Configuration" section on page 46-26.
Step 9	`Switch(config)# end`	Returns to privileged EXEC mode.

	Command	Purpose
Step 10	`Switch# show dot1x interface interface-id details`	(Optional) Verifies your entries.
Step 11	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

The following example shows how to configure MDA on an interface and 802.1X as the authentication mechanism:

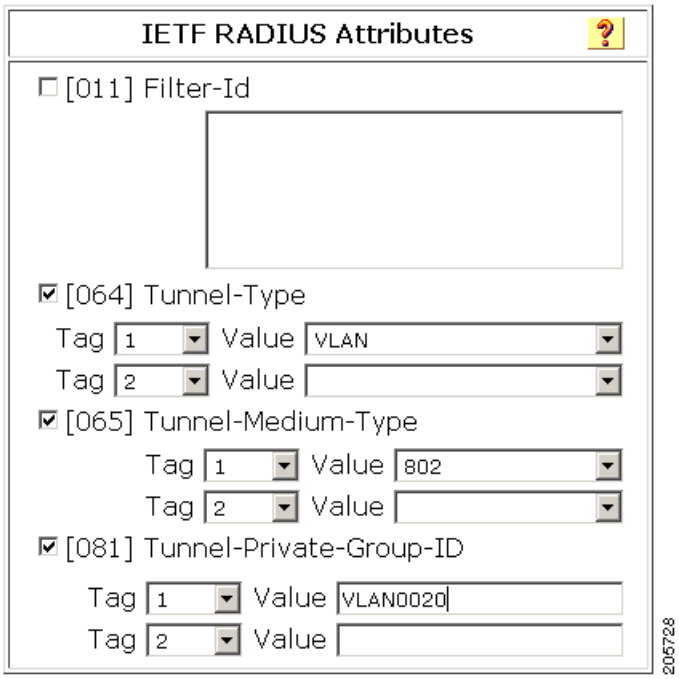
```
Switch(config)# interface FastEthernet3/3
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 16
Switch(config-if)# authentication host-mode multi-domain
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# end
```

Note You must configure VLAN assignment in the ACS server. No configuration changes are required on the switch.

Cisco ACS Configuration for VLAN Assignment

The procedure for enabling MDA with voice VLAN assignment is the same as that for activating MDA except for one step: Configure a VLAN for dynamic VLAN assignment after selecting **User > IETF RADIUS Attributes** (Figure 46-16). This step ensures correct functioning of the ACS configuration required for dynamic VLAN assignment.

Figure 46-16 User Set Up



Note The procedure is the same for voice devices except that the AAA server must be configured to send a Cisco Attribute-Value (AV) pair attribute with a value of device-traffic-class=voice.

Enabling Fallback Authentication

On a port in multiauthentication mode, either or both of MAB and web-based authentication can be configured as fallback authentication methods for non-802.1X hosts (those that do not respond to EAPOL). You can configure the order and priority of the authentication methods.

For detailed configuration information for MAB, see the "Configuring 802.1X with MAC Authentication Bypass" section on page 46-59.

For detailed configuration information for web-based authentication, see Chapter 48, "Configuring Web-Based Authentication."

Note When web-based authentication and other authentication methods are configured on an MDA or multiauthentication port, downloadable ACL policies must be configured for all devices attached to that port.

To enable fallback authentication, perform this task:

	Command	Purpose
Step 1	`Switch(config)# ip admission name rule-name proxy http`	Configures an authentication rule for web-based authentication.
Step 2	`Switch(config)# fallback profile profile-name`	Creates a fallback profile for web-based authentication.
Step 3	`Switch(config-fallback-profile)# ip access-group rule-name in`	Specifies the default ACL to apply to network traffic before web-based authentication.
Step 4	`Switch(config-fallback-profile)# ip admission name rule-name`	Associates an IP admission rule with the profile and specifies that a client connecting by web-based authentication uses this rule.
Step 5	`Switch(config-fallback-profile)# exit`	Returns to global configuration mode.
Step 6	`Switch(config)# interface type slot/port`	Specifies the port to be configured and enters interface configuration mode. *type* = **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

Step 7	Cisco IOS Release 12.2(50)SG and later
	`Switch(config-if)# authentication port-control auto`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x port-control auto`
		Enables authentication on the port.

Step 8	`Switch(config-if)# authentication order method1 [method2] [method3]`	(Optional) Specifies the fallback order of authentication methods to be used. The three values of *method*, in the default order, are **dot1x**, **mab**, and **webauth**. The specified order also determines the relative priority of the methods for reauthentication (highest to lowest).

	Command	Purpose
Step 9	`Switch(config-if)# authentication priority method1 [method2] [method3]`	(Optional) Overrides the relative priority of authentication methods to be used. The three values of *method*, in the default order of priority, are **dot1x**, **mab**, and **webauth**.
Step 10	`Switch(config-if)# authentication event fail action next-method`	Specifies that the next configured authentication method be applied if authentication fails.

Step 11	Cisco IOS Release 12.2(50)SG and later
	`Switch(config-if)# mab [eap]`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x mac-auth-bypass [eap]`
		Enables MAC authentication bypass. The optional **eap** keyword specifies that the EAP extension be used during RADIUS authentication.

Step 12	`Switch(config-if)# authentication fallback profile-name`	Enables web-based authentication using the specified profile.
Step 13	`Switch(config-if)# authentication violation [shutdown | restrict]`	(Optional) Configures the disposition of the port if a security violation occurs. The default action is to shut down the port. If the **restrict** keyword is configured, the port does not shut down, but trap entries are installed for the violating MAC address, and traffic from that MAC address is dropped.
Step 14	`Switch(config-if)# authentication timer inactivity {seconds | server}`	(Optional) Configures the inactivity timeout value for MAB and 802.1X. By default, inactivity aging is disabled for a port. • *seconds*—Specifies inactivity timeout period. The range is from 1 to 65535 seconds. • server—Specifies that the inactivity timeout period value be obtained from the authentication server.
Step 15	`Switch(config-if)# authentication timer restart seconds`	(Optional) Specifies a period after which the authentication process restarts in an attempt to authenticate an unauthorized port. • *seconds*—Specifies the restart period. The range is from 1 to 65535 seconds.
Step 16	`Switch(config-if)# exit`	Returns to global configuration mode.
Step 17	`Switch(config)# ip device tracking`	Enables the IP device tracking table, which is required for web-based authentication.
Step 18	`Switch(config)# exit`	Returns to privileged EXEC mode.
Step 19	`Switch# show dot1x interface type slot/port`	Verifies your entries.

This example shows how to enable 802.1X fallback to MAB, and then to enable web-based authentication, on an 802.1X-enabled port:

```
Switch(config)# ip admission name rule1 proxy http
Switch(config)# fallback profile fallback1
Switch(config-fallback-profile)# ip access-group default-policy in
Switch(config-fallback-profile)# ip admission rule1
Switch(config-fallback-profile)# exit
Switch(config)# interface gigabit5/9
```

```
Switch(config-if)# switchport mode access
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication order dot1x mab webauth
Switch(config-if)# mab eap
Switch(config-if)# authentication fallback fallback1
Switch(config-if)# exit
Switch(config)# ip device tracking
Switch(config)# exit
```

To determine if a host was authenticated using 802.1X when fallback authentication is configured on the port, enter the following commands:

```
Switch# show authentication sessions interface g7/2

            Interface:  GigabitEthernet7/2
          MAC Address:  0060.b057.4687
           IP Address:  Unknown
            User-Name:  test2
               Status:  Authz Success
               Domain:  DATA
      Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A8013F0000000901BAB560
      Acct Session ID:  0x0000000B
               Handle:  0xE8000009

Runnable methods list:
       Method   State
       dot1x    Authc Success
       mab      Not run

Switch# show dot1x interfaces g7/2 detail

Dot1x Info for GigabitEthernet7/2
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_AUTH
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 2

Dot1x Authenticator Client List
-------------------------------
Supplicant                = 0060.b057.4687
Session ID                = C0A8013F0000000901BAB560
    Auth SM State         = AUTHENTICATED
    Auth BEND SM State    = IDLE
Port Status               = AUTHORIZED
```

To determine if a host was authenticated using MAB when fallback authentication is configured on the port, enter the following commands:

```
Switch# show authentication sessions interface g7/2

            Interface:  GigabitEthernet7/2
          MAC Address:  0060.b057.4687
           IP Address:  192.168.22.22
            User-Name:  0060b0574687
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A8013F0000000B01BBD278
      Acct Session ID:  0x0000000D
               Handle:  0xF500000B

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success

Switch# show mab interface g7/2 detail

MAB details for GigabitEthernet7/2
-------------------------------------
Mac-Auth-Bypass           = Enabled


MAB Client List
---------------
Client MAC                = 0060.b057.4687
Session ID                = C0A8013F0000000B01BBD278
MAB SM state              = TERMINATE
Auth Status               = AUTHORIZED
```

To determine if a host was authenticated using web authentication when fallback authentication is configured on the port, enter the following commands:

```
Switch# show authentication sessions interface G4/3
            Interface:  GigabitEthernet4/3
          MAC Address:  0015.e981.0531
           IP Address:  10.5.63.13
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A053F0F0000000200112FFC
      Acct Session ID:  0x00000003
               Handle:  0x09000002

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Failed over
       webauth  Authc Success
```

```
Switch# show ip admission cache
Authentication Proxy Cache
Total Sessions: 1 Init Sessions: 0
 Client IP 10.5.63.13 Port 4643, timeout 1000, state ESTAB
```

Cisco IOS Release 12.2(46)SG or earlier

```
Switch(config)# ip admission name rule1 proxy http
Switch(config)# fallback profile fallback1
Switch(config-fallback-profile)# ip access-group default-policy in
Switch(config-fallback-profile)# ip admission rule1
Switch(config-fallback-profile)# exit
Switch(config)# interface gigabit5/9
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication order dot1x mab webauth
Switch(config-if)# dot1x mac-auth-bypass eap
Switch(config-if)# adot1x fallback fallback1
Switch(config-if)# exit
Switch(config)# ip device tracking
Switch(config)# exit
```

Enabling Periodic Reauthentication

You can enable periodic 802.1X client reauthentication and specify how often it occurs. If you do not specify a time value before enabling reauthentication, the interval between reauthentication attempts is 3600 seconds.

Automatic 802.1X client reauthentication is a per-interface setting and can be set for clients connected to individual ports. To manually reauthenticate the client connected to a specific port, see the "Changing the Quiet Period" section on page 46-83.

To enable periodic reauthentication of the client and to configure the number of seconds between reauthentication attempts, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface` *interface-id*	Enters interface configuration mode and specifies the interface to be enabled for periodic reauthentication.
Step 3	`Switch(config-if)# switchport mode access`	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
Step 4	`Switch(config-if)# dot1x pae authenticator`	Enables 802.1X authentication on the port with default parameters. Refer to the "Default 802.1X Configuration" section on page 46-26.

Step 5	Cisco IOS Release 12.2(50)SG and later
	`Switch(config-if)# authentication periodic`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x reauthentication`
		Enables periodic reauthentication of the client, which is disabled by default.
		To disable periodic reauthentication, use the **no authentication periodic** interface configuration command (for earlier releases, use the **no dot1x reauthentication** interface configuration command).

	Command	Purpose

Step 6	Cisco IOS Release 12.2(50)SG and later
	`Switch(config-if)# authentication timer reauthenticate {seconds | server}`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x timeout reauth-period {seconds | server}`
		Specifies the number of seconds between reauthentication attempts or have the switch use a RADIUS-provided session timeout.
		The range is 1 to 65,535; the default is 3600 seconds.
		To return to the default number of seconds between reauthentication attempts, use the **no authentication timer reauthenticate** global configuration command (for earlier releases, use the **dot1x timeout reauth-attempts** command).
		This command affects the behavior of the switch only if periodic reauthentication is enabled.

Step 7	Cisco IOS Release 12.2(50)SG and later
	`Switch(config-if)# authentication port-control auto`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x port-control auto`
		Enables 802.1X authentication on the interface.

Step 8	`Switch(config-if)# end`	Returns to privileged EXEC mode.

This example shows how to enable periodic reauthentication and set the number of seconds between reauthentication attempts to 4000:

Cisco IOS Release 12.2(50)SG and later

```
Switch# configure terminal
Switch(config)# interface fastethernet5/9
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication periodic
Switch(config-if)# authentication timer reauthenticate 4000
Switch(config-if)# authentication port-control auto
Switch(config-if)# end
Switch#
```

Cisco IOS Release 12.2(46)SG or earlier

```
Switch# configure terminal
Switch(config)# interface fastethernet5/9
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

Enabling Multiple Hosts

You can attach multiple hosts (clients) to a single 802.1X-enabled port as shown in Figure 46-9 on page 46-25. In this mode, when the port is authorized, all other hosts that are indirectly attached to the port are granted access to the network. If the port becomes unauthorized (reauthentication fails or an EAPOL-logoff message is received), the switch denies access to the network for all wireless access point-attached clients.

To allow multiple hosts (clients) on an 802.1X-authorized port that has the **dot1x port-control** interface configuration command set to **auto**, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface interface-id`	Enters interface configuration mode and specifies the interface to which multiple hosts are indirectly attached.
Step 3	`Switch(config-if)# switchport mode access`	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
Step 4	`Switch(config-if)# dot1x pae authenticator`	Enables 802.1X authentication on the port with default parameters. Refer to the "Default 802.1X Configuration" section on page 46-26.

Step 5	Cisco IOS Release 12.2(50)SG and later
	`Switch(config-if)# authentication host-mode multi-host`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x host-mode multi-host`
		Allows multiple hosts (clients) on an 802.1X-authorized port.
		Note Ensure that the **dot1x port-control** interface configuration command set is set to **auto** for the specified interface.
		
		To disable multiple hosts on the port, use the **no authentication host-mode multi-host** interface configuration command (for earlier releases, use the **no dot1x host-mode multi-host** interface configuration command).

Step 6	Cisco IOS Release 12.2(50)SG and later
	`Switch(config-if)# authentication port-control auto`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x port-control auto`
		Enables 802.1X authentication on the interface.

Step 7	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 8	`Switch# show dot1x all interface interface-id`	Verifies your entries.
Step 9	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

This example shows how to enable 802.1X on Fast Ethernet interface 5/9 and to allow multiple hosts:

Cisco IOS Release 12.2(50)SG and later

```
Switch# configure terminal
Switch(config)# interface fastethernet5/9
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication host-mode multi-host
Switch(config-if)# authentication port-control auto
Switch(config-if)# end
Switch#
```

Cisco IOS Release 12.2(46)SG or earlier

```
Switch# configure terminal
Switch(config)# interface fastethernet5/9
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
```

```
Switch(config-if)# dot1x host-mode multi-host
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

Changing the Quiet Period

When the switch cannot authenticate the client, the switch remains idle for a set period of time, and then tries again. The idle time is determined by the **quiet-period** value. A failed authentication of the client might occur because the client provided an invalid password. You can provide a faster response time to the user by entering a number smaller than the default.

To change the quiet period, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface interface-id`	Enters interface configuration mode and specifies the interface to be enabled for timeout **quiet-period**.
Step 3	`Switch(config-if)# switchport mode access`	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
Step 4	`Switch(config-if)# dot1x pae authenticator`	Enables 802.1X authentication on the port with default parameters. Refer to the "Default 802.1X Configuration" section on page 46-26.
Step 5	`Switch(config-if)# dot1x timeout quiet-period seconds`	Sets the number of seconds that the switch remains in the **quiet-period** following a failed authentication exchange with the client. To return to the default quiet-period, use the **no dot1x timeout quiet-period** configuration command. The range is 0 to 65,535 seconds; the default is 60.
Step 6	`Switch(config-if)# authentication port-control auto`	Enables 802.1X authentication on the interface.
Step 7	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 8	`Switch# show dot1x all`	Verifies your entries.
Step 9	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

This example shows how to set the quiet period on the switch to 30 seconds:

Cisco IOS Release 12.2(50)SG and later

```
Switch# configure terminal
Switch(config)# interface fastethernet4/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x timeout quiet-period 30
Switch(config-if)# authentication port-control auto
Switch(config-if)# end
Switch#
```

Cisco IOS Release 12.2(46)SG or earlier

```
Switch# configure terminal
Switch(config)# interface fastethernet4/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x timeout quiet-period 30
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

Changing the Switch-to-Client Retransmission Time

The client responds to the EAP-request/identity frame from the switch with an EAP-response/identity frame. If the switch does not receive this response, it waits a set period of time (known as the retransmission time) and then retransmits the frame.

Note 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.

To change the amount of time that the switch waits for client notification, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface` *interface-id*	Enters interface configuration mode and specifies the interface to be enabled for timeout tx-period.
Step 3	`Switch(config-if)# switchport mode access`	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
Step 4	`Switch(config-if)# dot1x pae authenticator`	Enables 802.1X authentication on the port with default parameters. Refer to the "Default 802.1X Configuration" section on page 46-26.
Step 5	`Switch(config-if)# dot1x timeout tx-period` *seconds*	Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is 1 to 65,535 seconds; the default is 30. To return to the default retransmission time, use the **no dot1x timeout tx-period** interface configuration command.

Step 6	Cisco IOS Release 12.2(50)SG and later
	`Switch(config-if)# authentication port-control auto`
	
	Cisco IOS Release 12.2(46)SG or earlier releases
	`Switch(config-if)# dot1x port-control auto`
		Enables 802.1X authentication on the interface.

Step 7	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 8	`Switch# show dot1x all`	Verifies your entries.
Step 9	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

This example shows how to set the retransmission time to 60 seconds:

Cisco IOS Release 12.2(50)SG and later

```
Switch# configure terminal
Switch(config)# interface fastethernet5/9
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# authentication port-control auto
Switch(config-if)# end
Switch#
```

Cisco IOS Release 12.2(46)SG or earlier

```
Switch# configure terminal
Switch(config)# interface fastethernet5/9
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

Setting the Switch-to-Client Frame-Retransmission Number

In addition to changing the switch-to-client retransmission times, you can change the number of times that the switch sends EAP-Request/Identity and other EAP-Request frames to the client before restarting the authentication process. The number of EAP-Request/Identity retransmissions is controlled by the **dot1x max-reauth-req** command; the number of retransmissions for other EAP-Request frames is controlled by the **dot1x max-req** command.

Note You should change the default values of these commands only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

To set the switch-to-client frame-retransmission numbers, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface` *interface-id*	Enters interface configuration mode and specifies the interface to be enabled for **max-reauth-req and/or max-req**.
Step 3	`Switch(config-if)# switchport mode access`	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
Step 4	`Switch(config-if)# dot1x pae authenticator`	Enables 802.1X authentication on the port with default parameters. Refer to the "Default 802.1X Configuration" section on page 46-26.

	Command	Purpose
Step 5	`Switch(config-if)# dot1x max-req` *count* or `Switch(config-if)#` **dot1x max-reauth-req** *count*	Specifies the number of times EAPOL DATA packets are retransmitted (if lost or not replied to). For example, if you have a supplicant that is authenticating and it experiences a problem, the authenticator retransmits requests for data three times before abandoning the authentication request. The range for *count* is 1 to 10; the default is 2. Specifies the timer for EAPOL-Identity-Request frames (only). If you plug in a device incapable of 802.1X, three EAPOL-Id-Req frames are sent before the state machine resets. Alternatively, if you have configured Guest-VLAN, three frames are sent before the port is enabled. This parameter has a default value of 2. To return to the default retransmission number, use the **no dot1x max-req** and **no dot1x max-reauth-req** global configuration command.
Step 6	`Switch(config-if)# authentication port-control auto`	Enables 802.1X authentication on the interface.
Step 7	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 8	`Switch# show dot1x all`	Verifies your entries.
Step 9	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

This example shows how to set 5 as the number of times that the switch retransmits an EAP-request/identity request before restarting the authentication process:

Cisco IOS Release 12.2(50)SG and later

```
Switch# configure terminal
Switch(config)# interface fastethernet5/9
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x max-reauth-req 5
Switch(config-if)# authentication port-control auto
Switch(config-if)# end
Switch#
```

Cisco IOS Release 12.2(46)SG or earlier

```
Switch# configure terminal
Switch(config)# interface fastethernet5/9
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x max-reauth-req 5
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

Configuring an Authenticator and a Supplicant Switch with NEAT

Configuring NEAT requires that one switch outside a wiring closet is configured as a supplicant and is connected to an authenticator switch.

This section includes these topics:

- Configuring NEAT with ASP, page 46-91
- Configuration Guidelines, page 46-91

Note For overview information, see the "802.1X Supplicant and Authenticator Switches with Network Edge Access Topology" section on page 46-23.

Configuring Switch as an Authenticator

To configure a switch as an authenticator, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# cisp enable`	Enables CISP.
Step 3	`Switch(config)# interface` *interface-id*	Specifies the port to be configured, and enter interface configuration mode.
Step 4	`Switch(config-if)# switchport mode access`	Sets the port mode to access.
Step 5	`Switch(config-if)# authentication port-control auto`	Sets the port-authentication mode to auto.
Step 6	`Switch(config-if)# dot1x pae authenticator`	Configures the interface as a port access entity (PAE) authenticator.
Step 7	`Switch(config-if)# spanning-tree portfast`	Enables Port Fast on an access port connected to a single workstation or server.
Step 8	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 9	`Switch# show running-config interface` *interface-id*	Verifies your configuration.
Step 10	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

When CISP is enabled on a trunk port, the following features are inert. When CISP is neither running nor configured, these features operate as expected:

- VLAN assignment
- Guest, Authentication Failure, voice, and critical VLANs
- Critical authentication
- Wake-on-LAN
- Web authentication
- Port security
- Violation modes (restrict, shut down, and shut down VLAN)

The following example shows how to enable CISP on a port. You must configure the following procedure in the Cisco ACS server. Configuring a user with Cisco AV Pair value, allows SSW to authenticate itself with the ASW. Because the user is attached with the AV pair value, upon successful authentication on ASW, the macro is executed on the interface on which SSW is authenticated:

```
Switch# configure terminal
Switch(config)# cisp enable
```

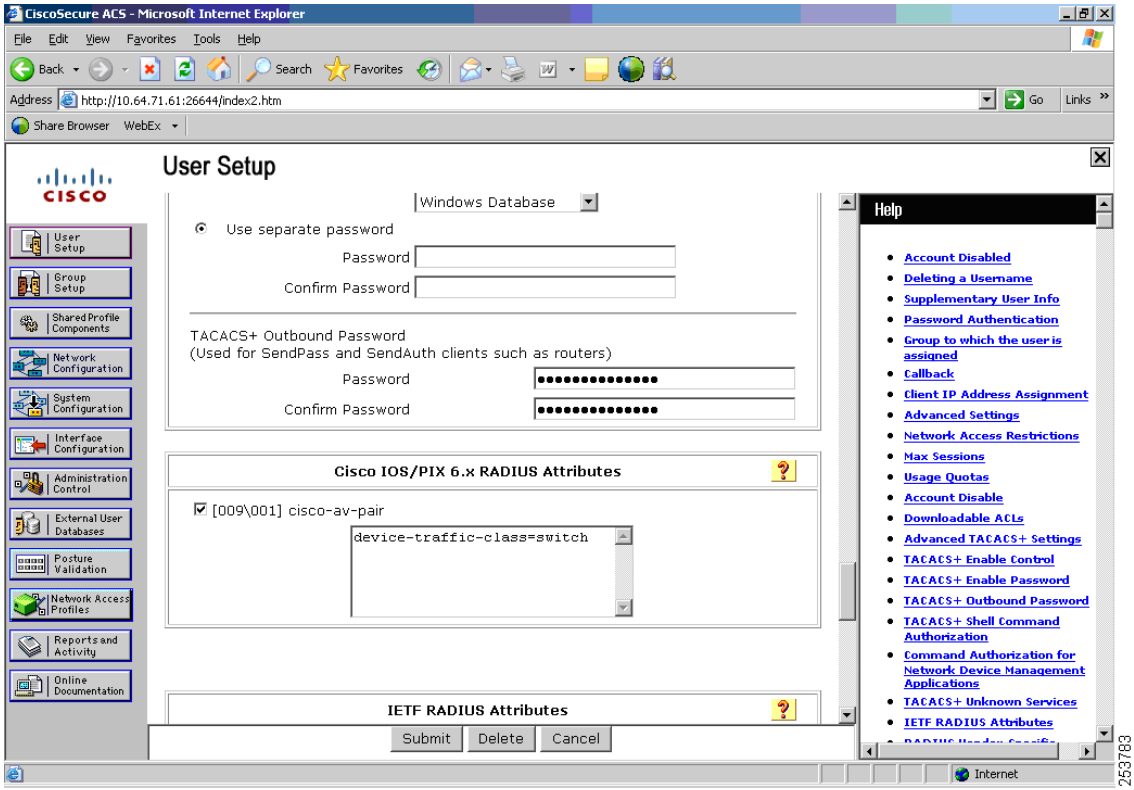
```
Switch(config)# interface GigabitEthernet5/23
Switch(config-if)# switchport mode access
Switch(config-if)# spanning-tree portfast
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication port-control auto
```

Cisco AV Pair Configuration

Next, you need to configure a Cisco AV pair value.

Log into ACS, and Select/Create a User. Go to User Setup and scroll down to the **[009\001] cisco-av-pair** Tab. Enter **device-traffic-class=switch** (Figure 46-17).

Figure 46-17 Specifying the Cisco AV Pair



Starting with Cisco IOS XE Release 3.2.0 SG (15.0(2)SG) the spanning-tree bpduguard feature is automatically disabled or enabled as part of a macro provided it was previously enabled in the port configuration. If the configuration did not have BPDU Guard enabled before the supplicant switch was authenticated, the spanning-tree bpduguard feature is not applied to the macro.

Note Disabling spanning-tree bpduguard happens only if it was previously enabled through the **port level** command. Enabling it globally without a specific port level CLI prevents NEAT from disabling it on the port after the authenticator switch receives a device-traffic-class=switch AV Pair and applies the macro.

There are 2 scenarios:

Scenario 1: With Port Level BPDU Guard Configuration

Before Authorization

```
interface GigabitEthernet5/1
  switchport access vlan 81
  switchport mode access
  dot1x pae authenticator
  authentication port-control auto
  spanning-tree bpduguard enable
end
```

Post Authorization and Application of Internal Macro

```
interface GigabitEthernet5/1
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 81
  switchport mode trunk
  dot1x pae authenticator
  authentication port-control auto
  spanning-tree portfast trunk
  no spanning-tree bpduguard
  end
```

Scenario 2: Without port level BPDU Guard Configuration (with or without globally enabling BPDU Guard)

Before Authorization

```
interface GigabitEthernet5/1
  switchport access vlan 81
  switchport mode access
  dot1x pae authenticator
  authentication port-control auto
end
```

Post Authorization and Application of Internal Macro

```
interface GigabitEthernet5/1
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 81
  switchport mode trunk
  dot1x pae authenticator
  authentication port-control auto
  spanning-tree portfast trunk
  no spanning-tree bpduguard
  end
```

When the authenticator switch receives a device-traffic-class=switch AV pair, the following macro is applied to the authenticator switch port:

```
no switchport access vlan $AVID
no switchport nonegotiate
switchport mode trunk
switchport trunk native vlan $AVID
no spanning-tree bpduguard enable
spanning-tree portfast trunk
```

After the supplicant switch is authenticated as a switch device, the configuration will appear as follows:

```
interface GigabitEthernet5/23
 switchport mode trunk
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast trunk
end
```

Radius Config (Cisco AV Pair value)

```
-------------------------------------------------------
device-traffic-class=switch
```

show running-config interface is the only command that informs you that the smart macro has been applied after the supplicant switch is authenticated:

```
Switch# show authentication session

Interface  MAC Address     Method   Domain   Status         Session ID
Gi5/23     0024.9844.de23  dot1x    DATA     Authz Success  0909117A000000000010561C

Switch# show running-configuration interface gi 5/23

Building configuration...

Current configuration : 149 bytes
!
interface GigabitEthernet5/23
 switchport mode trunk
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast trunk
end

Switch#
```

NEAT changes the port configuration on the authenticator switch. So, to perform ISSU from one version that supports NEAT to another that does not support NEAT, you must first deactivate NEAT on all switch ports for ISSU. Similarly, NEAT cannot activate when ISSU is in progress. If a supplicant switch tries to authenticate during ISSU, authorization would fail on the port.

Configuring Switch as a Supplicant

Note The Catalyst 4500 series switch does not support supplicant switch functionality. The following supplicant specific commands are mentioned for a quick reference. For more details, see the *Catalyst 3750 Switch Software Configuration Guide*.

To configure a switch as a supplicant, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# cisp enable`	Enables CISP.
Step 3	`Switch(config)# dot1x credentials profile`	Creates 802.1x credentials profile. This must be attached to the port that is configured as supplicant.
Step 4	`Switch(config)# sername suppswitch`	Creates a username.
Step 5	`Switch(config)# password password`	Creates a password for the new username.
Step 6	`Switch(config)# dot1x supplicant force-multicast`	Forces the switch to send *only* multicast EAPOL packets when it receives either unicast or multicast packets. This also allows NEAT to work on the supplicant switch in all host modes.

	Command	Purpose
Step 7	`Switch(config)# interface interface-id`	Specifies the port to be configured, and enter interface configuration mode.
Step 8	`Switch(config-if)# switchport trunk encapsulation dot1q`	Sets the port to trunk mode.
Step 9	`Switch(config-if)# switchport mode trunk`	Configures the interface as a VLAN trunk port.
Step 10	`Switch(config-if)# dot1x pae supplicant`	Configures the interface as a port access entity (PAE) supplicant.
Step 11	`Switch(config-if)# dot1x credentials profile-name`	Attaches the 802.1x credentials profile to the interface.
Step 12	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 13	`Switch# show running-config interface interface`	Verifies your configuration. **Note** it is the only command that tells you that the smart macro has been applied after the supplicant switch has been authenticated.
Step 14	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

This example shows how to configure a switch as a supplicant:

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# dot1x credentials test
Switch(config)# username suppswitch
Switch(config)# password myswitch
Switch(config)# dot1x supplicant force-multicast
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# dot1x pae supplicant
Switch(config-if)# dot1x credentials test
Switch(config-if)# end
```

The following macro is applied to the authenticator switch port after the supplicant switch is deauthenticated due to a link-down or a reauthenticating event:

```
no switchport nonegotiate
switchport mode access
no switchport trunk native vlan $AVID
no spanning-tree portfast trunk
switchport access vlan $AVID
spanning-tree bpduguard enable
spanning-tree portfast
```

Configuring NEAT with ASP

You can also use an AutoSmart Ports user-defined macro rather than a switch VSA to configure the authenticator switch. For more information, see the Chapter 20, “Configuring Cisco IOS Auto Smartport Macros.”

Configuration Guidelines

- If BPDU Guard was enabled prior to supplicant switch authentication, it is re-enabled after the supplicant switch unauthenticates.

- You can configure NEAT ports and non-NEAT ports with the same configuration. When the supplicant switch authenticates, the port mode is changed from access to trunk based on the switch vendor-specific attributes (device-traffic-class=switch).
- To enable NEAT, you must configure the vendor-specific attributes (VSA) attribute as switch. Configuring the trunk with an 802.1X configuration and enabling CISP globally will not enable NEAT.
- VSA device-traffic-class=switch assists the authenticator switch in identifying the supplicant as a switch-device. This identification changes the authenticator switch port mode from access to trunk and enables 802.1X trunk encapsulation. The access VLAN, if any, is converted to a native trunk VLAN. VSA does not change any of the port configurations on the supplicant.
- Although modified trunk parameters are retained, when the trunk link is down or authentication is cleared, the interface is reconfigured to the following:
  - **spanning-tree portfast**
  - **switchport mode access**
  - **switchport access vlan** *access-vlan-id*

Note *access-vlan-id* is derived from the **switchport trunk native vlan** *x* command entered on the interface. If you have modified the trunk native VLAN, the configured native VLAN is used as the access-vlan-id when the port returns to access mode.

- We recommend using 802.1X authentication mode single-host for NEAT configuration on the interface.
- The cisco-av-pairs must be configured as device-traffic-class=switch on the ACS. This sets the interface as a trunk after the supplicant is successfully authenticated.
- You should not modify the trunk mode configurations that are based on *device-traffic-class* either manually or through features such as AutoSmart Ports. it is because 802.1X configuration is not supported for trunk ports.
- To change the host mode and apply a standard port configuration on the authenticator switch port, you can also use AutoSmart ports user-defined macros rather than the switch VSA. Doing this allows you to remove unsupported configurations on the authenticator switch port and to change the port mode from access to trunk. For details, see Chapter 20, “Configuring Cisco IOS Auto Smartport Macros.”

Note Configuring only the Auto SmartPorts macro does not identify the end host as a supplicant switch. The switch VSA is required to identify the supplicant switch. However, when Auto Smartports macro is configured, the internal macro that reconfigures the port from access to trunk is not executed and the Auto Smartports macro should ensure that the port reconfigures as a trunk port.

Manually Reauthenticating a Client Connected to a Port

You can manually reauthenticate a client connected to a specific port at any time by entering the **dot1x re-authenticate interface** privileged EXEC command. If you want to enable or disable periodic reauthentication, see the "Enabling Periodic Reauthentication" section on page 46-80.

This example shows how to manually reauthenticate the client connected to Fast Ethernet port 1/1:

```
Switch# dot1x re-authenticate interface fastethernet1/1
Starting reauthentication on FastEthernet1/1
```

Initializing the 802.1X Authentication State

The **dot1x initialize** command causes the authentication process to be restarted regardless of its current state.

This example shows how to restart the authentication process on Fast Ethernet port 1/1:

```
Switch# dot1x initialize interface fastethernet1/1
```

This example shows how to restart the authentication process on all ports of the switch:

```
Switch# dot1x initialize
```

Removing 802.1X Client Information

The **clear dot1x** command causes all existing supplicants to be completely deleted from an interface or from all the interfaces on a switch.

This example shows how to remove 802.1X client information on Fast Ethernet port 1/1:

```
Switch# clear dot1x interface fastethernet1/1
```

This example shows how to remove 802.1X client information on all ports of the switch:

```
Switch# clear dot1x all
```

Resetting the 802.1X Configuration to the Default Values

To reset the 802.1X configuration to the default values, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# dot1x default`	Resets the configurable 802.1X parameters to the default values.
Step 3	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 4	`Switch# show dot1x all`	Verifies your entries.
Step 5	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Controlling Switch Access with RADIUS

This section describes how to enable and configure the RADIUS, which provides detailed accounting information and flexible administrative control over authentication and authorization processes. RADIUS is facilitated through AAA and can be enabled only through AAA commands.

Note For complete syntax and usage information for the commands used in this section, see the *Cisco IOS Security Command Reference, Release 12.2*.

These sections contain this configuration information:

Understanding RADIUS

RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported Cisco routers and switches. Clients send authentication requests to a central RADIUS server, which contains all user authentication and network service access information. The RADIUS host is normally a multiuser system running RADIUS server software from Cisco (Cisco Secure Access Control Server Version 3.0), Livingston, Merit, Microsoft, or another software provider. For more information, see the RADIUS server documentation.

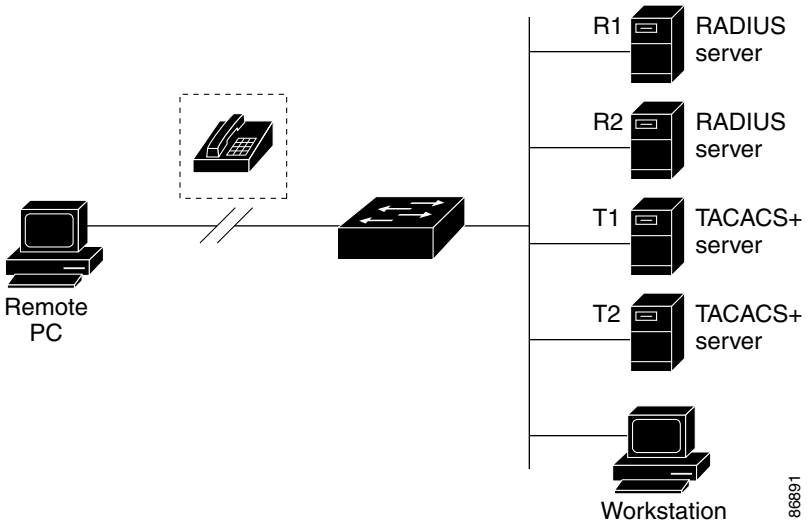
Use RADIUS in these network environments that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server that has been customized to work with the Kerberos security system.
- Turnkey network security environments in which applications support the RADIUS protocol, such as in an access environment that uses a *smart card* access control system. In one case, RADIUS has been used with Enigma's security cards to validates users and to grant access to network resources.
- Networks already using RADIUS. You can add a Cisco switch containing a RADIUS client to the network. This might be the first step when you make a transition to a TACACS+ server. See Figure 46-18 on page 46-95.
- Network in which the user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to the network through a protocol such as IEEE 802.1X.
- Networks that require resource accounting. You can use RADIUS accounting independently of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, showing the amount of resources (such as time, packets, bytes, and so forth) used during the session. An Internet service provider might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

RADIUS is not suitable in these network security situations:

- Multiprotocol access environments. RADIUS does not support AppleTalk Remote Access (ARA), NetBIOS Frame Control Protocol (NBFCP), NetWare Asynchronous Services Interface (NASI), or X.25 PAD connections.
- Switch-to-switch or router-to-router situations. RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one device to a non-Cisco device if the non-Cisco device requires authentication.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

Figure 46-18 Transitioning from RADIUS to TACACS+ Services



RADIUS Operation

When a user attempts to log in and authenticate to a switch that is access controlled by a RADIUS server, these events occur:

1. The user is prompted to enter a username and password.
2. The username and encrypted password are sent over the network to the RADIUS server.
3. The user receives one of these responses from the RADIUS server:
   a. ACCEPT—The user is authenticated.
   b. REJECT—The user is either not authenticated and is prompted to re-enter the username and password, or access is denied.
   c. CHALLENGE—A challenge requires additional data from the user.
   d. CHALLENGE PASSWORD—A response requests the user to select a new password.

The ACCEPT or REJECT response is bundled with additional data that is used for privileged EXEC or network authorization. Users must first successfully complete RADIUS authentication before proceeding to RADIUS authorization, if it is enabled. The additional data included with the ACCEPT or REJECT packets includes these items:

- Telnet, SSH, rlogin, or privileged EXEC services
- Connection parameters, including the host or client IP address, access list, and user timeouts

RADIUS Change of Authorization

This section provides an overview of the RADIUS interface including available primitives and how they are used during a Change of Authorization (CoA).

Overview

A standard RADIUS interface is typically used in a pulled model where the request originates from a network attached device and the response come from the queried servers. Catalyst switches support the RADIUS Change of Authorization (CoA) extensions defined in RFC 5176 that are typically used in a pushed model and allow for the dynamic reconfiguring of sessions from external authentication, authorization, and accounting (AAA) or policy servers.

The switch supports these per-session CoA requests:

- Session reauthentication
- Session termination
- Session termination with port shut down
- Session termination with port bounce

The RADIUS interface is enabled by default on Catalyst switches.

Change-of-Authorization Requests

Change of Authorization (CoA) requests, as described in RFC 5176, are used in a push model to allow for session identification, host reauthentication, and session termination. The model is comprised of one request (CoA-Request) and two possible response codes:

- CoA acknowledgement (ACK) [CoA-ACK]
- CoA non-acknowledgement (NAK) [CoA-NAK]

The request is initiated from a CoA client (typically a RADIUS or policy server) and directed to the switch that acts as a listener.

This section includes these topics:

RFC 5176 Compliance

The Disconnect Request message, which is also referred to as Packet of Disconnect (POD), is supported by the switch for session termination.

Table 46-2 shows the IETF attributes are supported for this feature.

Table 46-2 Supported IETF Attributes

Attribute Number	Attribute Name
24	State
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

Table 46-3 shows the possible values for the Error-Cause attribute.

Table 46-3 Error-Cause Values

Value	Explanation
201	Residual Session Context Removed
202	Invalid EAP Packet (Ignored)
401	Unsupported Attribute
402	Missing Attribute
403	NAS Identification Mismatch
404	Invalid Request
405	Unsupported Service
406	Unsupported Extension
407	Invalid Attribute Value
501	Administratively Prohibited
502	Request Not Routable (Proxy)
503	Session Context Not Found
504	Session Context Not Removable
505	Other Proxy Processing Error
506	Resources Unavailable
507	Request Initiated
508	Multiple Session Selection Unsupported

Preconditions

To use the CoA interface, a session must already exist on the switch. CoA can be used to identify a session and enforce a disconnect request. The update affects only the specified session.

CoA Request Response Code

The CoA Request response code can be used to convey a command to the switch. The supported commands are listed in Table 46-4 on page 46-99.

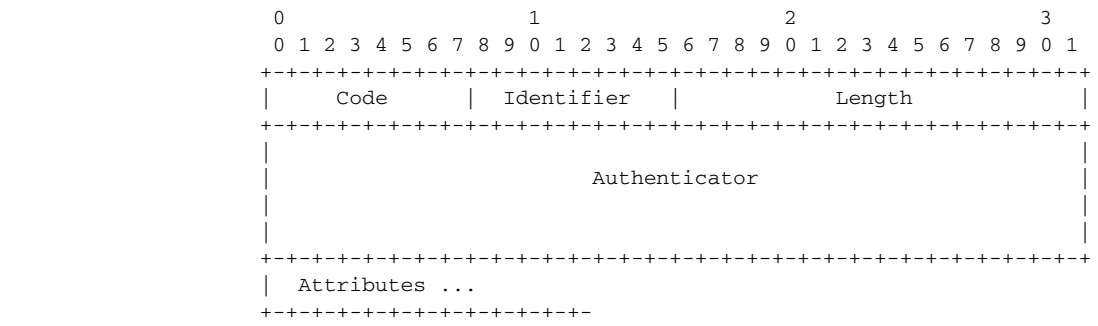
Session Identification

For disconnect and CoA requests targeted at a particular session, the switch locates the session based on one or more of the following attributes:

- Calling-Station-Id (IETF attribute #31 which contains the host MAC address)
- Audit-Session-Id (Cisco VSA)
- Acct-Session-Id (IETF attribute #44)

Unless all session identification attributes included in the CoA message match the session, the switch returns a Disconnect-NAK or CoA-NAK with the "Invalid Attribute Value" error-code attribute.

The packet format for a CoA Request code as defined in RFC 5176 consists of the fields: Code, Identifier, Length, Authenticator, and Attributes in Type:Length:Value (TLV) format.



The attributes field is used to carry Cisco VSAs.

CoA ACK Response Code

If the authorization state is changed successfully, a positive acknowledgement (ACK) is sent. The attributes returned within CoA ACK will vary based on the CoA Request and are discussed in individual CoA Commands.

CoA NAK Response Code

A negative acknowledgement (NAK) indicates a failure to change the authorization state and can include attributes that indicate the reason for the failure. Use **show** commands to verify a successful CoA.

CoA Request Commands

This section includes:

- Session Reauthentication
- Session Termination
- CoA Disconnect-Request
- CoA Request: Disable Host Port
- CoA Request: Bounce-Port

The switch supports the commands shown in Table 46-4.

Table 46-4 CoA Commands Supported on the Switch

Command[1]	Cisco VSA
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	it is a standard disconnect request that does not require a VSA.
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"

1. All CoA commands must include the session identifier between the switch and the CoA client.

Session Reauthentication

The AAA server typically generates a session reauthentication request when a host with an unknown identity or posture joins the network and is associated with a restricted access authorization profile (such as a guest VLAN). A reauthentication request allows the host to be placed in the appropriate authorization group when its credentials are known.

To initiate session authentication, the AAA server sends a standard CoA-Request message which contains a Cisco vendor-specific attribute (VSA) in this form:
Cisco:Avpair="subscriber:command=reauthenticate" and one or more session identification attributes.

The current session state determines the switch response to the message. If the session is currently authenticated by IEEE 802.1x, the switch responds by sending an EAPoL[1]-RequestId message (see footnote 1 below) to the server.

If the session is currently authenticated by MAC authentication bypass (MAB), the switch sends an access-request to the server, passing the same identity attributes used for the initial successful authentication.

If session authentication is in progress when the switch receives the command, the switch terminates the process, and restarts the authentication sequence, starting with the method configured to be attempted first.

If the session is not yet authorized, or is authorized by using guest VLAN, or critical VLAN, or similar policies, the reauthentication message restarts the access control methods, beginning with the method configured to be attempted first. The current authorization of the session is maintained until the reauthentication leads to a different authorization result.

Session Termination

Three types of CoA requests can trigger session termination. A CoA Disconnect-Request terminates the session, without disabling the host port. This command causes re-initialization of the authenticator state machine for the specified host, but does not restrict that hosts' access to the network.

To restrict a hosts' access to the network, use a CoA Request with the Cisco:Avpair="subscriber:command=disable-host-port" VSA. This command is useful when a host is known to be causing problems on the network, and you need to immediately block network access for the host. When you want to restore network access on the port, reenable it using a non-RADIUS mechanism.

When a device with no supplicant, such as a printer, needs to acquire a new IP address (for example, after a VLAN change), terminate the session on the host port with port-bounce (temporarily disable and then re-enable the port).

1. Extensible Authentication Protocol over Lan

CoA Disconnect-Request

This command is a standard Disconnect-Request. Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the "Session Identification" section on page 46-98. If the session cannot be located, the switch returns a Disconnect-NAK message with the "Session Context Not Found" error-code attribute. If the session *is* located, the switch terminates the session. After the session has been completely removed, the switch returns a Disconnect-ACK.

If the switch fails-over to a standby switch before returning a Disconnect-ACK to the client, the process is repeated on the new active switch when the request is re-sent from the client. If the session is not found following re-sending, a Disconnect-ACK is sent with the "Session Context Not Found" error-code attribute.

CoA Request: Disable Host Port

This command is carried in a standard CoA-Request message that has this new VSA:

Cisco:Avpair="subscriber:command=disable-host-port"

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the "Session Identification" section on page 46-98. If the session cannot be located, the switch returns a CoA-NAK message with the "Session Context Not Found" error-code attribute. If the session is located, the switch disables the hosting port and returns a CoA-ACK message.

If the switch fails before returning a CoA-ACK to the client, the process is repeated on the new active switch when the request is re-sent from the client. If the switch fails after returning a CoA-ACK message to the client but before the operation has completed, the operation is restarted on the new active switch.

Note A Disconnect-Request failure following command re-sending could be the result of either a successful session termination before change-over (if the Disconnect-ACK was not sent) or a session termination by other means (for example, a link failure) that occurred after the original command was issued and before the standby switch became active.

CoA Request: Bounce-Port

This command is carried in a standard CoA-Request message that contains the following new VSA:

Cisco:Avpair="subscriber:command=bounce-host-port"

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the "Session Identification" section on page 46-98. If the session cannot be located, the switch returns a CoA-NAK message with the "Session Context Not Found" error-code attribute. If the session is located, the switch disables the hosting port for a period of 10 seconds, re-enables it (port-bounce), and returns a CoA-ACK.

If the switch fails before returning a CoA-ACK to the client, the process is repeated on the new active switch when the request is re-sent from the client. If the switch fails after returning a CoA-ACK message to the client but before the operation has completed, the operation is re-started on the new active switch.

Configuring RADIUS

This section describes how to configure your switch to support RADIUS. At a minimum, you must identify the host or hosts that run the RADIUS server software and define the method lists for RADIUS authentication. You can optionally define method lists for RADIUS authorization and accounting.

A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on a user. You can use method lists to designate one or more security protocols to be used (such as TACACS+ or local username lookup), thus ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on users. If that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

You should have access to and should configure a RADIUS server before configuring RADIUS features on your switch.

Default RADIUS Configuration

RADIUS and AAA are disabled by default.

To prevent a lapse in security, you cannot configure RADIUS through a network management application. When enabled, RADIUS can authenticate users accessing the switch using the CLI.

Identifying the RADIUS Server Host

Switch-to-RADIUS-server communication involves several components:

- Hostname or IP address
- Authentication destination port
- Accounting destination port
- Key string
- Timeout period
- Retransmission value

You identify RADIUS security servers by their hostname or IP address, hostname and specific UDP port numbers, or their IP address and specific UDP port numbers. The combination of the IP address and the UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address.

If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as a failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the `%RADIUS-4-RADIUS_DEAD` message appears, and then the switch tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order that they are configured.)

A RADIUS server and the switch use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the switch.

The timeout, retransmission, and encryption key values can be configured globally for all RADIUS servers, on a per-server basis, or in some combination of global and per-server settings. To apply these settings globally to all RADIUS servers communicating with the switch, use the three unique global configuration commands: **radius-server timeout**, **radius-server retransmit**, and **radius-server key**. To apply these values on a specific RADIUS server, use the **radius-server host** global configuration command.

Note If you configure both global and per-server functions (timeout, retransmission, and key commands) on the switch, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands. For information on configuring these settings on all RADIUS servers, see the "Configuring Settings for All RADIUS Servers" section on page 46-110.

You can configure the switch to use AAA server groups to group existing server hosts for authentication. For more information, see the "Defining AAA Server Groups" section on page 46-106.

To configure per-server RADIUS server communication, perform this task. This procedure is required.

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]`	Specifies the IP address or hostname of the remote RADIUS server host. • (Optional) For **auth-port** *port-number*, specify the UDP destination port for authentication requests. • (Optional) For **acct-port** *port-number*, specify the UDP destination port for accounting requests. • (Optional) For **timeout** *seconds*, specify the time interval that the switch waits for the RADIUS server to reply before resending. The range is 1 to 1000. This setting overrides the **radius-server timeout** global configuration command setting. If no timeout is set with the **radius-server host** command, the setting of the **radius-server timeout** command is used. • (Optional) For **retransmit** *retries*, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the **radius-server host** command, the setting of the **radius-server retransmit** global configuration command is used. • (Optional) For **key** *string*, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. To configure the switch to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The switch software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.
Step 3	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 4	`Switch# show running-config`	Verifies your entries.
Step 5	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

To remove the specified RADIUS server, use the **no radius-server host** *hostname | ip-address* global configuration command.

This example shows how to configure one RADIUS server to be used for authentication and another to be used for accounting:

```
Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
Switch(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

This example shows how to configure *host1* as the RADIUS server and to use the default ports for both authentication and accounting:

```
Switch(config)# radius-server host host1
```

Note You also need to configure some settings on the RADIUS server. These settings include the IP address of the switch and the key string to be shared by both the server and the switch. For more information, see the RADIUS server documentation.

Configuring RADIUS Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various ports. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific port before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all ports except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

To configure login authentication, perform this task. This procedure is required.

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# aaa new-model`	Enables AAA.

	Command	Purpose
Step 3	`Switch(config)# aaa authentication login {default | list-name} method1 [method2...]`	Creates a login authentication method list. • To create a default list that is used when a named list is *not* specified in the **login authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports. • For *list-name*, specify a character string to name the list you are creating. • For *method1...*, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: – **enable**—Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the **enable** *password* global configuration command. – **group radius**—Use RADIUS authentication. Before you can use this authentication method, you must configure the RADIUS server. For more information, see the "Identifying the RADIUS Server Host" section on page 46-101. – **line**—Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the **password** *password* line configuration command. – **local**—Use the local username database for authentication. You must enter username information in the database. Use the **username** *name* **password** global configuration command. – **local-case**—Use a case-sensitive local username database for authentication. You must enter username information in the database by using the **username** *password* global configuration command. – **none**—Do not use any authentication for login.
Step 4	`Switch(config)# line [console | tty | vty] line-number [ending-line-number]`	Enters line configuration mode, and configure the lines to which you want to apply the authentication list.
Step 5	`Switch(config)# login authentication {default | list-name}`	Applies the authentication list to a line or set of lines. • If you specify **default**, use the default list created with the **aaa authentication login** command. • For *list-name*, specify the list created with the **aaa authentication login** command.
Step 6	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	`Switch# show running-config`	Verifies your entries.
Step 8	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable AAA authentication, use the **no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] global configuration command. To either disable RADIUS authentication for logins or to return to the default value, use the **no login authentication** {**default** | *list-name*} line configuration command.

Note To secure the switch for HTTP access by using AAA methods, you must configure the switch with the **ip http authentication aaa** global configuration command. Configuring AAA authentication does not secure the switch for HTTP access by using AAA methods.

For more information about the **ip http authentication** command, see the *Cisco IOS Security Command Reference, Release 12.2* from the Cisco.com page under **Documentation > Cisco IOS Software > 12.2 Mainline > Command References**.

Defining AAA Server Groups

You can configure the switch to use AAA server groups to group existing server hosts for authentication. You select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list, which lists the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. If you configure two different host entries on the same RADIUS server for the same service, (for example, accounting), the second configured host entry acts as a failover backup to the first one.

You use the **server** group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional **auth-port** and **acct-port** keywords.

To define the AAA server group and associate a particular RADIUS server with it, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]`	Specifies the IP address or hostname of the remote RADIUS server host. • (Optional) For **auth-port** *port-number*, specify the UDP destination port for authentication requests. • (Optional) For **acct-port** *port-number*, specify the UDP destination port for accounting requests. • (Optional) For **timeout** *seconds*, specify the time interval that the switch waits for the RADIUS server to reply before resending. The range is 1 to 1000. This setting overrides the **radius-server timeout** global configuration command setting. If no timeout is set with the **radius-server host** command, the setting of the **radius-server timeout** command is used. • (Optional) For **retransmit** *retries*, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the **radius-server host** command, the setting of the **radius-server retransmit** global configuration command is used. • (Optional) For **key** *string*, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. To configure the switch to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The switch software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.
Step 3	`Switch(config)# aaa new-model`	Enables AAA.
Step 4	`Switch(config)# aaa group server radius group-name`	Defines the AAA server-group with a group name. This command puts the switch in a server group configuration mode.
Step 5	`Switch(config)# server ip-address`	Associates a particular RADIUS server with the defined server group. Repeat this step for each RADIUS server in the AAA server group. Each server in the group must be previously defined in Step 2.
Step 6	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	`Switch# show running-config`	Verifies your entries.

	Command	Purpose
Step 8	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.
Step 9		Enables RADIUS login authentication. See the "Configuring RADIUS Login Authentication" section on page 46-104.

To remove the specified RADIUS server, use the **no radius-server host** *hostname* | *ip-address* global configuration command. To remove a server group from the configuration list, use the **no aaa group server radius** *group-name* global configuration command. To remove the IP address of a RADIUS server, use the **no server** *ip-address* server group configuration command.

In this example, the switch is configured to recognize two different RADIUS group servers (*group1* and *group2*). Group1 has two different host entries on the same RADIUS server configured for the same services. The second host entry acts as a failover backup to the first entry.

```
Switch(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
Switch(config)# aaa new-model
Switch(config)# aaa group server radius group1
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config-sg-radius)# exit
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# exit
```

Configuring RADIUS Authorization for User Privileged Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the switch uses information retrieved from the user's profile, which is in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

You can use the **aaa authorization** global configuration command with the **radius** keyword to set parameters that restrict a user's network access to privileged EXEC mode.

The **aaa authorization exec radius local** command sets these authorization parameters:

- Use RADIUS for privileged EXEC access authorization if authentication was performed by using RADIUS.
- Use the local database if authentication was not performed by using RADIUS.

Note Authorization is bypassed for authenticated users who log in using the CLI even if authorization has been configured.

To specify RADIUS authorization for privileged EXEC access and network services, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# aaa authorization network radius`	Configures the switch for user RADIUS authorization for all network-related service requests.

	Command	Purpose
Step 3	`Switch(config)# aaa authorization exec radius`	Configures the switch for user RADIUS authorization if the user has privileged EXEC access. The **exec** keyword might return user profile information (such as **autocommand** information).
Step 4	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	`Switch# show running-config`	Verifies your entries.
Step 6	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

To disable authorization, use the **no aaa authorization** {**network** | **exec**} *method1* global configuration command.

Starting RADIUS Accounting

The AAA accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the switch reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

To enable RADIUS accounting for each Cisco IOS privilege level and for network services, perform these steps:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# aaa accounting network start-stop radius`	Enables RADIUS accounting for all network-related service requests.
Step 3	`Switch(config)# aaa accounting exec start-stop radius`	Enables RADIUS accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end.
Step 4	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	`Switch# show running-config`	Verifies your entries.
Step 6	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

To disable accounting, use the **no aaa accounting** {**network** | **exec**} {**start-stop**} *method1...* global configuration command.

Configuring Settings for All RADIUS Servers

To configure global communication settings between the switch and all RADIUS servers, perform these steps:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# radius-server key` *string*	Specifies the shared secret text string used between the switch and all RADIUS servers. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
Step 3	`Switch(config)# radius-server retransmit` *retries*	Specifies the number of times the switch sends each RADIUS request to the server before giving up. The default is 3; the range 1 to 1000.
Step 4	`Switch(config)# radius-server timeout` *seconds*	Specifies the number of seconds a switch waits for a reply to a RADIUS request before resending the request. The default is 5 seconds; the range is 1 to 1000.
Step 5	`Switch(config)# radius-server deadtime` *minutes*	Specifies the number of minutes a RADIUS server, which is not responding to authentication requests, to be skipped, thus avoiding the wait for the request to timeout before trying the next configured server. The default is 0; the range is 1 to 1440 minutes.
Step 6	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	`Switch# show running-config`	Verifies your settings.
Step 8	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

To return to the default setting for the retransmit, timeout, and deadtime, use the **no** forms of these commands.

Configuring the Switch to Use Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the switch and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named *cisco-avpair*. The value is a string with this format:

```
protocol : attribute sep value *
```

Protocol is a value of the Cisco protocol attribute for a particular type of authorization. *Attribute* and *value* are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and *sep* is = for mandatory attributes and is * for optional attributes. The full set of features available for TACACS+ authorization can then be used for RADIUS.

For example, this AV pair activates Cisco's *multiple named ip address pools* feature during IP authorization (during PPP IPCP address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

This example shows how to provide a user logging in from a switch with immediate access to privileged EXEC commands:

```
cisco-avpair= "shell:priv-lvl=15"
```

This example shows how to specify an authorized VLAN in the RADIUS server database:

```
cisco-avpair= "tunnel-type(#64)=VLAN(13)"
cisco-avpair= "tunnel-medium-type(#65)=802 media(6)"
cisco-avpair= "tunnel-private-group-ID(#81)=vlanid"
```

This example shows how to apply an input ACL in ASCII format to an interface for the duration of this connection:

```
cisco-avpair= "ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0"
cisco-avpair= "ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any"
cisco-avpair= "mac:inacl#3=deny any any decnet-iv"
```

This example shows how to apply an output ACL in ASCII format to an interface for the duration of this connection:

```
cisco-avpair= "ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any"
```

Other vendors have their own unique vendor-IDs, options, and associated VSAs. For more information about vendor-IDs and VSAs, see RFC 2138, "Remote Authentication Dial-In User Service (RADIUS)."

To configure the switch to recognize and use VSAs, perform these steps:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# radius-server vsa send [accounting | authentication]`	Enables the switch to recognize and use VSAs as defined by RADIUS IETF attribute 26. • (Optional) Use the **accounting** keyword to limit the set of recognized vendor-specific attributes to only accounting attributes. • (Optional) Use the **authentication** keyword to limit the set of recognized vendor-specific attributes to only authentication attributes. If you enter this command without keywords, both accounting and authentication vendor-specific attributes are used.
Step 3	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 4	`Switch# show running-config`	Verifies your settings.
Step 5	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Note For a complete list of RADIUS attributes or more information about vendor-specific attribute 26, see the "RADIUS Attributes" appendix in the *Cisco IOS Security Configuration Guide, Release 12.2* from the Cisco.com page under **Documentation > Cisco IOS Software > 12.2 Mainline > Command References**.

Configuring the Switch for Vendor-Proprietary RADIUS Server Communication

Although an IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the switch and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. Cisco IOS software supports a subset of vendor-proprietary RADIUS attributes.

As mentioned earlier, to configure RADIUS (whether vendor-proprietary or IETF draft-compliant), you must specify the host running the RADIUS server daemon and the secret text string it shares with the switch. You specify the RADIUS host and secret text string by using the **radius-server** global configuration commands.

To specify a vendor-proprietary RADIUS server host and a shared secret text string, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# radius-server host {hostname | ip-address} non-standard`	Specifies the IP address or hostname of the remote RADIUS server host and identify that it is using a vendor-proprietary implementation of RADIUS.
Step 3	`Switch(config)# radius-server key string`	Specifies the shared secret text string used between the switch and the vendor-proprietary RADIUS server. The switch and the RADIUS server use this text string to encrypt passwords and exchange responses. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
Step 4	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	`Switch# show running-config`	Verifies your settings.
Step 6	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

To delete the vendor-proprietary RADIUS host, use the **no radius-server host** {*hostname* | *ip-address*} **non-standard** global configuration command. To disable the key, use the **no radius-server key** global configuration command.

This example shows how to specify a vendor-proprietary RADIUS host and to use a secret key of *rad124* between the switch and the server:

```
Switch(config)# radius-server host 172.20.30.15 nonstandard
Switch(config)# radius-server key rad124
```

Configuring CoA on the Switch

To configure CoA on a switch, perform these steps. This procedure is required.

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# aaa new-model`	Enables AAA.
Step 3	`Switch(config)# aaa server radius dynamic-author`	Configures the switch as an authentication, authorization, and accounting (AAA) server to facilitate interaction with an external policy server.
Step 4	`Switch(config-locsvr-da-radius)# client {`*ip-address* | *name*`} [vrf` *vrfname*`] [server-key` *string*`]`	Enters dynamic authorization local server configuration mode and specify a RADIUS client from which a device will accept CoA and disconnect requests.
Step 5	`Switch(config-locsvr-da-radius)# server-key [0 | 7]` *string*	Configures the RADIUS key to be shared between a device and RADIUS clients.
Step 6	`Switch(config-locsvr-da-radius)# port` *port-number*	Specifies the port on which a device listens for RADIUS requests from configured RADIUS clients.
Step 7	`Switch(config-locsvr-da-radius)# auth-type {any | all | session-key}`	Specifies the type of authorization the switch uses for RADIUS clients. The client must match all the configured attributes for authorization.
Step 8	`Switch(config-locsvr-da-radius)# ignore session-key`	(Optional) Configures the switch to ignore the session-key. For more information about the **ignore** command, see the *Cisco IOS Intelligent Services Gateway Command Reference* on Cisco.com.
Step 9	`Switch(config-locsvr-da-radius)# ignore server-key`	(Optional) Configures the switch to ignore the server-key. For more information about the **ignore** command, see the *Cisco IOS Intelligent Services Gateway Command Reference* on Cisco.com.
Step 10	`Switch(config-locsvr-da-radius)# exit`	Switches to global configuration mode.
Step 11	`Switch(config)# authentication command bounce-port ignore`	(Optional) Configures the switch to ignore a CoA request to temporarily disable the port hosting a session. The purpose of temporarily disabling the port is to trigger a DHCP renegotiation from the host when a VLAN change occurs and there is no supplicant on the endpoint to detect the change.
Step 12	`Switch(config)# authentication command disable-port ignore`	(Optional) Configures the switch to ignore a nonstandard command requesting that the port hosting a session be administratively shut down. Shutting down the port results in termination of the session. Use standard CLI or SNMP commands to re-enable the port.
Step 13	`Switch# end`	Returns to privileged EXEC mode.
Step 14	`Switch# show running-config`	Verifies your entries.
Step 15	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable the AAA server functionality on the switch, use the **no aaa server radius dynamic authorization** global configuration command:

```
Switch(config)# aaa server radius dynamic-author
Switch(config-locsvr-da-radius)# client ip addr vrf vrfname
Switch(config-locsvr-da-radius)# server-key cisco123
Switch(config-locsvr-da-radius)# port 3799
```

Note Default port for packet of disconnect is 1700. Port 3799 is required to interoperate with ACS 5.1.

```
Switch(config)# authentication command bounce-port ignore
```

Monitoring and Troubleshooting CoA Functionality

The following Cisco IOS commands can be used to monitor and troubleshoot CoA functionality on the switch:

- **debug radius**
- **debug aaa coa**
- **debug aaa pod**
- **debug aaa subsys**
- **debug cmdhd** [**detail** | **error** | **events**]
- **show aaa attributes protocol radius**

Configuring RADIUS Server Load Balancing

This feature allows access and authentication requests to be evenly across all RADIUS servers in a server group. For more information, see the *RADIUS Server Load Balancing* chapter of the *Cisco IOS Security Configuration Guide*, Release 12.2:

http://www.ciscosystems.com/en/US/docs/ios/12_2sb/feature/guide/sbrdldbl.html

Displaying the RADIUS Configuration

To display the RADIUS configuration, use the **show running-config** privileged EXEC command.

Configuring Device Sensor

This section includes the following:

About Device Sensor

Device Sensor uses protocols such as Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), and DHCP to obtain endpoint information from network devices and make this information available to its clients. Device Sensor has internal clients, such as the embedded Device Classifier (local analyzer), Auto Smartports (ASP), MediaNet Service Interface Media Services Proxy, and EnergyWise. Device Sensor also has an external client, Identity Services Engine (ISE), which uses RADIUS accounting to receive and analyze endpoint data. When integrated with ISE, Device Sensor provides central policy management and device-profiling capabilities.

Note Cisco Identity Services Engine (ISE) based profiling is not supported on the LAN Base image.

Device profiling capability consists of two parts:

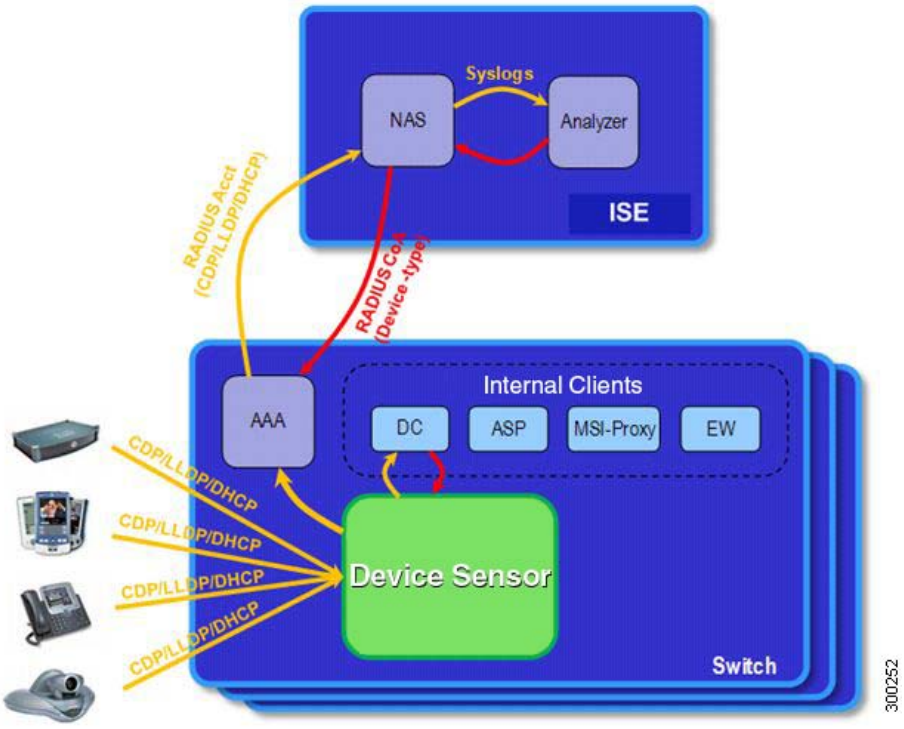
- Collector--Gathers endpoint data from network devices.
- Analyzer--Processes the data and determines the type of device.

For more information on device profiling, see the "Configuring Endpoint Profiling Policies" chapter in the *Cisco Identity Services Engine User Guide* at this URL:

http://www.cisco.com/en/US/docs/security/ise/1.1/user_guide/ise_prof_pol.html

Device Sensor represents the embedded collector functionality. Figure 19shows a Device Sensor in the context of its internal clients and the ISE.

Figure 19 Device Sensor and Clients



Client notifications and accounting messages that contain profiling data and other session-related data are generated and sent to the internal clients and the ISE. By default, client notifications and accounting events are generated only when an incoming packet includes a Type-Length-Value (TLV) that has not previously been received within a given access session. You can enable client notifications and accounting events for TLV changes; that is, when a previously received TLV is received with a different value.

Device Sensor port security protects a switch from consuming memory and crashing during deliberate or unintentional denial-of-service (DoS)-type attacks. Device Sensor limits the maximum number of device monitoring sessions to 32 per port. While hosts are inactive, the age session limit is 12 hours.

MSP-IOS Sensor Device Classifier Interaction

Note To enable MSP, you must configure the **profile flow** command. Once done, when SIP, H323, or mDNS traffic are present, appropriate (SIP, H323, or mDNS) TLV notifications are sent to the IOS sensor.

MSP (Media Service Proxy) offers bandwidth reservation for audio or video flows and Metadata services to 3rd-party endpoints. To offer and install Media services, MSP must identify flow attributes and device details. MSP device identification requires automatic identification of various media end points in the network, thereby avoiding any change to the installed end point base. To offer MSP device discovery services, MSP leverages current IOS sensor capability for device classification. (Starting with Release IOS XE 3.3.0SG and IOS 15.1(1)SG, IOS sensor can be used to perform device identification. MSP uses the same functionality with the addition of SIP, H323, and Multicast DNS (mDNS) protocols.) Starting with Release IOS XE 3.4.0SG and IOS 15.1(2)SG, MSP offers Media services to two kinds of media endpoints: IP Surveillance Cameras and Video-Conferencing Endpoints. Surveillance cameras are identified using mDNS protocol whereas Video-conference-Endpoints are identified using SIP and H.323 protocols.

mDNS compatible devices (Axis, Pelco cameras etc) send mDNS messages for DNS service discovery to a multicast IP address (224.0.0.251) on a standard mDNS port 5353. The mDNS client module listens to this UDP port, receives the mDNS message, and sends it in TLV format to the mDNS IOS sensor shim for further device classification. The module parses the mDNS query and Answer messages fields to create these TLVs.

A Session Initiation Protocol (SIP) registration message is used for SIP based device-discovery and is sent to Cisco Call manager by the SIP Client. A H.225 RAS client registration message is used for H323-based device discovery.

If no Cisco Unified Communicator Manager or GateKeeper exists in the topology, the Endpoint will not generate device Register messages. To handle device discovery in these scenarios, MSP expects the endpoint to make a SIP or H323 call so that MSP snoops the SIP invite or the H323 setup message to identify endpoint details and notify the IOS sensor.

After the IOS sensor receives these protocol details from MSP, the IOS sensor prepares Normalized TLVs, with the new protocols. These protocol details are sent to session manager for further classification.

Configuring Device Sensor

Device Sensor is enabled by default. Complete the following tasks when you want Device Sensor to include or exclude a list of TLVs (termed filter lists) for a particular protocol.

Note If you do not perform any Device Sensor configuration tasks, the following TLVs are included by default:

- CDP filter--secondport-status-type and powernet-event-type (types 28 and 29)
- LLDP filter--organizationally-specific (type 127)
- DHCP filter--message-type (type 53)

Enabling MSP

You must configure the MSP **profile flow** command to activate the MSP platform Packet parser. This is because the MSP device handler is tightly coupled with MSP flow parser. Not enabling this command means that MSP will not send SIP, H323 notifications to the IOS sensor.

To enable MSP, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**configure terminal** Switch# configure terminal	Enters global configuration mode.
Step 2	**profile flow** Switch(config)# profile flow	Enables MSP.
Step 3	**end** Switch(config)# end	Returns to privileged EXEC mode.

Use the **no** form of the profile flow command to disable MSP.

Enabling Accounting Augmentation

For the Device Sensor protocol data to be added to accounting messages, you must first enable session accounting by using the following standard Authentication, Authorization, and Accounting (AAA) and RADIUS configuration commands:

```
Switch(config)# aaa new-model
Switch(config)# aaa accounting dot1x default start-stop group radius
```

```
Switch(config)# radius-server host{hostname|ip-address}[auth-port
port-number][acct-port port-number] [timeout seconds][retransmit retries][key string]
Switch(config)# radius-server vsa send accounting
```

To add Device Sensor protocol data to accounting records, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**configure terminal** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**device-sensor accounting** `Switch(config)# device-sensor accounting`	Enables the addition of sensor protocol data to accounting records and also enables the generation of additional accounting events when new sensor data is detected.
Step 3	**end** `Switch(config)# end`	Returns to privileged EXEC mode.

Creating a Cisco Discovery Protocol Filter

To create a CDP filter containing a list of TLVs that can be included or excluded in the Device Sensor output, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**configure terminal** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**device-sensor filter-list cdp list tlv-list-name** `Switch(config)# device-sensor filter-list cdp list cdp-list`	Creates a TLV list and enters CDP sensor configuration mode, where you can configure individual TLVs.
Step 3	**tlv** {**name** *tlv-name* | **number** *tlv-number*} `Switch(config-sensor-cdplist)# tlv number 10`	Adds individual CDP TLVs to the TLV list. You can delete the TLV list without individually removing TLVs from the list by using the **no device-sensor filter-list cdp list tlv-list-name** command.
Step 4	**end** `Switch(config-sensor-cdplist)# end`	Returns to privileged EXEC mode.

Creating an LLDP Filter

To create an LLDP filter containing a list of TLVs that can be included or excluded in the Device Sensor output, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**configure terminal** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**device-sensor filter-list lldp list tlv-list-name** `Switch(config)# device-sensor filter-list lldp list lldp-list`	Creates a TLV list and enters LLDP sensor configuration mode, where you can configure individual TLVs.
Step 3	**tlv** {**name** *tlv-name* | **number** *tlv-number*} `Switch(config-sensor-cdplist)# tlv number 10`	Adds individual LLDP TLVs to the TLV list. You can delete the TLV list without individually removing TLVs from the list by using the **no device-sensor filter-list lldp list tlv-list-name** command.
Step 4	**end** `Switch(config-sensor-lldplist)# end`	Returns to privileged EXEC mode.

Creating a DHCP Filter

To create a DHCP filter containing a list of DHCP options that can be included or excluded in the Device Sensor output, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**configure terminal** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**device-sensor filter-list dhcp list option-list-name** `Switch(config)# device-sensor filter-list dhcp list dhcp-list`	Creates an options list and enters DHCP sensor configuration mode, where you can specify individual DHCP options.
Step 3	**option** {**name** *option-name* | **number** *option-number*} `Switch(config-sensor-dhcplist)# option number 50`	Adds individual DHCP options to the option list. You can delete the entire option list without removing options individually from the list by using the **no device-sensor filter-list dhcp list option-list-name** command.
Step 4	**end** `Switch(config)# end`	Returns to privileged EXEC mode.

Applying a Protocol Filter to the Device Sensor Output

Beginning in privileged EXEC mode, follow these steps to apply a CDP, LLDP, or DHCP filter to the sensor output. The output is session notifications to internal sensor clients and accounting requests to the RADIUS server.

Note Only one filter list can be included or excluded at a time.

	Command	Purpose
Step 1	**configure terminal** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**device-sensor filter-spec** {**cdp** | **dhcp** | **lldp**} {**exclude** {**all** | **list** *list-name*} | **include list** *list-name*} `Switch(config)# device-sensor filter-spec cdp include list list1`	Applies a specific protocol filter containing a list of protocol TLV fields or DHCP options to the Device Sensor output. • **cdp**--Applies a CDP TLV filter list to the device sensor output. • **lldp**--Applies an LLDP TLV filter list to the device sensor output. • **dhcp**--Applies a DHCP option filter list to the device sensor output. • **exclude**--Specifies the TLVs that must be excluded from the device sensor output. • **include**--Specifies the TLVs that must be included from the device sensor output. • **all**--Disables all notifications for the associated protocol. • **list** *list-name*--Specifies the protocol TLV filter list name.
Step 3	**end** `Switch(config)# end`	Returns to privileged EXEC mode.

Tracking TLV Changes

By default, client notifications and accounting events are generated only when an incoming packet includes a TLV that has not previously been received within a given session.

To enable client notifications and accounting events for TLV changes, follow these steps, beginning in privileged EXCEC mode:

	Command	Purpose
Step 1	**configure terminal** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**device-sensor notify all-changes** `Switch(config)# device-sensor notify all-changes`	Enables client notifications and accounting events for all TLV changes, that is, where either a new TLV is received or a previously received TLV is received with a new value in the context of a given session. **Note** Use the default device-sensor notify or the device-sensor notify new-tlvs command to return to the default TLV.
Step 3	**end** `Switch(config)# end`	Returns to privileged EXEC mode.

Verifying the Device Sensor Configuration

To verify the sensor cache entries for all devices, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**show device-sensor cache mac** *mac-address*	Displays sensor cache entries (the list of protocol TLVs or options received from a device) for a specific device. • **mac-address** is the MAC address of the endpoint
Step 2	**show device-sensor cache all** `Switch(config)# device-sensor notify all-changes`	Displays sensor cache entries for all devices.

This is an example of the **show device-sensor cache mac mac-address** privileged EXEC command output:

```
Switch# show device-sensor cache mac 0024.14dc.df4d

Device: 0024.14dc.df4d on port GigabitEthernet1/0/24
-----------------------------------------------
Proto Type:Name                          Len Value
cdp     26:power-available-type           16 00 1A 00 10 00 00 00 01 00 00 00 00 FF FF FF FF
cdp     22:mgmt-address-type              17 00 16 00 11 00 00 00 01 01 01 CC 00 04 09 1B 65
                                             0E
cdp     11:duplex-type                     5 00 0B 00 05 01
cdp      9:vtp-mgmt-domain-type            4 00 09 00 04
cdp      4:capabilities-type               8 00 04 00 08 00 00 00 28
cdp      1:device-name                    14 00 01 00 0E 73 75 70 70 6C 69 63 61 6E 74
lldp     0:end-of-lldpdu                   2 00 00
lldp     8:management-address             14 10 0C 05 01 09 1B 65 0E 03 00 00 00 01 00
lldp     7:system-capabilities             6 0E 04 00 14 00 04
lldp     4:port-description               23 08 15 47 69 67 61 62 69 74 45 74 68 65 72 6E 65
                                             74 31 2F 30 2F 32 34
lldp     5:system-name                    12 0A 0A 73 75 70 70 6C 69 63 61 6E 74
dhcp    82:relay-agent-info               20 52 12 01 06 00 04 00 18 01 18 02 08 00 06 00 24
                                             14 DC DF 80
dhcp    12:host-name                      12 0C 0A 73 75 70 70 6C 69 63 61 6E 74
dhcp    61:client-identifier              32 3D 1E 00 63 69 73 63 6F 2D 30 30 32 34 2E 31 34
                                             64 63 2E 64 66 34 64 2D 47 69 31 2F 30 2F 32 34
dhcp    57:max-message-size                4 39 02 04 80
```

This is an example of the **show device-sensor cache all** privileged EXEC command output:

```
Switch# show device-sensor cache all

Device: 001c.0f74.8480 on port GigabitEthernet2/1
-----------------------------------------------
Proto Type:Name Len Value
dhcp 52:option-overload 3 34 01 03
dhcp 60:class-identifier 11 3C 09 64 6F 63 73 69 73 31 2E 30
dhcp 55:parameter-request-list 8 37 06 01 42 06 03 43 96
dhcp 61:client-identifier 27 3D 19 00 63 69 73 63 6F 2D 30 30 31 63 2E 30 66
37 34 2E 38 34 38 30 2D 56 6C 31
dhcp 57:max-message-size 4 39 02 04 80
Device: 000f.f7a7.234f on port GigabitEthernet2/1
-----------------------------------------------
Proto Type:Name Len Value
cdp 22:mgmt-address-type 8 00 16 00 08 00 00 00 00
```

```
cdp 19:cos-type 5 00 13 00 05 00
cdp 18:trust-type 5 00 12 00 05 00
cdp 11:duplex-type 5 00 0B 00 05 01
cdp 10:native-vlan-type 6 00 0A 00 06 00 01
cdp 9:vtp-mgmt-domain-type 9 00 09 00 09 63 69 73 63 6F
```

Troubleshooting Commands

The following commands can help troubleshoot Device Sensor.

- **debug device-sensor** {**errors** | **events**}
- **debug authentication all**

Restrictions for Device Sensor

- Only CDP, LLDP, and DHCP protocols are supported.
- The session limit for profiling ports is 32.
- The length of one TLV must not be more than 1024 and the total length of TLVs (combined length of TLVs) of all protocols must not be more than 4096.
- Device Sensor profiles devices that are only one hop away.

Configuration Examples for the Device Sensor Feature

The following example shows how to create a CDP filter containing a list of TLVs:

```
Switch> enable
Switch# configure terminal
Switch(config)# device-sensor filter-list cdp list cdp-list
Switch(config-sensor-cdplist)# tlv name address-type
Switch(config-sensor-cdplist)# tlv name device-name
Switch(config-sensor-cdplist)# tlv number 34
Switch(config-sensor-cdplist)# end
```

The following example shows how to create an LLDP filter containing a list of TLVs:

```
Switch> enable
Switch# configure terminal
Switch(config)# device-sensor filter-list lldp list lldp-list
Switch(config-sensor-lldplist)# tlv name chassis-id
Switch(config-sensor-lldplist)# tlv name management-address
Switch(config-sensor-lldplist)# tlv number 28
Switch(config-sensor-lldplist)# end
```

The following example shows how to create a DHCP filter containing a list of options:

```
Switch> enable
Switch# configure terminal
Switch(config)# device-sensor filter-list dhcp list dhcp-list
Switch(config)# device-sensor filter-list dhcp list dhcp-list
Switch(config-sensor-dhcplist)# option name domain-name
Switch(config-sensor-dhcplist)# option name host-name
Switch(config-sensor-dhcplist)# option number 50
Switch(config-sensor-dhcplist)# end
```

The following example shows how to apply a CDP TLV filter list to the Device Sensor output:

```
Switch> enable
Switch# configure terminal
Switch(config)# device-sensor filter-spec cdp include cdp-list1
```

The following example shows how to enable client notifications and accounting events for all TLV changes:

```
Switch> enable
Switch# configure terminal
Switch(config)# device-sensor notify all-changes
```

Displaying 802.1X Statistics and Status

To display 802.1X statistics for all interfaces, use the **show dot1x all statistics** privileged EXEC command.

To display the 802.1X administrative and operational status for the switch, use the **show dot1x all details** privileged EXEC command. To display the 802.1X administrative and operational status for a specific interface, use the **show dot1x interface details** privileged EXEC command.

Displaying Authentication Details

This section includes these topics:

Determining the Authentication Methods Registered with the Auth Manager

This example show how to display the registered authentication methods:

Enter the following:

```
Switch# show authentication registrations
Handle  Priority  Name
      3         0       dot1x
      2         1       mab
      1         2       webauth
```

Displaying the Auth Manager Summary for an Interface

In the following example, MAB was configured for a higher priority (lower value) than 802.1X:

```
Switch# show authentication int gi1/5
Client list:
Interface  MAC Address     Method   Domain   Status         Session ID
  Gi1/5      000f.23c4.a401  mab      DATA     Authz Success  0A3462B10000000D24F80B58
  Gi1/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94

Available methods list:
  Handle  Priority  Name
    3        0      dot1x
    2        1      mab
Runnable methods list:
  Handle  Priority  Name
    2        0      mab
    3        1      dot1x
```

Displaying the Summary of All Auth Manager Sessions on the Switch

This example shows how ti display the summary of all sessions:

```
Switch# show authentication sessions
Interface  MAC Address     Method   Domain   Status         Session ID
Gi1/48     0015.63b0.f676  dot1x    DATA     Authz Success  0A3462B1000000102983C05C
Gi1/5      000f.23c4.a401  mab      DATA     Authz Success  0A3462B10000000D24F80B58
Gi1/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94
```

Displaying a Summary of All Auth Manager Sessions on the Switch Authorized for a Specified Authentication Method

This example shows how to display a summary of all sessions for a specific authentication method:

```
Switch# show authentication method dot1x
Interface  MAC Address     Method   Domain   Status         Session ID
Gi1/48     0015.63b0.f676  dot1x    DATA     Authz Success  0A3462B1000000102983C05C
Gi1/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94
```

Verifying the Auth Manager Session for an Interface

The Auth manage session can be verified by using the **show authentication sessions** command:

```
Switch# show authentication sessions int gi1/5
Interface: GigabitEthernet1/5
MAC Address: 000f.23c4.a401
IP Address: Unknown
User-Name: 000f23c4a401
Status: Authz Success
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
```

```
Vlan Policy: N/A
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A3462B10000000D24F80B58
Acct Session ID: 0x0000000F
Handle: 0x2400000D
Runnable methods list:
Method State
dot1x Failed over
mab Authc Success
----------------------------------------
Interface: GigabitEthernet1/5
MAC Address: 0014.bf5d.d26d
IP Address: 20.0.0.7
User-Name: johndoe
Status: Authz Success
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: N/A
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A3462B10000000E29811B94
Acct Session ID: 0x00000010
Handle: 0x1100000E
Runnable methods list:
Method State
dot1x Authc Success
mab Not run
```

The individual output can be further refined by using the **handle**, **interface**, **MAC**, **session-id**, or **method** keywords:

```
Switch# show authentication sessions mac 000f.23c4.a401
Interface: GigabitEthernet1/5
MAC Address: 000f.23c4.a401
IP Address: Unknown
User-Name: 000f23c4a401
Status: Authz Success
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: N/A
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A3462B10000000D24F80B58
Acct Session ID: 0x0000000F
Handle: 0x2400000D
Runnable methods list:
Method State
dot1x Failed over
mab Authc Success

Switch# show authentication sessions session-id 0A3462B10000000D24F80B58
Interface: GigabitEthernet1/5
MAC Address: 000f.23c4.a401
IP Address: Unknown
User-Name: 000f23c4a401
```

```
Status: Authz Success
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: N/A
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A3462B10000000D24F80B58
Acct Session ID: 0x0000000F
Handle: 0x2400000D
Runnable methods list:
Method State
dot1x Failed over
mab uthc Success

Switch# show authentication session method dot1x int gi1/5
Interface: GigabitEthernet1/5
MAC Address: 0014.bf5d.d26d
IP Address: 20.0.0.7
User-Name: johndoe
Status: Authz Success
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: N/A
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A3462B10000000E29811B94
Acct Session ID: 0x00000010
Handle: 0x1100000E
Runnable methods list:
Method State
dot1x Authc Success
mab Not run
```

Displaying MAB Details

The following commands display these details:

```
Switch# show mab all
MAB details for FastEthernet5/9
-------------------------------------
Mac-Auth-Bypass           = Enabled
Inactivity Timeout        = None

Switch# show mab all detail
MAB details for FastEthernet5/9
-------------------------------------
Mac-Auth-Bypass           = Enabled
Inactivity Timeout        = None
MAB Client List
---------------
Client MAC                = 000f.23c4.a401
MAB SM state              = TERMINATE
Auth Status               = AUTHORIZED
```

```
Switch# show mab int fa5/9
MAB details for FastEthernet5/9
--------------------------------------
Mac-Auth-Bypass           = Enabled
Inactivity Timeout        = None

Switch# show mab int fa5/9 detail
MAB details for FastEthernet5/9
--------------------------------------
Mac-Auth-Bypass           = Enabled
Inactivity Timeout        = None
MAB Client List
---------------
Client MAC                = 000f.23c4.a401
MAB SM state              = TERMINATE
Auth Status               = AUTHORIZED
```

EPM Logging

EPM logging enables you to display EPM logging messages by using the **epm logging** command in global configuration mode. To disable EPM logging, enter **no epm logging**.

Logging messages are displayed during the following events:

- POLICY_APP_SUCCESS—Policy application success events on Named ACLs, Proxy ACLs, and service policies, URL redirect policies.
- POLICY_APP_FAILURE—Policy application failure conditions similar to unconfigured policies, wrong policies, download request failures and download failures from AAA.
- IPEVENT—IP assignment, IP release and IP wait events for clients.
- AAA—AAA events (similar to download requests, or download successes from AAA)

Example 1

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# epm logging
Switch# clear dot1x all
Switch#
*May 15 08:31:26.561: %EPM-6-POLICY_REQ: IP=100.0.0.222| MAC=0000.0000.0001|
        AUDITSESID=0A050B2C000000030004956C| AUTHTYPE=DOT1X|
        EVENT=REMOVE
*May 15 08:31:26.581: %AUTHMGR-5-START: Starting 'dot1x' for client (0000.0000.0001) on
Interface Fa9/25
*May 15 08:31:26.681: %DOT1X-5-SUCCESS: Authentication successful for client
(0000.0000.0001) on Interface Fa9/25
*May 15 08:31:26.681: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for
client (0000.0000.0001) on Interface Fa9/25
```

Example 2

```
Switch# conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# epm logging
Switch(config)# int f9/25
Switch(config-if)# shut
Switch(config-if)# no shut
*May 15 08:41:56.329: %EPM-6-IPEVENT: IP=100.0.0.222| MAC=0000.0000.0001|
        AUDITSESID=0A050B2C0000026108FB7924| AUTHTYPE=DOT1X|
        EVENT=IP-RELEASE
*May 15 08:41:56.333: %EPM-6-IPEVENT: IP=100.0.0.222| MAC=0000.0000.0001|
        AUDITSESID=0A050B2C0000026108FB7924| AUTHTYPE=DOT1X|
        EVENT=IP-WAIT
```

Cisco IOS Security Features

This document provides a list of security software features that are supported in Cisco IOS XE 3.1.0SG. Links to the feature documentation are included.

Feature guides may contain information about more than one feature. To find information about a specific feature within a feature guide, see the Feature Information table at the end of the guide.

Feature guides document features that are supported on many different software releases and platforms. Your Cisco software release or platform may not support all the features documented in a feature guide. See the Feature Information table at the end of the feature guide for information about which features in that guide are supported in your software release. Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Role-Based Access Control CLI Commands

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_role_base_cli.html

Authentication Proxy Accounting for HTTP

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_authen_prxy.html

Enhanced Password Security

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_sec_4cli.html

IEEE 802.1X - Flexible Authentication

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_authen_prxy.html

Image Verification

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_image_verifctn.html

Manual Certificate Enrollment via TFTP

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cert_enroll_pki.html

Pre-fragmentation For Ipsec VPNs

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_pre_frag_vpns.html

Router Security Audit Manageability

http://www.cisco.com/en/US/prod/collateral/routers/ps10537/product_bulletin_ISRG2_Manageability.pdf

Trusted Root Certification Authority

http://www.cisco.com/en/US/docs/security/cta/admin_guide/ctaCerts.html