

Configuring 802.1X

This chapter describes how to configure IEEE 802.1X port-based authentication on Cisco NX-OS devices.

This chapter includes the following sections:

- About 802.1x, on page 1
- About 802.1x for voice VLAN, on page 10
- About DACL, on page 14
- Violation restrict mode , on page 14
- Prerequisites for 802.1x, on page 14
- 802.1X guidelines and limitations, on page 15
- Guidelines and limitations of 802.1x for voice VLAN, on page 19
- Guidelines and limitations for Per-User DACL support for 802.1x, on page 20
- Guidelines and limitations for critical authentication, on page 21
- Default settings for 802.1x, on page 21
- Configuring 802.1x, on page 23
- 802.1X configuration verification commands, on page 51
- 802.1X support for VXLAN EVPN, on page 52
- Critical authentication verification, on page 57
- Monitor 802.1x statistics, on page 57
- 802.1X port configuration commands, on page 58
- Configuration example for Per-User DACL, on page 60
- Additional references for 802.1x, on page 61

About 802.1x

802.1X is a client-server based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports.

- Authenticates each client connected to a Cisco NX-OS device port using an authentication server.
- Allows only Extensible Authentication Protocol over LAN (EAPOL) traffic until authentication is successful.
- Permits normal traffic through the port after successful authentication.

Device roles

Device roles in 802.1X define the responsibilities of network devices in port-based authentication, including the supplicant, authenticator, and authentication server.

- **Supplicant** : The client device that requests access to the LAN and responds to requests from the Cisco NX-OS device, requiring 802.1X-compliant client software.
- **Authentication server** : Performs the actual authentication of the supplicant, validates its identity, and notifies the Cisco NX-OS device about authorization. RADIUS with EAP extensions is the only supported authentication server.
- **Authenticator** : Controls physical access to the network based on the supplicant's authentication status, acts as an intermediary between the supplicant and authentication server, and includes the RADIUS client for EAP frame handling.

Details of device roles in 802.1x authentication

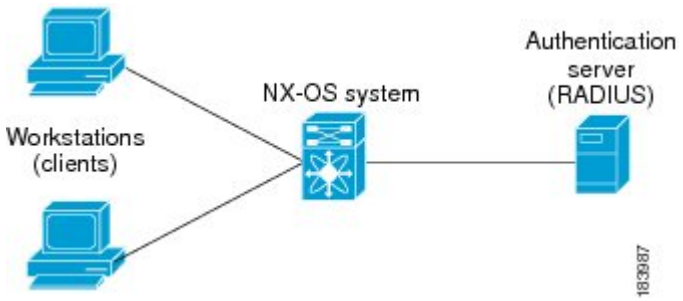
With 802.1X port-based authentication, devices in the network have specific roles that determine how access is granted and managed.

- The supplicant is typically a workstation or client device running 802.1X-compliant software, such as Microsoft Windows XP.
- The authentication server is usually a RADIUS server with EAP extensions, such as Cisco Secure Access Control Server, version 3.0.
- The authenticator is the Cisco NX-OS device, which acts as a proxy between the supplicant and the authentication server.

1. When the authenticator receives EAPOL frames from the supplicant, it strips the Ethernet header and encapsulates the EAP frame in RADIUS format for the authentication server.
2. The authentication server processes the EAP frame and sends a response back to the authenticator.
3. The authenticator removes the server’s frame header, encapsulates the EAP frame for Ethernet, and sends it to the supplicant.

Note The Cisco NX-OS device can only be an 802.1X authenticator.

Figure 1: 802.1X device roles



Device roles in 802.1x

For example, when a user connects a workstation (supplicant) to a network port, the Cisco NX-OS device (authenticator) requests identity information. The authentication server (RADIUS) validates the credentials and authorizes access if the supplicant is verified.

Authentication initiation and message exchange

Authentication initiation and message exchange describe the process by which either the authenticator (Cisco NX-OS device) or the supplicant (client) starts the authentication process, and how EAP frames are exchanged to establish network access.

- Authentication can be initiated by either the authenticator or the supplicant.
- The authenticator sends EAP-request/identity frames when a port transitions from down to up.
- The supplicant responds with EAP-response/identity frames or can initiate authentication with an EAPOL-start frame if no request is received.

Details of authentication initiation and message exchange

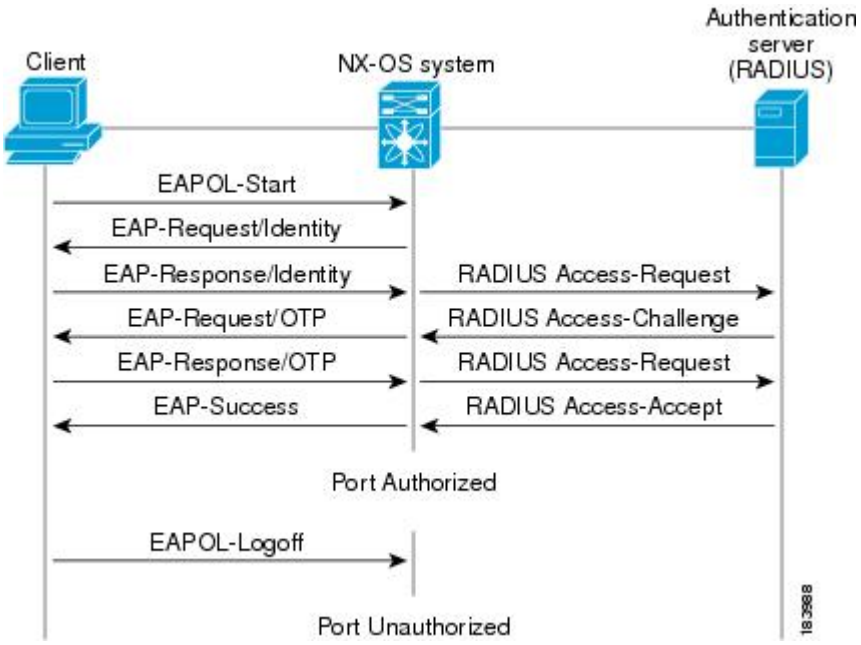
Authentication on Cisco NX-OS devices can be initiated by either the authenticator or the supplicant. When authentication is enabled on a port and the link state transitions from down to up, the authenticator sends an EAP-request/identity frame to the supplicant. The supplicant responds with an EAP-response/identity frame. If the supplicant does not receive a request, it can initiate authentication by sending an EAPOL-start frame. The authenticator then acts as an intermediary, passing EAP frames between the supplicant and the authentication server until authentication succeeds or fails. If authentication is successful, the port becomes authorized.



Note If 802.1X is not enabled or supported on the network access device, the Cisco NX-OS device drops any EAPOL frames from the supplicant. If the supplicant does not receive an EAP-request/identity frame after three attempts to start authentication, the supplicant transmits data as if the port is in the authorized state. A port in the authorized state means that the supplicant has been successfully authenticated.

The specific exchange of EAP frames depends on the authentication method being used.

Figure 2: Message Exchange



The user's secret pass-phrase never crosses the network at any time such as during authentication or during pass-phrase changes.

Authentication message exchange

This example shows a message exchange initiated by the supplicant using the One-Time-Password (OTP) authentication method with a RADIUS server. The OTP authentication device uses a secret pass-phrase to generate a sequence of one-time (single use) passwords.

Authenticator PAE status for interfaces

An authenticator PAE (Port Access Entity) is a protocol entity that supports authentication on an interface when 802.1X is enabled.

- Created automatically when 802.1X is enabled on an interface.
- Not automatically cleared when 802.1X is disabled on the interface.
- Can be explicitly removed and reapplied as needed.

When 802.1X is enabled on an interface, the Cisco NX-OS software creates an authenticator PAE instance to support authentication. Disabling 802.1X does not automatically remove the PAE instance; manual removal and reapplication may be required.

Managing authenticator PAE instances

For example, after disabling 802.1X on an interface, you may need to explicitly remove the authenticator PAE before re-enabling it to ensure proper authentication behavior.

Ports in authorized and unauthorized states

The port authorization state determines whether a supplicant is granted access to the network. Ports can be in authorized or unauthorized states, which control the flow of network traffic based on authentication status.

- In the unauthorized state, the port blocks all ingress and egress traffic except for 802.1X protocol packets.
- When a supplicant is successfully authenticated, the port transitions to the authorized state, allowing all traffic for the supplicant.
- Ports support three authorization states: Force authorized, Force unauthorized, and Auto.

Authorization states and port behavior

Ports can operate in different authorization states, each affecting how authentication and network access are managed.

- **Force authorized** : Disables 802.1X port-based authentication and transitions to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. This authorization state is the default.
- **Force unauthorized** : Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The authenticator cannot provide authentication services to the client through the interface.
- **Auto** : Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received from the supplicant. The authenticator requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each supplicant that attempts to access the network is uniquely identified by the authenticator by using the supplicant's MAC address.

When a client that does not support 802.1X is connected to an unauthorized 802.1X port, the authenticator requests the client's identity. If the client does not respond, the port remains in the unauthorized state and the client is not granted access to the network.

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. If no response is received, the client retries a fixed number of times and then begins sending frames as if the port is in the authorized state.

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

When a supplicant logs off, it sends an EAPOL-logoff message, which causes the authenticator port to transition to the unauthorized state. If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

Port state transitions

For example, if a supplicant is authenticated successfully, the port transitions to the authorized state and allows all traffic. If authentication fails or the supplicant logs off, the port returns to the unauthorized state, restricting network access.

If a non-802.1X client is connected to an unauthorized port, it does not respond to identity requests, and the port remains unauthorized, denying network access.

Port authorization states are like a security checkpoint: only authenticated individuals (supplicants) are allowed through (authorized state), while others are stopped at the gate (unauthorized state).

MAC authentication bypass

MAC Authentication Bypass is a feature that enables a Cisco NX-OS device to authorize a supplicant based on its MAC address when 802.1X authentication is not available or times out.

- Allows network access for devices without 802.1X capability by using their MAC address as identity.
- Triggers when 802.1X authentication times out or is not supported by the connected device.
- Relies on an authentication server with a database of permitted MAC addresses for authorization.

How MAC authentication bypass works and interacts with other features

MAC Authentication Bypass (MAB) is used to authorize devices on Cisco NX-OS interfaces when 802.1X authentication is unavailable or times out. The device uses the MAC address as the supplicant identity and communicates with the authentication server to grant or deny network access.

- When 802.1X authentication times out, the device attempts MAB.
- If an EAPOL packet is detected, 802.1X authentication is used instead of MAB.
- Reauthentication can occur for clients authorized by MAB, following the same process as 802.1X clients.
- MAB interacts with features such as 802.1X authentication, port security, and Network Admission Control (NAC) Layer 2 IP validation.

1. Enable 802.1X authentication on the port.
2. If 802.1X times out, MAB is triggered and the MAC address is used for authorization.
3. If EAPOL is detected, revert to 802.1X authentication.

- 802.1X authentication: MAB can only be enabled if 802.1X is enabled on the port.
- Port security: 802.1X authentication and port security cannot be configured on the same Layer 2 ports.
- NAC Layer 2 IP validation: Takes effect after an 802.1X port is authenticated with MAB, including hosts in the exception list.

Comparison of authentication methods and their triggers:

Table 1: Authentication method comparison

Attributes	802.1X Authentication	MAC Authentication Bypass
Trigger	EAPOL packet detected	802.1X timeout or not supported
Identity Used	Supplicant credentials	MAC address

Tip Enable MAC Authentication Bypass only if 802.1X authentication is enabled on the port, and do not configure port security on the same Layer 2 ports.

Using MAC authentication bypass for a printer

For example, if a printer is connected to an interface configured for 802.1X and does not support 802.1X, the Cisco NX-OS device can use MAC Authentication Bypass to authorize the printer based on its MAC address, granting it network access.

If a device connected to the interface is 802.1X-capable and sends an EAPOL packet, the Cisco NX-OS device uses 802.1X authentication instead of MAC Authentication Bypass.

MAC Authentication Bypass acts like a backup key for network access, allowing entry when the primary method (802.1X) is unavailable or fails.

Dynamic VLAN assignment based on MAC-Based authentication (MAB)

Dynamic VLAN assignment based on MAC-Based Authentication (MAB) is a process where a switch assigns a VLAN to a device after successful authentication, as directed by a RADIUS server.

- Supports dynamic VLAN assignment on Cisco Nexus 9000 Series switches.
- Uses 802.1x or MAB for authentication before port activation.
- RADIUS server specifies the VLAN using tunnel attributes in the Access-Accept message.

How dynamic VLAN assignment works with MAB

Dynamic VLAN assignment allows a switch to place authenticated devices into specific VLANs as determined by a RADIUS server, enhancing network segmentation and security.

Dynamic VLAN assignment with MAB

For example, when a device connects to a Cisco Nexus 9000 Series switch port, the switch uses MAB to authenticate the device's MAC address. Upon successful authentication, the RADIUS server responds with tunnel attributes specifying the VLAN, and the switch assigns the port to that VLAN dynamically.

VLAN assignment from RADIUS

VLAN assignment from RADIUS is the process of dynamically assigning a VLAN to a port based on tunnel attributes received from the RADIUS server after successful authentication.

- The RADIUS server sends tunnel attributes in the Accept-Access message.
- The required tunnel attributes for VLAN assignment are Tunnel-type=VLAN(13), Tunnel-Medium-Type=802, and Tunnel-Private-Group-ID=VLANID.
- All three parameters must be received to configure the access VLAN.

After authentication via 802.1X or MAB, the RADIUS server can provide dynamic VLAN information in the Accept-Access message using tunnel attributes.

- **Tunnel-type=VLAN(13)**
- **Tunnel-Medium-Type=802**
- **Tunnel-Private-Group-ID=VLANID**

VLAN assignment from RADIUS

For example, when a device authenticates using 802.1X, the RADIUS server responds with the required tunnel attributes, allowing the switch to assign the appropriate VLAN to the port dynamically.

Single host and multiple hosts support

Single-host and multiple-host support in 802.1X define how many endpoint devices can access a port and how authentication and security violations are handled.

- Single-host mode restricts port access to only one authenticated endpoint device.
- Multiple-host mode allows multiple endpoint devices to access a port after the first device is authenticated.
- Security violations are handled differently in each mode, with stricter enforcement in single-host mode.

Details of single host and multiple hosts support in 802.1x

The 802.1X feature can restrict traffic on a port to only one endpoint device (single-host mode) or allow traffic from multiple endpoint devices on a port (multi-host mode).

- Single-host mode: Only one endpoint device is allowed on the port. After authentication, the port is authorized. If the device leaves, the port becomes unauthorized. Any traffic from a different MAC address triggers a security violation, disabling the interface. This mode is used for host-to-switch topologies and applies to both Layer 2 and Layer 3 ports.
- Multiple-host mode: Only the first host must be authenticated. Once authorized, additional hosts can access the network without separate authentication. If the port becomes unauthorized, all hosts lose access. Security violation shutdown is disabled in this mode. It is applicable to both switch-to-switch and host-to-switch topologies.

Single host and multiple hosts support

For example, in single-host mode, a single computer connected to a switch port must authenticate before gaining network access. In multiple-host mode, once the first device authenticates, other devices connected to the same port can access the network without additional authentication.

Supported topology

Supported topology for 802.1X port-based authentication refers to the network configuration in which the authentication protocol operates.

- Supports point-to-point topology.
- Only one supplicant (client) can connect to the 802.1X-enabled authenticator port at a time.
- The authenticator detects the supplicant when the port link state changes to up, and returns to unauthorized state if the supplicant leaves or is replaced.

The 802.1X port-based authentication is designed for point-to-point topologies, ensuring that only a single client is authenticated per port.

For example, when a client device connects to a Cisco NX-OS device port configured for 802.1X, the device authenticates the client. If the client disconnects and another device connects, the port transitions to the unauthorized state until the new device is authenticated.

About Per-User DACLs

Per-user DACLs are dynamic access control lists that are downloaded from the Cisco ISE Server and applied to authenticated users on 802.1X ports in Cisco NX-OS.

- They provide different levels of network access and service to 802.1X-authenticated users.
- The switch applies the DACL attributes for the duration of the user session and removes them when the session ends or authentication fails.
- Per-user DACLs use RADIUS vendor-specific attributes (VSAs) in the octet-string format, specifically `inacl#<n>` for ingress direction.

Per-user DACLs are configured and enforced using RADIUS authentication and vendor-specific attributes (VSAs) in Cisco NX-OS environments.

- VSAs are used in the ingress direction only.
- The syntax for per-user DACLs is: `ip:inacl#<n>=permit | deny [protocol] [source_subnet] [dest_subnet] [operator][port]`

Table 2: Per-user DACL VSA syntax comparison

Attribute	Example 1	Example 2
VSA Syntax	`ip:inacl#1=permit udp any any eq 5555`	`ip:inacl#2=deny udp any any eq 6666`



Note TIP: The switch supports VSAs only in the ingress direction.

Per-user DACL example

For example, to permit UDP traffic on port 5555 for a user, use `ip:inacl#1=permit udp any any eq 5555` . To deny UDP traffic on port 6666, use `ip:inacl#2=deny udp any any eq 6666` .

Critical authentication

Critical Authentication is a feature that allows 802.1X users to access the network when RADIUS or ISE servers are unreachable or authentication fails.

- Permits network access for 802.1X users who fail RADIUS authentication due to server unreachability.
- Supported when 802.1X authentication is performed only through RADIUS or ISE servers.
- Can be enabled using the **dot1x authentication event server dead action authorize** command and disabled with the **no** command.

Beginning with Cisco NX-OS Release 10.5(2)F, the 802.1X feature and critical authentication feature are supported on multi-domain ports.

About 802.1x for voice VLAN

Explains 802.1x for voice VLAN.

Overview of 802.1X for Voice VLAN

The IEEE 802.1X Voice VLAN feature is a network capability that enables multi-domain 802.1X authentication on a single port, supporting both VoIP phones and data clients.

- Allows configuration of a special access port associated with two VLAN identifiers: one for voice traffic and one for data traffic.
- Supports multi-domain host mode, accommodating one voice client and one data client on the same port.
- Enables secure and efficient management of network traffic for both voice and data devices.

Supporting reference information for 802.1X Voice VLAN

The 802.1X Voice VLAN feature is used to ensure secure and efficient network traffic management for both voice and data devices connected through a single access port.

Example of 802.1X Voice VLAN Usage

For instance, a network administrator can configure a port to authenticate both a VoIP phone and a computer connected to it. The phone's traffic is assigned to the voice VLAN, while the computer's traffic is assigned to the data VLAN, ensuring both security and quality of service.

Functionalities of 802.1x for voice VLAN

- Enables multi-domain 802.1X authentication on a single port.
- Supports one voice device (typically an IP phone) and one data device (typically a PC) on a single port using a new multi-domain host mode.
- Runs a single authenticator on the port to distinguish users and place them in appropriate domains (different VLANs for data and voice).
- Maintains separation between data traffic and voice traffic on the same port.
- Sends a CDP message to the switch when a host is unplugged behind a Cisco IP phone.
- Allows seamless client mobility by enabling the switch to detect when a device MAC address moves from one MDA port to another.

Figure 3: 802.1X Multi-Domain authentication example



802.1x for voice VLAN

For example, when both an IP phone and a PC are connected to the same switch port, 802.1X multi-domain authentication ensures that voice and data traffic are separated into their respective VLANs, maintaining security and quality of service.

Message exchange of 802.1x for voice VLAN

- **VoIP Phone Connection** : A VoIP phone is connected to a switch where 802.1X is configured.
- **VoIP Phone Authentication** : The VoIP phone can authenticate using either EAP or MAB.
- **Voice Device Recognition** : The VoIP phone is recognized as a voice device by the RADIUS server, and 802.1X secures the phone in the voice VLAN.

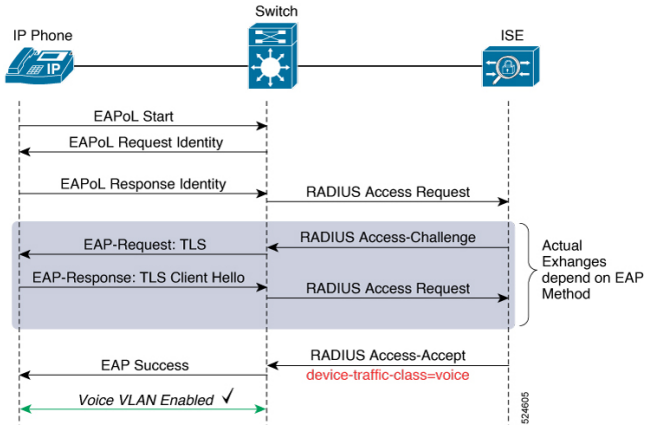
- **Data Device Connection** : A data device (e.g., a laptop) is connected to the switch using the VoIP phone.
- **Data Device Authentication** : The data device triggers 802.1X authentication and gets authorized by the RADIUS server in the data VLAN.

Message exchange steps for 802.1x voice VLAN

The following steps outline the message exchange process for 802.1X authentication in a Voice VLAN environment:

- **VoIP Phone Connection** : A VoIP phone is connected to a switch where 802.1X is configured.
- **VoIP Phone Authentication** : The VoIP phone can authenticate using either EAP or MAB.
- **Voice Device Recognition** : The VoIP phone is recognized as a voice device by the RADIUS server, and 802.1X secures the phone in the voice VLAN.
- **Data Device Connection** : A data device (e.g., a laptop) is connected to the switch using the VoIP phone.
- **Data Device Authentication** : The data device triggers 802.1X authentication and gets authorized by the RADIUS server in the data VLAN.

Figure 4: 802.1X authentication for voice and data devices



802.1x authentication for VoIP and data devices

For example, when a VoIP phone is connected to a switch port with 802.1X enabled, it authenticates using EAP or MAB and is placed in the voice VLAN. If a laptop is then connected through the VoIP phone, it triggers its own 802.1X authentication and is placed in the data VLAN after successful authorization.

Open mode

An open mode is a network authentication feature that

- allows clients to gain immediate network access while authentication is ongoing

- provides network access when a RADIUS server is unreachable or sends an ACCESS-REJECT response, and
- ensures users experience uninterrupted connectivity by authorizing access without delay.

The status "Authenticated By = Open Mode" indicates that the client has been given network access through open mode when ISE is unreachable.

Functionality

- Open mode allows clients complete access to the network.
- While the client enjoys network access, authentication processes such as MAC Authentication Bypass (MAB) continue in the background.
- RADIUS server interaction includes these scenarios:
  - If the RADIUS server responds with an ACCESS-ACCEPT, the client proceeds with normal authorization protocols.
  - If the RADIUS server is unreachable or sends an ACCESS-REJECT, the client remains authorized under Open mode, ensuring uninterrupted access.

DACL for multi-domain mode

A Dynamic Access Control List (DACL) is a network security feature that

- applies per-client access control lists received from a RADIUS server to both voice and data VLANs
- enforces specific traffic restrictions based on each client's MAC address and VLAN, and
- enables flexible, granular network policy enforcement in multi-domain environments.

Change of authorizations

Change of Authorization (COA) is a RADIUS protocol feature that

- enables dynamic updates to user or device authorization policies in real time,
- allows administrators to trigger client reauthentication or session termination remotely, and
- ensures policy changes are applied without unnecessary disruption to active client sessions.

COA operations are initiated by the RADIUS or Identity Services Engine (ISE) server to update a client's authorization state as needed.

- **COA reauthentication**
  - Triggers the client to re-authenticate so policy changes (such as VLAN assignment or dynamic ACL updates) take effect,
  - is used to apply, update, or remove network access policies dynamically,
  - allows the client to remain connected throughout the process.

- **COA session termination (disconnect)**
  - Immediately disconnects the client's network session,
  - removes the client entry from dot1x or similar network authentication tables, and
  - requires the client to reconnect and re-authenticate to regain access.

About DACL

Dynamic ACL (DACL) is a single access control list that specifies what users and groups can access, and is used to restrict access to dot1x MAB clients.

- The DACL policy is pushed from the Cisco ISE server to blacklist a MAC address.
- It applies ACLs on the blacklisted MAC, enabling limited access to the MAB client.
- A single DACL supports all blacklisted MAB clients.

Preconfiguration of DACL

In Cisco NX-OS Release 9.3(5), the DACL is preconfigured on the Cisco Nexus switches.

Violation restrict mode

A violation restrict mode is a port security action that

- keeps the port operational when a security violation (such as a MAC address limit breach) occurs,
- blocks only the violating MAC address from sending traffic, and
- generates an alert, such as a syslog message, to notify administrators of the violation.

When violation restrict mode is enabled on an interface:

- The port remains up and fully operational for authorized clients (such as permitted voice or data devices).
- A new MAC address that exceeds the configured host limit triggers a security violation.
- Instead of disabling the port (ERR-DISABLE state), the violating MAC address is dropped.
- Legitimate, previously authenticated clients continue to communicate without disruption.
- The system logs a security violation event for visibility and auditing.

Prerequisites for 802.1x

Use this reference to review prerequisites for 802.1x.

General 802.1X prerequisites

- 802.1X requires Cisco Nexus Release 7.0(3)I7(1) software.
- One or more RADIUS servers must be accessible in the network.
- 802.1X supplicants must be attached to the ports unless MAC address authentication bypass is enabled.
- System-message logging levels for 802.1X must meet or exceed Cisco DCNM requirements; exceptions apply for Cisco Nexus 7000 Series switches running Cisco NX-OS Release 4.0.

EAP-TLS prerequisites

- For EAP-TLS profile, PKI infrastructure is required for certificate management, including RSA key-pair generation, trustpoint creation, and CA authentication.
- 802.1X with EAP-TLS requires a remote EAP server such as ISE; local authentication server is not supported.
- All participating devices, the CA server, and Cisco Identity Services Engine (ISE) must be synchronized using Network Time Protocol (NTP) to ensure certificate validation.
- AAA server reachability is required for mutual authentication between switches, and both switches must have proper AAA configurations and connectivity.

802.1X prerequisite example

For example, to enable 802.1X with EAP-TLS, ensure that the switch is running Cisco Nexus Release 7.0(3)I7(1), a RADIUS server is reachable, PKI infrastructure is in place for certificate management, and all devices are synchronized using NTP.

802.1X guidelines and limitations

Use this reference to review the 802.1X guidelines and limitations.

802.1X guideline overview

- 802.1X port-based authentication is subject to specific guidelines and limitations depending on the Cisco NX-OS release and switch platform.
- Support and restrictions apply to features such as multi-authentication, dynamic VLAN assignment, MAC authentication bypass, and port types (physical, FEX, vPC, port-channels, etc.).
- Some features and configurations are mutually exclusive or unsupported, including certain protocol enhancements, interface types, and feature combinations.

Port-based authentication upgrade and interface guidelines

802.1X port-based authentication on Cisco Nexus Series switches is governed by a set of guidelines and limitations that vary by NX-OS release and hardware platform. The following points summarize the key considerations and restrictions.

- When upgrading to Cisco NX-OS Release 9.2(1), disable 802.1X using **no feature dot1x** and re-enable it with **feature dot1x** for multi-authentication to function.
- From Release 9.2(1), multi-authentication mode is enabled on 802.1X ports. Dynamic VLAN assignment is successful for the first authenticated host; subsequent hosts must have no VLAN assignment or match the first host's VLAN.
- Release 9.2(3) adds support for 802.1X authentication on FEX-ST and host interface (HIF) ports, including both straight-through and dual-homed FEX.
- 802.1X is not supported on transit topology setups, vPC ports, PVLAN ports, L3 (routed) ports, port security, ports enabled with CTS and MACsec PSK, or with LACP port-channels. Static port-channels are supported.
- Disable 802.1X on vPC ports and all unsupported features.
- 802.1X authentication is supported only on physical ports; not on port channels or subinterfaces.
- 802.1X is supported on member ports of a port channel, but not on the port channel itself. Only multi-host mode is supported on port channel members.
- Member ports with and without 802.1X configuration can coexist in a port channel, but identical 802.1X configuration is required for channeling to operate.
- Supplicants are authenticated before any other Layer 2 or Layer 3 features are enabled on an Ethernet interface when 802.1X is enabled.

Interface and feature compatibility limitations

- STP BPDUs are permitted only after successful authentication on 802.1X enabled ports. Enable 802.1X only on STP edge ports to avoid STP disputes.
- 802.1X authentication is supported only on Ethernet/FEX HIF ports and orphan ports with single access-vlan.
- Dynamic VLAN assignment is supported only on Cisco Nexus 9300-FX/EX/FX2 Platform switches.
- 802.1X does not work with CTS or MACsec PSK features. "mac-learn disable" and 802.1X are mutually exclusive and cannot be configured together.
- 802.1X is mutually exclusive with IP Source Guard and uRPF features. Disable one of these features when upgrading to Release 9.2(3).
- Single host mode is not supported on trunk interfaces or member interfaces in a port channel.
- MAC address authentication bypass is not supported on port channels; only multi-host mode is supported on port-channels.
- In Release 9.2(1), MAC authentication bypass is not supported on the N3K-C3164Q-40GE switch.
- 802.1X is not supported on vPC ports and MCT.

Authentication behavior and protocol limitations

- During a switch reload, 802.1X does not generate RADIUS accounting stops.

- 802.1X protocol enhancements not supported: one-to-many logical VLAN name to ID mapping, web authorization, dynamic domain bridge assignment, IP telephony, and guest VLANs.
- To prevent reauthentication of inactive sessions, set the inactivity timer to an interval shorter than the reauthentication interval.
- Selective enabling/disabling of 802.1X on N9K-M12PQ uplink module ports is not supported for Cisco Nexus 9300 platform switches.
- A security violation occurs when the same MAC is learned on a different VLAN with 802.1X enabled on the interface.
- Configuring mac learn disable with 802.1X enabled on a DME enabled platform does not display error messages.
- In Release 9.2(1), tagged EAPOL frames are processed even if the VLAN is not configured on the interface, and authentication is successful for the client.
- Secure MAC learned on the orphan port is not synced on the vPC peer.
- MAC authentication bypass is supported on Cisco Nexus 9300-EX/FX/FX2 TOR switches from Release 9.2(1).

Platform and release support

- From Release 10.5(2)F, MAC authentication bypass is supported on Cisco Nexus 9300-FX3, GX, GX2, H2R, and H1 Series switches.
- From Release 9.3(5), 802.1X is supported on Cisco Nexus 9300-FX3 platform switches.
- From Release 10.1(2), 802.1X is supported on Cisco Nexus 9300-GX platform switches.
- From Release 10.2(1)F, 802.1X is supported on N9K-C9364D-GX2A and N9K-C9332D-GX2B switches.
- From Release 10.3(2)F, MAC authentication bypass and multi-auth are supported on Cisco Nexus 9508 switches with N9K-X9788TC-FX and N9K-X97160YC-EX line cards.
- Cisco Nexus N9K-C9348GC-FXP switches and C9508 switches with N9K-X9788TC-FX and N9K-X97160YC-EX line cards do not support DVLAN, DACL, FEX-AA, VXLAN and mac-move, CoA, only MAB as authentication method (no EAP), and support is for access port with single access VLAN.
- For Cisco Nexus 9000 PX/TX/PQ EoR or ToR switches, when 802.1X is configured on a vPC domain, traffic traversing the peer-link may get punted to CPU if the source MAC belongs to the vPC peer and traffic needs to be bridged over the same VLAN to an orphan port.
- From Release 10.3(3)F, IPv6 underlay is supported on 802.1X for VXLAN EVPN on Cisco Nexus 9300-EX/FX/FX2/FX3/GX/GX2 switches and Cisco Nexus 9500 switches with X97160YC-EX, 9700-EX/FX/GX line cards.
- From Release 10.4(1)F, certain Cisco Nexus switches and line cards support 802.1X port-based authentication using EAP/EAP-TLS for uplink ports where MACSec is required, with specific limitations (see below).

EAP-TLS and MACsec configuration limitations

- From Release 10.4(3)F, EAP-TLS supports TLS v1.3 and v1.2 on Cisco Nexus switches. If the RADIUS server does not support TLS v1.3, TLS v1.2 is used as the minimum supported version.
- EAP-TLS supported TLS version is 1.2.
- Single EAP profile per switch is supported; multiple interfaces can use the same profile.
- No support for MAC Move profiles of supplicants.
- Authenticator profile is enabled for L3 ports, trunk ports, vPC for only MACsec EAP-TLS. 802.1X authenticator functionality for MAB/EAP clients is not supported for L3 or Trunk and vPC ports.
- EAP-TLS is supported only for EAP on MACsec configured interfaces and only on Multi-Host mode.
- DACL/Critical AUTH/FEX-AA and other 802.1X features on 802.1X MACsec enabled interfaces are not supported.
- EAP-TLS is supported only for remote authentication (ISE/RADIUS - ISE 3.0 and above); local authentication is not supported.
- Order for EAP-TLS configuration: configure **macsec eap policy** first, then **dot1x supplicant eap profile TLS** . For removal, remove **dot1x supplicant eap profile TLS** first, then **macsec eap policy** . For **no feature** , remove 802.1X feature first, then MACsec feature.

MACsec session and interface limitations

- Single EAP profile configured across the switch can be applied on different interfaces.
- If **macsec eap policy** is configured on interfaces, regular 802.1X authenticator functions or commands are not supported.
- Peer-to-peer MACsec enabled switches must have the same 802.1X or MACsec configurations. If commands differ, shut/no-shut is required to recover.
- Once a MACsec secure session is created with a trust point and eap profile is added to the interface, removal of trustpoint or 802.1X supplicant command will not delete the MACsec session; only MACsec interface-specific command removal will delete the session.
- MACsec PKI is supported only on directly connected switches (no intermediate switches or hops). MACsec PKI (802.1X EAP-TLS) mode does not support EoR Stateful Switch Over (SSO).
- EAP-TLS is supported only on L2/L3 ports, port-channel member ports, trunk ports, and breakout ports. Unsupported interface types have no command-level restriction.
- The number of MACsec sessions supported depends on the physical interface scale.

Upgrade limitations

For example, when upgrading a Cisco Nexus 9300-FX switch to NX-OS Release 9.2(1), you must disable 802.1X before the upgrade and re-enable it after the upgrade to ensure multi-authentication works. Additionally, dynamic VLAN assignment is only available for the first authenticated host on a port, and 802.1X is not supported on vPC or L3 ports.

Attempting to configure 802.1X on a port channel or enabling MAC authentication bypass on a port channel will not work, as these configurations are not supported by Cisco NX-OS software.

Guidelines and limitations of 802.1x for voice VLAN

Follow these guidelines and limitations when configuring 802.1X voice VLAN:

Supported platforms

- Beginning with Cisco NX-OS Release 10.5(2)F, the 802.1X voice VLAN feature is supported on these Cisco Nexus switches:
  - N9K-C9348GC-FXP
  - N9K-C93108TC-FX3P
  - N9K-C9348GC-FX3
  - N9K-C9348GC-FX3PH

Supported and unsupported features

- Only Layer 2 switchport mode access is supported with voice VLAN configuration.
- Only one voice VLAN and one data VLAN are supported.
- Beginning with Cisco NX-OS Release 10.6(3)F, DACL and COA are supported on MDA ports.
- Open mode is supported for MAB clients only on MDA ports.
- Violation restrict is supported for all host modes.
- Dynamic VLAN (DVLAN) is not supported for MDA ports.
- The 802.1X voice VLAN feature is not supported on port-channel, PVLAN, trunk mode, or FEX ports.

Feature limitations

- These commands are not supported for voice VLAN configuration on ports configured with 802.1X:
  - **switchport voice vlan untagged**
  - **switchport voice vlan dot1p**

  If these configurations are present on the 802.1X port, the phone cannot be authorized. To permit authorization, configure the multi-domain port with a specific voice VLAN ID.
- Do not configure the same value for both access VLAN and voice VLAN. If both are set to the same value, change one of them, and then reset the port.
- The data client disconnect feature relies on CDP messages. If the IP phone is unauthorized, or CDP is not enabled, the second port disconnect functionality does not operate as intended.
- In open mode, some initial packets may be dropped because 802.1X and L2FM require time to register the MAC address as secure.
- ACL provided must be identical for both the voice endpoint (phone) and the data endpoint (device behind the phone) on the same port.

- When a MAC address is designated as a drop entry in L2FM, all incoming and outgoing traffic associated with that MAC is blocked, including traffic on other ports. This blocking continues until the inactivity timer expires or the MAC address ages out.
- Open mode only ignores authentication failures; authorization failures are not ignored. If an authorization failure occurs, the port is placed in the **Authorization Failed** state.

ND-ISSU support

All features (Open mode, DACL, COA, and violation restrict) support Non-Disruptive ISSU.

Guidelines and limitations for Per-User DACL support for 802.1x

Use this reference to review the guidelines and limitations for Per-User DACL support for 802.1x.

Follow these guidelines and limitations when configuring Per-User DACL:

Supported platforms

The following switch platforms support per-user DACL for 802.1X:

- Cisco Nexus 9300-FX platform switches
- Cisco Nexus 9300-FX2 platform switches
- Cisco Nexus 9300-FX3, GX, GX2, H2R, and H1 Series switches (from NX-OS Release 10.5(2)F)
- Beginning with Cisco NX-OS Release 10.2(1), the DACL feature is supported on Cisco Nexus 9300-FX/FX2/EX TOR switches.

Feature limitations and configuration notes

Feature limitations and configuration notes:

- Per-user DACL supports IPv4 TCP, UDP, and ICMP ACL rules, but does not support IPv6 ACL rules.
- Per-user DACLs are limited to a single RADIUS response of less than 4KB and a maximum of 32 ACEs.
- This feature does not support standard ACLs on the switch port.
- Only one DACL per port is supported. The maximum number of DACLs supported across a switch is the same as the number of ports in that switch.
- DACL and dynamic VLAN are not supported together on the same port.
- Dynamically modifying DACL content from ISE is not supported. To update, clear the previously applied DACL from the port using the **clear dot1x interface** command, then apply the new one from ISE. This causes transient traffic disruption for all clients on the port.
- Cisco Nexus 9000 series switches in AA FEX mode do not support per-user DACL.
- Per-user DACL is supported for MAB clients only.
- Per-user DACL is supported only on physical ports (regular L2 access ports) and not on trunk, vPC, port-channel and its members, or subinterfaces.

- The maximum limit of the per-user DACL is 4000 ASCII characters.
- MAC-move profiles for the per-user DACL feature are not supported.

Per-User DACL support example

For example, on a Cisco Nexus 9300-FX2 switch running NX-OS Release 10.2(1), a per-user DACL can be applied to a physical access port for a MAB client, supporting up to 32 ACEs in a single RADIUS response.

Guidelines and limitations for critical authentication

Use this reference to review the guidelines and limitations for critical authentication.

- Critical Authentication is supported only for basic MAB clients and is not supported on topologies such as FEX-AA and VxLAN.
- Enabling the **authentication event server dead action authorize** command at all times poses a security risk, as it allows all unauthorized client traffic.
- Beginning with Cisco NX-OS Release 10.1(2), the Critical Authentication feature is supported on Cisco Nexus 9300- FX/FX2/FX3/GX TOR switches.
- Beginning with Cisco NX-OS Release 10.2(1)F, the Critical Authentication feature is supported on the N9K-C9364D-GX2A and N9K-C9332D-GX2B switches.
- Beginning with Cisco NX-OS Release 10.3(2)F, the Critical Authentication feature is supported on Cisco Nexus 9508 switches with N9K-X9788TC-FX and N9K-X97160YC-EX line cards.

Default settings for 802.1x

Use this reference to review the default settings for 802.1x.

- 802.1X is disabled by default on Cisco NX-OS devices.
- The default authentication method for AAA 802.1X is not configured.
- Per-interface 802.1X protocol is disabled (**force-authorized**), allowing normal traffic without authentication.
- Periodic reauthentication is disabled by default.
- The default number of seconds between reauthentication attempts is 3600 seconds.
- The quiet timeout period is 60 seconds, which is the time the device remains in the quiet state after a failed authentication exchange.
- The retransmission timeout period is 30 seconds, representing the wait time for a response to an EAP request/identity frame before retransmitting.
- The maximum retransmission number is 2 times, indicating how many times the device will send an EAP-request/identity frame before restarting authentication.
- The default host mode is single host.

- The supplicant timeout period is 30 seconds, which is the wait time for a response from the supplicant before retransmitting the request.
- The authentication server timeout period is 30 seconds, which is the wait time for a reply from the authentication server before retransmitting the response.

Default 802.1x parameters reference

This section provides a detailed reference table listing the default settings for 802.1X parameters in Cisco NX-OS.

Table 3: Default 802.1x parameters

Parameters	Default
802.1X feature	Disabled
AAA 802.1X authentication method	Not configured
Per-interface 802.1X protocol enable state	Disabled (**force-authorized**) **Note** The port transmits and receives normal traffic without 802.1X-based authentication of the supplicant.
Periodic reauthentication	Disabled
Number of seconds between reauthentication attempts	3600 seconds
Quiet timeout period	60 seconds (number of seconds that the Cisco NX-OS device remains in the quiet state following a failed authentication exchange with the supplicant)
Retransmission timeout period	30 seconds (number of seconds that the Cisco NX-OS device should wait for a response to an EAP request/identity frame from the supplicant before retransmitting the request)
Maximum retransmission number	2 times (number of times that the Cisco NX-OS device will send an EAP-request/identity frame before restarting the authentication process)
Host mode	Single host
Supplicant timeout period	30 seconds (when relaying a request from the authentication server to the supplicant, the amount of time that the Cisco NX-OS device waits for a response before retransmitting the request to the supplicant)
Authentication server timeout period	30 seconds (when relaying a response from the supplicant to the authentication server, the amount of time that the Cisco NX-OS device waits for a reply before retransmitting the response to the server)

Configuring 802.1x

802.1X configuration refers to the process of enabling and setting up the 802.1X authentication feature on Cisco NX-OS and DCNM devices.

- 802.1X provides port-based network access control.
- Configuration steps may differ between Cisco NX-OS and Cisco IOS platforms.
- Familiarity with the specific CLI commands for NX-OS is important for successful configuration.

Key information for configuring 802.1x

This section describes how to configure the 802.1X feature.

Configure the 802.1x feature

This section describes the process for configuring 802.1X.

Procedure

Step 1 Enable the 802.1X feature.
Step 2 Configure the connection to the remote RADIUS server.
Step 3 Enable 802.1X feature on the Ethernet interfaces.

Enable the 802.1x feature

You must enable the 802.1X feature on the Cisco NX-OS device before authenticating any supplicant devices.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminalswitch(config)#
```

Enters global configuration mode.

Step 2 **feature dot1x**

Example:

```
switch(config)#feature dot1x
```

Enables the 802.1X feature. The default is disabled.

Step 3 **exit**

Example:

```
switch(config)#exit
switch#
```

Exits configuration mode.

Step 4 (Optional) **show dot1x**

Example:

```
switch#show dot1x
```

Displays the 802.1X feature status.

Step 5 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Configure AAA authentication methods for 802.1x

You can use remote RADIUS servers for 802.1X authentication. You must configure RADIUS servers and RADIUS server groups and specify the default AAA authentication method before the Cisco NX-OS device can perform 802.1X authentication.

Before you begin

Obtain the names or addresses for the remote RADIUS server groups.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **aaa authentication dot1x default group** *group-list*

Example:

```
switch(config)#aaa authentication dot1x default group rad2
```

Specifies the RADIUS server groups to use for 802.1X authentication.

The *group-list* argument consists of a space-delimited list of group names. The group names are the following:

- **radius** —Uses the global pool of RADIUS servers for authentication.
- *named-group* —Uses the global pool of RADIUS servers for authentication.

Step 3 **exit**

Example:

```
switch(config)#exit
switch#
```

Exits configuration mode.

Step 4 (Optional) **show radius-server**

Example:

```
switch#show radius-server
```

Displays the RADIUS server configuration.

Step 5 (Optional) **show radius-server group** [*group-name*]

Example:

```
switch#show radius-server group rad2
```

Displays the RADIUS server group configuration.

Step 6 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Control 802.1x authentication on an interface

You can control the 802.1X authentication performed on an interface. An interface can have the following 802.1X authentication states:

- **Auto** : Enables 802.1X authentication on the interface.
- **Force-authorized** : Disables 802.1X authentication on the interface and allows all traffic on the interface without authentication. This state is the default.
- **Force-unauthorized** : Disallows all traffic on the interface.

Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **interface ethernet** *slot* / *port*

Example:

```
switch(config)#interface ethernet 2/1
switch(config-if)#
```

Selects the interface to configure and enters interface configuration mode.

Step 3 **dot1x port-control** {**auto** | **force-authorized** | **forced-unauthorized**}

Example:

```
switch(config-if)#dot1x port-control auto
```

Changes the 802.1X authentication state on the interface. The default is force-authorized.

Step 4 **exit**

Example:

```
switch(config-if)#exit
switch(config)#exit
switch#
```

Exits configuration mode.

Step 5 (Optional) **show dot1x all**

Example:

```
switch#show dot1x all
```

Displays all 802.1X feature status and configuration information.

Step 6 (Optional) **show dot1x interface ethernet** *slot* / *port*

Example:

```
switch#show dot1x interface ethernet 2/1
```

Displays 802.1X feature status and configuration information for an interface.

Step 7 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Configure 802.1x for voice VLAN

Beginning with Cisco NX-OS Release 10.5(2)F, you can enable multi-domain 802.1X authentication on a single port.

Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **interface ethernet** *slot* / *port*

Example:

```
switch(config)#interface ethernet 2/1
switch(config-if)#
```

Selects the interface to configure and enters interface configuration mode.

Step 3 **dot1x host-mode multi-domain**

Example:

```
switch(config-if)#dot1x host-mode multi-domain
```

Enables or disables the multi-domain host mode at the interface level.

Use **no** form of this command to disable the multi-domain host mode at the interface level.

Note
Voice clients will be successfully authenticated only on ports with host-mode multi-domain. If the host-mode is anything else, the voice client will fail authentication and be disabled.

Step 4 **exit**

Example:

```
switch(config-if)#exit
switch(config)#exit
switch#
```

Exits configuration mode.

Configure 802.1x open mode and restrict violation action on an interface

802.1X (dot1x) enables secure network access control. Open mode provides authentication flexibility. Configuring the violation action to restrict limits access for unauthorized devices.

Follow these steps to configure 802.1X open mode and violation restrict action:

Before you begin

- You must have access to a device with administrative privileges.
- Identify the target Ethernet interface number and the required VLAN assignments.

Procedure

Step 1 Enter global configuration mode.

Example:

```
switch#configure terminal
switch(config)#
```

Step 2 Select the target interface.

Example:

```
switch(config)#interface Ethernet1/26
switch(config-if)#
```

Step 3 Enable switchport.

Example:

```
switch(config-if)#switchport
```

Step 4 Create an authenticator PAE instance on the interface.

Example:

```
switch(config-if)#dot1x pae authenticator
```

Use the **no** form to remove the PAE instance from the interface.

Note
If an authenticator PAE already exists on the interface the **dot1x pae authenticator** command does not change the configuration on the interface.

Step 5 Set port control to auto.

Example:

```
switch(config-if)#dot1x port-control auto
```

The default is force-authorized.

Step 6 Specify host mode as multi-domain.

Example:

```
switch(config-if)#dot1x host-mode multi-domain
```

Use **no** form of this command to disable the multi-domain host mode at the interface level.

Note
Voice clients will be successfully authenticated only on ports with host-mode multi-domain. If the host-mode is anything else, the voice client will fail authentication and be disabled.

Step 7 Enable MAC Authentication Bypass.

Example:

```
switch(config-if)#dot1x mac-auth-bypass
```

By default bypass is disabled.

Step 8 Enable MAB to authenticate data traffic with the RADIUS server.

Example:

```
switch(config-if)#dot1x authentication order mab
```

The **no** form of this command changes the default authentication method to EAPOL.

Step 9 Set authentication mode to open and violation action to restrict.

Example:

```
switch(config-if)#dot1x authentication mode open
switch(config-if)#dot1x authentication violation action restrict
```

The interface now supports dot1x and MAC authentication, and restricts access for unauthorized devices.

Configure COA

Follow these steps to configure COA:

COA support is required in environments where administrators must update or terminate access policies or user sessions without requiring users to disconnect and reconnect. This procedure configures the RADIUS server and the appropriate AAA services on your device.

Before you begin

- Ensure you have administrative access to the device.
- Obtain the IP address and shared secret for your RADIUS server.
- Confirm network connectivity between your device and the RADIUS server.

Procedure

Step 1 Enable dynamic authorization on the RADIUS server.

Example:

```
switch(config)#aaa server radius dynamic-author
```

Step 2 Configure the RADIUS dynamic author client IP, VRF, and server key.

Example:

```
switch(config-radius-da)#client 192.0.2.10 vrf management server-key 7 "fewhg"
switch(config-radius-da)#server-key 7 "fewhg"
```

Step 3 Specify the RADIUS server host and set the key.

Example:

```
switch(config)#radius-server host 192.0.2.10 key 7 "fewhg" authentication accounting
```

Step 4 Define the AAA group and add the RADIUS server to it.

Example:

```
switch(config)#aaa group server radius ISE_245
switch(config-radius)#server 192.0.2.10
```

```
switch(config-radius)#use-vrf management
switch(config-radius)#source-interface mgmt0
```

Step 5 Configure AAA authentication and accounting to use the RADIUS group.

Example:

```
switch(config)#aaa authentication dot1x default group ISE_245
switch(config)#aaa accounting dot1x default group ISE_245
```

Step 6 Verify COA reauthentication triggered from ISE for data client.

Example:

```
switch#show aaa client radius statistics 192.0.2.10
Dynamic Author Client 192.0.2.10
  COA Statistics
    Requests:             1
    Transactions:         1
    Retransmissions:      0
    Active Transactions:  0
    Ack Responses:        1    ! COA ACK sent to ISE
    Nak Responses:        0
    Invalid Requests:     0
    Errors:               0
```

COA is enabled on the device. The RADIUS server can now send dynamic authorization commands to this device as needed.

Configure the EAP-TLS profile for 802.1x authentication

Beginning with Cisco NX-OS Release 10.4(1)F, you can use EAP-TLS profile for 802.1X authentication.

Before you begin

- Enable the 802.1X feature on the Cisco NX-OS device.
- On the interface, configure the MACsec EAP policy and then attach the **dot1x supplicant eap profile** *eap profile name* . For configuring MACsec EAP policy, see Configure MACsec EAP section.

Procedure

Step 1 **configure terminal**

Enters global configuration mode.

Example:

```
switch#configure terminal
switch(config)#
```

Step 2 **[no] eap profile TLS**

Example:

```
switch(config)#eap profile TLS
switch(config-eap-profile)#
```

Configures the 802.1X EAP profile mode.

The **no** form of the command is used to remove the eap profile.

Step 3 **pki-trustpoint** *trustpoint name*

Example:

```
switch(config-eap-profile)#pki-trustpoint tp1
switch(config-eap-profile)#
```

Specifies the trustpoint to be used.

Step 4 **method** *type*

Enters global configuration mode.

Example:

```
switch(config-eap-profile)#method TLS
switch(config-eap-profile)#
```

Specifies the EAP method to be used.

Step 5 **interface ethernet** *slot / port*

Example:

```
switch(config-eap-profile)#interface ethernet 1/30
switch(config-if)#
```

Selects the interface to configure and enters interface configuration mode.

Step 6 **[no] dot1x supplicant eap profile** *eap profile name*

Enters global configuration mode.

Example:

```
switch(config-if)#dot1x supplicant eap profile TLS
```

Configures the 802.1X supplicant to the EAP profile.

Create or remove an authenticator PAE on an interface

Use this procedure to create or remove an authenticator PAE instance on an interface.

You can create or remove the 802.1X authenticator port access entity (PAE) instance on an interface.



Note By default, the Cisco NX-OS software creates the authenticator PAE instance on the interface when you enable 802.1X on an interface.

Before you begin

Enable the 802.1X feature.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 (Optional) **show dot1x interface ethernet** *slot* / *port*

Example:

```
switch#show do1x interface ethernet 2/1
```

Displays the 802.1X configuration on the interface.

Step 3 **interface ethernet** *slot* / *port*

Example:

```
switch(config)#interface ethernet 2/1
switch(config-if)#
```

Selects the interface to configure and enters interface configuration mode.

Step 4 [**no**] **dot1x pae authenticator**

Example:

```
switch(config-if)#dot1x pae authenticator
```

Creates an authenticator PAE instance on the interface. Use the **no** form to remove the PAE instance from the interface.

Note
If an authenticator PAE already exists on the interface the **dot1x pae authenticator** command does not change the configuration on the interface.

Step 5 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Enable critical authentication

Before you begin

- Enable monitoring of RADIUS.
- Ensure that all servers in the group are RADIUS servers.

Procedure

Step 1 **radius-server test idle-time** *minutes*

Example:

```
switch#configure terminal
switch(config)#radius-server test idle-time 1
```

Specifies parameters for global server monitoring. The default username is test, and the default password is test. The default value for the idle timer is 0 minutes, and the valid range is from 0 to 1440 minutes.

Note
For periodic RADIUS server monitoring, the idle timer value must be greater than 0. If there are multiple servers in the group, set the idle timer to 1 for each server.

Step 2 **radius-server deadtime** *minutes*

Example:

```
switch(config)#radius-server deadtime 1
```

Specifies the number of minutes before the Cisco NX-OS device checks a RADIUS server that was previously unresponsive. The default value is 0 minutes, and the valid range is from 0 to 1440 minutes.

Note
Set the dead time to a value greater than 0 to enable monitoring.

Step 3 **radius-server host** *ipv4-address* **key** [**0** | **6** | **7**] *key-value*

Example:

```
switch(config)#radius-server host 10.105.222.183 key 7 "fewhg" authentication accounting
```

Specifies a RADIUS key for all RADIUS servers. You can specify if the key-value is in clear text format (**0**), type-6 encrypted (**6**), or type-7 encrypted (**7**). The Cisco NX-OS software encrypts a clear text key before saving it to the running configuration. The default format is clear text. The maximum length is 63 characters. By default, no RADIUS key is configured.

Note
If you already configured a shared secret using the **generate type7_encrypted_secret** command, enter it in quotation marks, as shown in the second example. For more information, see Configure the shared secret for RADIUS or TACACS+ .

Step 4 **radius-server host** *ipv4-address* **test idle-time** *minutes*

Example:

```
switch(config)#radius-server host 10.105.222.183 test idle-time 1
```

Specifies parameters for individual server monitoring. The default username is test, and the default password is test. The default value for the idle timer is 0 minutes, and the valid range is from 0 to 1440 minutes.

Note
For periodic RADIUS server monitoring, set the idle timer to a value greater than 0.

Step 5 **aaa group server radius** *group-name*

Example:

```
switch(config)#aaa group server radius ISE_2.4
 switch(config-radius)#
```

Creates a RADIUS server group and enters the RADIUS server group configuration submode for that group. The *group-name* argument is a case-sensitive alphanumeric string with a maximum length of 127 characters.

To delete a RADIUS server group, use the **no** form of this command.

Note
You are not allowed to delete the default system-generated default group (RADIUS).

Step 6 **server** {*ipv4-address* | *ipv6-address* | *hostname*}

Example:

```
switch(config-radius)#server 10.105.222.183
```

Configures the RADIUS server as a member of the RADIUS server group. If the specified RADIUS server is not found, configure it using the **radius-server host** command and retry this command.

Step 7 **use-vrf** *vrf-name*

Example:

```
switch(config-radius)#use-vrf management
```

Specifies the VRF to use to contact the servers in the server group.

Step 8 **source-interface** *interface*

Example:

```
switch(config-radius)#source-interface mgmt 0
switch(config-radius)#exit
```

Configures the global source interface for all RADIUS server groups configured on the device.

Step 9 **authentication event server dead action authorize**

Example:

```
switch(config)#authentication event server dead action authorize
```

Authorizes all the clients when the RADIUS server is unreachable.

Enable periodic reauthentication for an interface

You can enable periodic 802.1X reauthentication on an interface and specify how often it occurs. If you do not specify a time period before enabling reauthentication, the number of seconds between reauthentication defaults to the global value.

Note During the reauthentication process, the status of an already authenticated supplicant is not disrupted.

Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **interface ethernet** *slot* / *port*

Example:

```
switch(config)#interface ethernet 2/1
switch(config-if)#
```

Selects the interface to configure and enters interface configuration mode.

Step 3 **dot1x re-authentication**

Example:

```
switch(config-if)#dot1x re-authentication
```

Enables periodic reauthentication of the supplicants connected to the interface. By default, periodic authentication is disabled.

Step 4 (Optional) **dot1x timeout re-authperiod** *seconds*

Example:

```
switch(config-if)#dot1x timeout re-authperiod 3300
```

Sets the number of seconds between reauthentication attempts. The default is 3600 seconds. The range is from 1 to 65535.

Note
This command affects the behavior of the Cisco NX-OS device only if you enable periodic reauthentication on the interface.

Step 5 **exit**

Example:

```
switch(config-if)#exit
switch(config)#
```

Exits configuration mode.

Step 6 (Optional) **show dot1x all**

Example:

```
switch#show dot1x all
```

Displays all 802.1X feature status and configuration information.

Step 7 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Manually reauthenticate supplicants

You can manually reauthenticate the supplicants for the entire Cisco NX-OS device or for an interface.

Note During the reauthentication process, the status of an already authenticated supplicant is not disrupted.

Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

Procedure

dot1x re-authenticate [**interface** *slot* / *port*]

Example:

```
switch#dot1x re-authenticate interface 2/1
```

Reauthenticates the supplicants on the Cisco NX-OS device or on an interface.

Change 802.1x authentication timers for an interface

Use this procedure to change the 802.1X authentication timers for an interface on a Cisco NX-OS device.

You can change the following 802.1X authentication timers on the Cisco NX-OS device interfaces:

- **Quiet-period timer** : When the Cisco NX-OS device cannot authenticate the supplicant, the switch remains idle for a set period of time and then tries again. The quiet-period timer value determines the idle period. An authentication failure might occur because the supplicant provided an invalid password. You can provide a faster response time to the user by entering a smaller number than the default. The default is the value of the global quiet period timer. The range is from 1 to 65535 seconds.
- **Rate-limit timer** : The rate-limit period throttles EAPOL-Start packets from supplicants that are sending too many EAPOL-Start packets. The authenticator ignores EAPOL-Start packets from supplicants that have successfully authenticated for the rate-limit period duration. The default value is 0 seconds and the authenticator processes all EAPOL-Start packets. The range is from 1 to 65535 seconds.
- **Switch-to-authentication-server retransmission timer for Layer 4 packets** : The authentication server notifies the switch each time that it receives a Layer 4 packet. If the switch does not receive a notification after sending a packet, the Cisco NX-OS device waits a set period of time and then retransmits the packet. The default is 30 seconds. The range is from 1 to 65535 seconds.

- **Switch-to-supplicant retransmission timer for EAP response frames** : The supplicant responds to the EAP-request/identity frame from the Cisco NX-OS device with an EAP-response/identity frame. If the Cisco NX-OS device does not receive this response, it waits a set period of time (known as the retransmission time) and then retransmits the frame. The default is 30 seconds. The range is from 1 to 65535 seconds.
- **Switch-to-supplicant retransmission timer for EAP request frames** : The supplicant notifies the Cisco NX-OS device that it received the EAP request frame. If the authenticator does not receive this notification, it waits a set period of time and then retransmits the frame. The default is the value of the global retransmission period timer. The range is from 1 to 65535 seconds.
- **Inactive period timeout** : When the Cisco NX-OS device remains inactive for a set period of time. The timeout inactivity-period value determines the inactive period. The recommended minimum value is 1800 seconds. You must ensure that the value is less than the value of the re-authentication time.

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

Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

Procedure

Step 1 **interface ethernet** *slot* / *port*

Example:

```
switch#configure terminal
switch(config)#interface ethernet 2/1
switch(config-if)
```

Selects the interface to configure and enters interface configuration mode.

Step 2 (Optional) **dot1x timeout quiet-period** *seconds*

Example:

```
switch(config-if)#dot1x timeout quiet-period 25
```

Sets the number of seconds that the authenticator waits for a response to an EAP-request/identity frame from the supplicant before retransmitting the request. The default is the global number of seconds set for all interfaces. The range is from 1 to 65535 seconds.

Step 3 (Optional) **dot1x timeout ratelimit-period** *seconds*

Example:

```
switch(config-if)#dot1x timeout ratelimit-period 10
```

Sets the number of seconds that the authenticator ignores EAPOL-Start packets from supplicants that have successfully authenticated. The default value is 0 seconds. The range is from 1 to 65535 seconds.

Step 4 (Optional) **dot1x timeout server-timeout** *seconds*

Example:

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

Sets the number of seconds that the Cisco NX-OS device waits before retransmitting a packet to the authentication server. The default is 30 seconds. The range is from 1 to 65535 seconds.

Step 5 (Optional) **dot1x timeout supp-timeout** *seconds*

Example:

```
switch(config-if)#dot1x timeout supp-timeout 20
```

Sets the number of seconds that the Cisco NX-OS device waits for the supplicant to respond to an EAP request frame before the Cisco NX-OS device retransmits the frame. The default is 30 seconds. The range is from 1 to 65535 seconds.

Step 6 (Optional) **dot1x timeout tx-period** *seconds*

Example:

```
switch(config-if)#dot1x timeout tx-period 40
```

Sets the number of seconds between the retransmission of EAP request frames when the supplicant does not send notification that it received the request. The default is the global number of seconds set for all interfaces. The range is from 1 to 65535 seconds.

Step 7 (Optional) **dot1x timeout inactivity-period** *seconds*

Example:

```
switch(config-if)#dot1x timeout inactivity-period 1800
switch(config)#exit
```

Sets the number of seconds the switch can remain inactive. The recommended minimum value is1800 seconds.

Step 8 (Optional) **show dot1x all**

Example:

```
switch#show dot1x all
```

Displays the 802.1X configuration.

Step 9 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Enable MAC authentication bypass

You can enable MAC authentication bypass on an interface that has no supplicant connected.

Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **interface ethernet** *slot* / *port*

Example:

```
switch(config)#interface ethernet 2/1
switch(config-if)
```

Selects the interface to configure and enters interface configuration mode.

Step 3 **dot1x mac-auth-bypass** [**eap**]

Example:

```
switch(config-if)#dot1x mac-auth-bypass
```

Enables MAC authentication bypass. The default is bypass disabled. Use the **eap** keyword to configure the Cisco NX-OS device to use EAP for authorization.

Step 4 **exit**

Example:

```
switch(config-if)#exit
switch(config)#
```

Exits configuration mode.

Step 5 (Optional) **show dot1x all**

Example:

```
switch#show dot1x all
```

Displays all 802.1X feature status and configuration information.

Step 6 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Configure the default 802.1x authentication method using MAB

Configure the default 802.1X authentication method to use MAC Authentication Bypass (MAB) on Cisco NX-OS devices.

Beginning with Cisco NX-OS Release 9.3(5), all traffic that is received on the 802.1X enabled ports can be authenticated only by MAC authentication bypass (MAB). Prior to Cisco NX-OS Release 9.3(5), all traffic was first authenticated by EAPOL and authentication by MAB occurred only after the EAPOL authentication session timed out.

Before you begin

Enable the MAB feature on the Cisco NX-OS device.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **interface ethernet** *slot* / *port*

Example:

```
switch(config)#interface ethernet 2/1
switch(config-if)
```

Selects the interface and enters interface configuration mode.

Step 3 **dot1x mac-auth-bypass**

Example:

```
switch(config-if)#dot1x mac-auth-bypass
```

Enables MAC authentication bypass. The default is bypass disabled.

Step 4 [**no**] **dot1x authentication order mab**

Example:

```
switch(config-if)#dot1x authentication order mab
```

Enables MAB for the authentication of the data traffic with the radius server. The no form of this command changes the default authentication method to EAPOL.

Step 5 **exit**

Example:

```
switch(config-if)#exit
switch(config)#
```

Exits configuration mode.

Step 6 (Optional) **show dot1x all**

Example:

```
switch#show dot1x all
```

Displays the 802.1X feature status and configuration information.

Step 7 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Create a dynamic access list

Before you begin

Ensure the following:

- Pre-program the ACL name (acl-name) with all the ACEs to allow or block specific traffic class for the 802.1X MAB client. The configured ACL name (acl-name) on the device must match the acl-name received from the ISE Server.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **hardware access-list tcam region ing-dacl** *tcam size*

Example:

```
switch#hardware access-list tcam region ing-dacl 256
switch(config)#
```

Specifies the TCAM size. The range is between 0 to 2147483647.

Note
This configuration takes effect only after you enter copy running-config startup-config and reload the device, or reload all line card modules where supported. Multiple TCAM changes can be completed before a single reload.

Step 3 **ip access-list** *blacklist*

Example:

```
switch(config)#ip access-list creative_blacklist
```

Configures the defined blacklist and applies it based on the configured TCAM size.

Step 4 (Optional) **show ip access-list**

Example:

```
switch#show ip access-list creative_blacklist
```

Displays the configured IP access list.

Step 5 (Optional) **show ip access-list dynamic**

Example:

```
switch#show ip access-list dynamic
IP access list creative_blacklist1_new_Ethernet1/1 statistics per-entry
10 permit udp 0000.1b40.ff13 0000.0000.0000 any range bootps bootpc vlan 100 [match=123]
20 permit udp 0000.1b40.ff13 0000.0000.0000 any eq domain vlan 100 [match=456]
30 deny ip 0000.1b40.ff13 0000.0000.0000 any [match=789]
```

Displays the configured IP access list.

Step 6 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Configure Per-User DACLs

You can configure per-user DACLs in the Cisco ISE server. You can then implement it in your authorization policies for control of how different users and groups of users access the network.

Procedure

Step 1 **hardware access-list tcam region ing-dacl**

Example:

```
switch#hardware access-list tcam region ing-dacl
```

Configures TCAM on the switch to create a new DACL-TCAM region.

Note
This configuration takes effect only after you enter copy running-config startup-config and reload the device, or reload all line card modules where supported. Multiple TCAM changes can be completed before a single reload.

Step 2 **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Step 3 **reload**

Example:

```
switch#reload
```

Reloads the Cisco NX-OS device.

What to do next

Configure the DACL for the blocklisted clients on ISE.



Note The ACEs on ISE shouldn't have a deny rule for IP because an implicit deny is internally added for every DACL client.

The blocklist client connects to the 802.1X port and downloads the ACL AV-Pair as part of the radius access-accept message. The received ACL is then applied on the port for the particular client.

For more information about how to configure the DACLs, see the *Configure Permissions for Downloadable ACLs* section in the *Segmentation* chapter of the *Cisco Identity Services Engine Administrator Guide, Release 3.0* .

Enable single host or multiple hosts mode

You can enable single host or multiple hosts mode on an interface.

Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **interface ethernet** *slot* / *port*

Example:

```
switch(config)#interface ethernet 2/1
switch(config-if)
```

Selects the interface to configure and enters interface configuration mode.

Step 3 **dot1x host-mode** {**multi-host** | **single-host**}

Example:

```
switch(config-if)#dot1x host-mode multi-host
```

Configures the host mode. The default is single-host.

Note
Make sure that the **dot1x port-control** interface configuration command is set to **auto** for the specified interface.

Step 4 **dot1x host-mode multi-auth**

Example:

```
switch(config-if)#dot1x host-mode multi-auth
```

Configures the multiple authentication mode. The port is authorized only on a successful authentication of either EAP or MAB or a combination of both. Failure to authenticate will restrict network access.

authentication either EAP or MAB

Step 5 **exit**

Example:

```
switch(config-if)#exit
switch(config)#
```

Exits configuration mode.

Step 6 (Optional) **show dot1x all**

Example:

```
switch#show dot1x all
```

Displays all 802.1X feature status and configuration information.

Step 7 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Disable 802.1x authentication on the Cisco NX-OS device

You can disable 802.1X authentication on the Cisco NX-OS device. By default, the Cisco NX-OS software enables 802.1X authentication after you enable the 802.1X feature. However, when you disable the 802.1X feature, the configuration is removed from the Cisco NX-OS device. The Cisco NX-OS software allows you to disable 802.1X authentication without losing the 802.1X configuration.



Note When you disable 802.1X authentication, the port mode for all interfaces defaults to force-authorized regardless of the configured port mode. When you reenable 802.1X authentication, the Cisco NX-OS software restores the configured port mode on the interfaces.

Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **no dot1x system-auth-control**

Example:

```
switch(config)#no dot1x system-auth-control
```

Disables 802.1X authentication on the Cisco NX-OS device. The default is enabled.

Note
Use the **dot1x system-auth-control** command to enable 802.1X authentication on the Cisco NX-OS device.

Step 3 **exit**

Example:

```
switch(config)#exit
switch#
```

Exits configuration mode.

Step 4 (Optional) **show dot1x**

Example:

```
switch#show dot1x
```

Displays the 802.1X feature status.

Step 5 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Disable the 802.1x feature

Use this procedure to disable the 802.1X feature on a Cisco NX-OS device.

You can disable the 802.1X feature on the Cisco NX-OS device.

When you disable 802.1X, all related configurations are automatically discarded. The Cisco NX-OS software creates an automatic checkpoint that you can use if you reenable 802.1X and want to recover the configuration. For more information, see the *Cisco NX-OS System Management Configuration Guide* for your platform.

Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **no feature dot1x**

Example:

```
switch(config)#no feature dot1x
```

Disables 802.1X.

Caution
Disabling the 802.1X feature removes all 802.1X configuration.

Step 3 **exit**

Example:

```
switch(config)#exit
switch#
```

Exits configuration mode.

Step 4 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Reset the 802.1x interface configuration to the default values

You can reset the 802.1X configuration for an interface to the default values.

Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

Procedure

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

	Command or Action	Purpose
	`switch#configure terminal` `switch(config)#`	

Step 2	**interface ethernet** *slot* / *port*
	Example:
	`switch(config)#interface ethernet 2/1`
	`switch(config-if)`
		Selects the interface to configure and enters interface configuration mode.

Step 3	**dot1x default** **Example:** `switch(config-if)#dot1x default`	Reverts to the 802.1X configuration default values for the interface.

Step 4	**exit**
	Example:
	`switch(config-if)#exit`
	`switch(config)#`
		Exits configuration mode.

Step 5	(Optional) **show dot1x all** **Example:** `switch#show dot1x all`	Displays all 802.1X feature status and configuration information.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch#copy running-config startup-config`	Copies the running configuration to the startup configuration.

Set the maximum Authenticator-to-Supplicant frame for an interface

You can set the maximum number of times that the Cisco NX-OS device retransmits authentication requests to the supplicant on an interface before the session times out. The default is 2 times and the range is from 1 to 10.

Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **interface ethernet** *slot* / *port*

Example:

```
switch(config)#interface ethernet 2/1
switch(config-if)#
```

Selects the interface to configure and enters interface configuration mode.

Step 3 **dot1x max-req** *count*

Example:

```
switch(config-if)#dot1x max-req 3
```

Changes the maximum authorization request retry count. The default is 2 times and the range is from 1 to 10.

Note
Make sure that the **dot1x port-control** interface configuration command is set to **auto** for the specified interface.

Step 4 **exit**

Example:

```
switch(config)#exit
switch#
```

Exits interface configuration mode.

Step 5 (Optional) **show dot1x all**

Example:

```
switch#show dot1x all
```

Displays all 802.1X feature status and configuration information.

Step 6 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Enable RADIUS accounting for 802.1x authentication

You can enable RADIUS accounting for the 802.1X authentication activity.

Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **dot1x radius-accounting**

Example:

```
switch(config)#dot1x radius-accounting
```

Enables RADIUS accounting for 802.1X. The default is disabled.

Step 3 **exit**

Example:

```
switch(config)#exit
switch#
```

Exits configuration mode.

Step 4 (Optional) **show dot1x**

Example:

```
switch#show dot1x
```

Displays the 802.1X configuration.

Step 5 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Configure AAA accounting methods for 802.1x

You can enable AAA accounting methods for the 802.1X feature.

Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

Procedure

Step 1 **configure terminal**

Enters global configuration mode.

Step 2 **aaa accounting dot1x default group** *group-list*

Configures AAA accounting for 802.1X. The default is disabled.

The *group-list* argument consists of a space-delimited list of group names. The group names are the following:

- **radius** —For all configured RADIUS servers.

- *named-group* —Any configured RADIUS server group name.

Step 3 **exit**

Exits configuration mode.

Step 4 (Optional) **show aaa accounting**

Displays the AAA accounting configuration.

Step 5 (Optional) **copy running-config startup-config**

Copies the running configuration to the startup configuration.

This example shows how to configure AAA accounting:

```
switch#configure terminal
switch(config)#aaa accounting dot1x default group radius
switch(config)#exit
switch#show aaa accounting
switch#copy running-config startup-config
```

Set the maximum reauthentication retry count on an interface

You can set the maximum number of times that the Cisco NX-OS device retransmits reauthentication requests to the supplicant on an interface before the session times out. The default is 2 times and the range is from 1 to 10.

Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **interface ethernet** *slot* / *port*

Example:

```
switch(config)#interface ethernet 2/1
switch(config-if)#
```

Selects the interface to configure and enters interface configuration mode.

Step 3 **dot1x max-reauth-req** *retry-count*

Example:

```
switch(config-if)#dot1x max-reauth-req 3
```

Changes the maximum reauthentication request retry count. The default is 2 times and the range is from 1 to 10.

Step 4 **exit**

Example:

```
switch(config)#exit
switch#
```

Exits interface configuration mode.

Step 5 (Optional) **show dot1x all**

Example:

```
switch#show dot1x all
```

Displays all 802.1X feature status and configuration information.

Step 6 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

802.1X configuration verification commands

Use this reference to verify the 802.1X configuration.

Verifying the 802.1X configuration involves using specific show commands to display feature status and configuration information for 802.1X on Cisco NX-OS devices.

Table 4: 802.1X show commands and purpose

Command	Purpose
show dot1x	Displays the 802.1X feature status.
show dot1x all [**details** | **statistics** | **summary**]	Displays all 802.1X feature status and configuration information.
show dot1x interface ethernet *slot* / *port* [**details** | **statistics** | **summary**]	Displays the 802.1X feature status and configuration information for an Ethernet interface.
show running-config dot1x [**all**]	Displays the 802.1X feature configuration in the running configuration.
show startup-config dot1x	Displays the 802.1X feature configuration in the startup configuration.

For detailed information about the fields in the output from these commands, see the *Cisco NX-OS Security Command Reference* for your platform.

Displays EAP-TLS configuration on a port

The following example displays information about the EAP-TLS configuration on the port as both authenticator and supplicant in authorized state:

```
switch#show dot1x int eth 5/6 details
Dot1x Info for Ethernet5/6
-----------------------------------
PAE = AUTHENTICATOR
PortControl = AUTO
HostMode = MULTI HOST
ReAuthentication = Disabled
QuietPeriod = 60
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = 3600 (Locally configured)
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
RateLimitPeriod = 0
InactivityPeriod = 0
Mac-Auth-Bypass = Disabled

Dot1x Info for Ethernet5/6
-----------------------------------
PAE = SUPPLICANT
StartPeriod = 30
AuthPeriod = 30
HeldPeriod = 60
MaxStart = 3

Dot1x Authenticator Client List
-------------------------------
Supplicant = 00:00:5E:00:53:01
Domain = DATA
Auth SM State = AUTHENTICATED
Auth BEND SM State = IDLE
Port Status = AUTHORIZED
Authentication Method = EAP
Authenticated By = Remote Server
Auth-Vlan = 0
DACL-Applied = False
Dot1x Supplicant Client List

-------------------------------
Authenticator = 00:00:5E:00:53:01
Supp SM State = AUTHENTICATED
Supp Bend SM State = IDLE
Port Status = AUTHORIZED
```

802.1X support for VXLAN EVPN

This section describes how to configure 802.1X for VXLAN EVPN.

Guidelines and limitations for 802.1x support for VXLAN EVPN

This section provides the guidelines and limitations for 802.1X support for VXLAN EVPN.

Platform and interface support

- Beginning with Cisco NX-OS Release 9.3(7), 802.1X support for VXLAN EVPN feature is supported for Cisco Nexus 9300-GX platform switches.
- Port channel interfaces or the member ports of the port channel are not supported.
- vPC ports are not supported.
- Cisco Nexus 9504 and Cisco Nexus 9508 platform switches with -R line cards does not support multi-authentication and multi-authentication with VXLAN.
- 802.1X is not supported with Fabric Peering.

MAC move and VLAN behavior

- The current support of the feature uses regular and dynamic EVPN updates on the BGP-EVPN control plane for 802.1X secure MAC updates. As a result, the move across EVPN cannot be prevented even if the global policy is **dot1x mac-move deny**.
- Ensure that the **dot1x mac-move** policy is configured the same across the fabric. There is no configuration validation across the nodes, hence it could lead to unexpected behavior if the configuration policy is not in sync.
- The local to remote MAC moves behavior for the deny and permit modes is permitted. Therefore, the MAC move is permitted even if the deny mode is enabled.
- Ensure that the 802.1X and the port-security ports use different VLANs. The same VLAN cannot be assigned to both ports.
- 802.1X is not VLAN aware and hence having the same MAC in two different VLANs is not possible. Depending on the mac-move mode that is selected, either the MAC is moved to a new VLAN or it is denied.

Authentication and feature limitations

- You cannot configure static and secure MAC together.
- RADIUS change of Authorization is supported for VXLAN EVPN.
- The recommended re-authentication time interval for a scale setup is the default value, which is 3600 seconds.

Configure 802.1x support for VXLAN EVPN

This procedure configures 802.1X for VXLAN EVPN.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
```

Enters global configuration mode.

Step 2 **feature dot1x**

Example:

```
switch(config)#feature dot1x
```

Enables the 802.1X feature. The default is disabled.

Step 3 **dot1x mac-move {permit | deny}**

Example:

```
switch(config)#dot1x mac-move permit
```

The **deny** parameters denies MAC moves. The **permit** parameter permits MAC moves.

Step 4 (Optional) **show running-config dot1x all**

Example:

```
switch#show running-config dot1x all
!Command: show running-config dot1x all
!No configuration change since last restart
!Time: Thu Sep 20 10:22:58 2018
version 9.2(2) Bios:version 07.64
feature dot1x
dot1x system-auth-control
dot1x mac-move deny
interface Ethernet1/1
dot1x host-mode multi-auth
dot1x pae authenticator
dot1x port-control auto
no dot1x re-authentication
dot1x max-req 1
dot1x max-reauth-req 2
dot1x timeout quiet-period 60
dot1x timeout re-authperiod 3600
dot1x timeout tx-period 1
dot1x timeout server-timeout 30
dot1x timeout ratelimit-period 0
dot1x timeout supp-timeout 30
dot1x timeout inactivity-period 0
dot1x mac-auth-bypass
interface Ethernet1/33
dot1x host-mode multi-auth
dot1x pae authenticator
dot1x port-control auto
no dot1x re-authentication
dot1x max-req 1
dot1x max-reauth-req 2
dot1x timeout quiet-period 60
dot1x timeout re-authperiod 3600
dot1x timeout tx-period 1
dot1x timeout server-timeout 30
dot1x timeout ratelimit-period 0
dot1x timeout supp-timeout 30
dot1x timeout inactivity-period 0
dot1x mac-auth-bypass
```

Displays the 802.1X configuration.

802.1X support for VXLAN EVPN verification commands

To display the 802.1X support for VXLAN EVPN configuration information, enter one of the following commands.

Table 5: 802.1X VXLAN EVPN verification commands

Command	Purpose
show running-config dot1x all	Displays 802.1X running configuration.
show dot1x all summary	Displays the interface status.
show dot1x	Displays the default settings.
show dot1x all	Displays additional interface detail.

Example of show running-config dot1x all command

```
switch#show running-config dot1x all
!Command: show running-config dot1x all
!No configuration change since last restart
!Time: Thu Sep 20 10:22:58 2018
version 9.2(2) Bios:version 07.64
feature dot1x
dot1x system-auth-control
dot1x mac-move deny
interface Ethernet1/1
dot1x host-mode multi-auth
dot1x pae authenticator
dot1x port-control auto
no dot1x re-authentication
dot1x max-req 1
dot1x max-reauth-req 2
dot1x timeout quiet-period 60
dot1x timeout re-authperiod 3600
dot1x timeout tx-period 1
dot1x timeout server-timeout 30
dot1x timeout ratelimit-period 0
dot1x timeout supp-timeout 30
dot1x timeout inactivity-period 0
dot1x mac-auth-bypass
interface Ethernet1/33
dot1x host-mode multi-auth
dot1x pae authenticator
dot1x port-control auto
no dot1x re-authentication
dot1x max-req 1
dot1x max-reauth-req 2
dot1x timeout quiet-period 60
dot1x timeout re-authperiod 3600
dot1x timeout tx-period 1
dot1x timeout server-timeout 30
dot1x timeout ratelimit-period 0
dot1x timeout supp-timeout 30
dot1x timeout inactivity-period 0
dot1x mac-auth-bypass
```

Example of the show dot1x all summary command

```
switch#show dot1x all summary
Interface     PAE              Client          Status
--------------------------------------------------------------------
Ethernet1/1    AUTH                none    UNAUTHORIZED
Interface     PAE              Client          Status
--------------------------------------------------------------------
Ethernet1/33    AUTH   00:00:5E:00:53:01      AUTHORIZED
00:00:5E:00:53:02      AUTHORIZED
00:00:5E:00:53:03      AUTHORIZED
00:00:5E:00:53:04      AUTHORIZED
switch#show mac address-table vlan 10
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan
VLAN     MAC Address      Type      age     Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
*   10     0016.5a4c.0004   secure   -         T      F    Eth1/33
*   10     0016.5a4c.0005   secure   -         T      F    Eth1/33
*   10     0016.5a4c.0006   secure   -         T      F    Eth1/33
*   10     0016.5a4c.0007   secure   -         T      F    Eth1/33
switch#show mac address-table vlan 10 (VPC-PEER)
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan
VLAN     MAC Address      Type      age     Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
*   10     0016.5a4c.0004   secure   -         T      F    vPC Peer-Link
*   10     0016.5a4c.0005   secure   -         T      F    vPC Peer-Link
*   10     0016.5a4c.0006   secure   -         T      F    vPC Peer-Link
*   10     0016.5a4c.0007   secure   -         T      F    vPC Peer-Link
switch#show mac address-table vlan 10 (RVTEP)
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan
VLAN     MAC Address      Type      age     Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
C   10     0016.5a4c.0004   dynamic  0         F      F    nve1(192.0.2.1)
C   10     0016.5a4c.0005   dynamic  0         F      F    nve1(192.0.2.1)
C   10     0016.5a4c.0006   dynamic  0         F      F    nve1(192.0.2.1)
C   10     0016.5a4c.0007   dynamic  0         F      F    nve1(192.0.2.1)
```

Example of the show dot1x command

```
switch#show dot1x
 Sysauthcontrol Enabled
Dot1x Protocol Version 2Mac-Move Deny
```

Example of the show dot1x all command

```
switch#show dot1x all
Sysauthcontrol Enabled
Dot1x Protocol Version 2
Mac-Move Deny
Dot1x Info for Ethernet1/1
-----------------------------------
PAE = AUTHENTICATOR
PortControl = AUTO
HostMode = MULTI AUTH
```

```
ReAuthentication = Disabled
QuietPeriod = 60
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = 3600 (Locally configured)
ReAuthMax = 2
MaxReq = 1
TxPeriod = 1
RateLimitPeriod = 0
InactivityPeriod = 0
Mac-Auth-Bypass = Enabled
Dot1x Info for Ethernet1/33
-----------------------------------
PAE = AUTHENTICATOR
PortControl = AUTO
HostMode = MULTI AUTH
ReAuthentication = Disabled
QuietPeriod = 60
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = 3600 (Locally configured)
ReAuthMax = 2
MaxReq = 1
TxPeriod = 1
RateLimitPeriod = 0
InactivityPeriod = 0
Mac-Auth-Bypass = Enabled
```

Critical authentication verification

The following example shows how to view if the critical authentication feature is enabled.

The following example shows how to view if the critical authentication feature is enabled.

```
switch# show dot1x
  Sysauthcontrol               Enabled
  Dot1x Protocol Version       2
  Mac-Move Permit
  Server-Dead-Action-Authorize Enabled
```

If the value of the **Server-Dead-Action-Authorize** parameter is **Enabled** , the critical authentication feature is enabled.

Monitor 802.1x statistics

Monitor 802.1X statistics to review authentication activity and troubleshoot network access issues on Cisco NX-OS devices.

You can display the statistics that the Cisco NX-OS device maintains for the 802.1X activity.

Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

Procedure

show dot1x {**all** | **interface ethernet** *slot* / *port*} **statistics**

Example:

```
switch#show dot1x all statistics
```

Displays the 802.1X statistics.

802.1X port configuration commands

This reference provides the necessary commands to configure 802.1X authentication and illustrates expected system behavior through operational examples.

Configuration Commands

Configure 802.1X for an access port:

```
feature dot1x
aaa authentication dot1x default group rad2
interface Ethernet2/1
  dot1x pae authenticator
  dot1x port-control auto
```

Configure 802.1X for a trunk port:

```
feature dot1x
aaa authentication dot1x default group rad2
interface Ethernet2/1
  dot1x pae authenticator
  dot1x port-control auto
  dot1x host-mode multi-host
```

Note Repeat the **dot1x pae authenticator** and **dot1x port-control auto** commands for all interfaces that require 802.1X authentication.

Operational examples - open mode authentication

Example output from **show dot1x all details** on a port operating in open mode:

```
switch#show dot1x all details
Dot1x Info for Ethernet1/26
-----------------------------------
PAE = AUTHENTICATOR
PortControl = AUTO
HostMode = MULTI-DOMAIN
Mac-Auth-Bypass = Enabled
       AuthenticationOpen = Enabled         <-- Open Mode is Enabled
ViolationRestrict = Enabled

Dot1x Authenticator Client List
```

```
------------------------------
Supplicant = 00:00:5E:00:53:01
Domain = VOICE
Auth SM State = AUTHENTICATED
Port Status = AUTHORIZED
    Authentication Method = MAB
Authenticated By = Open Mode       <-- Authenticated via Open Mode
Voice-Vlan = 111

------------------------------
Supplicant = 00:00:5E:00:53:02
Domain = DATA
Auth SM State = AUTHENTICATED
Port Status = AUTHORIZED
    Authentication Method = MAB
Authenticated By = Open Mode       <-- Authenticated via Open Mode
Auth-Vlan = 110
```

Example output from **show mac address-table** in open mode:

```
switch#show mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan,
(NA)- Not Applicable A â–’ ESI Active Path, S â–’ ESI Standby Path
   VLAN     MAC Address      Type      age     Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
*  110     0030.3030.3030   secure   -         T      F    Eth1/26      <-- Data client on
 access VLAN
*  110     c414.3c97.2246   static   -         F      F    Drop         <-- Phone has drop
 entry on access VLAN
*  111     c414.3c97.2246   secure   -         T      F    Eth1/26      <-- Phone learnt
on voice VLAN
G    -     b44c.90a4.f907   static   -         F      F    sup-eth1(R)
```

Example output from **show mac address-table** when a security violation occurs:

```
switch#show mac address-table
   VLAN     MAC Address      Type      age     Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
*  110     0030.3030.3030   secure   -         T      F    Eth1/26
*  110     0030.3030.3040   static   -         F      F    Drop         <-- Drop entry on
second data client
*  110     c414.3c97.2246   static   -         F      F    Drop
*  111     c414.3c97.2246   secure   -         T      F    Eth1/26
G    -     b44c.90a4.f907   static   -         F      F    sup-eth1(R)
```

COA Examples

COA reauthentication triggered from ISE for data client:

```
switch#show aaa client radius statistics 10.76.80.245
Dynamic Author Client 10.76.80.245
COA Statistics
    Requests: 1
    Transactions: 1
    Retransmissions: 0
    Active Transactions: 0
    Ack Responses: 1                    ! COA ACK sent to ISE
    Nak Responses: 0
    Invalid Requests: 0
    Errors: 0
```

Session state before COA disconnect:

```
switch#show dot1x all summary
           Interface     PAE              Client          Status
-----------------------------------------------------------------
        Ethernet1/26    AUTH   00:00:5E:00:53:01      AUTHORIZED
                               00:00:5E:00:53:02      AUTHORIZED
```

Session state after COA disconnect:

```
switch#show dot1x all summary
           Interface     PAE              Client          Status
-----------------------------------------------------------------
        Ethernet1/26    AUTH   00:00:5E:00:53:01      AUTHORIZED

switch#show aaa client radius statistics 10.76.80.245
COA Statistics
    Requests: 3
    Ack Responses: 3
```

Configuration example for Per-User DACL

Use this reference to review a Per-User DACL configuration example.

Per-User DACL behavior

The per-user DACL is a security feature that allows dynamic application of access control lists to individual clients on a switch port, enabling granular traffic filtering based on client authentication status.

- Filters blocklist traffic by applying DACLs to authenticated clients.
- Identifies blocklist clients when the DACL-Applied parameter is set to true.
- Integrates with ISE to deliver ACLs dynamically to clients.

Viewing Per-User DACL configuration and blocklisted traffic

The following information describes how to verify per-user DACL configuration and view blocklisted traffic on a switch port.

- Use the **show dot1x all summary** and **show dot1x all details** commands to check client authentication and DACL application status.
- Use the **show ip access-list dynamic** command to view blocklisted traffic entries.

Example: Verifying Per-User DACL and blocklisted traffic

The following example shows the per-user DACL configured on one of the ports. When the DACL is applied, the blocklist traffic is filtered out. If the value of the DACL-Applied parameter is true, the client is a blocklist client, which has received an ACL from ISE.

```
switch#show dot1x all summary
Interface      PAE        Client               Status
Ethernet1/1    AUTH       00:00:5E:00:53:01    AUTHORIZED
                          00:00:5E:00:53:02    AUTHORIZED

switch#show dot1x all details
----------------------------
Supplicant = 00:00:5E:00:53:01
Domain = DATA
```

```
Auth SM State = AUTHENTICATED
DACL-Applied = False
------------------------------

Supplicant = 00:00:5E:00:53:02
Domain = DATA
Auth SM State = AUTHENTICATED
DACL-Applied = True
```

The following example shows how to view the blocklisted traffic.

```
switch#show ip access-list dynamic
IP access list DOT1X_Restricted_base_acl_Ethernet1/1_new statistics per-entry fragments
deny-all
  10 permit udp any 3612.6151.2153 0000.0000.0000 any eq 5555 vlan 100 [match=0]
  20 permit udp any 3612.6151.2153 0000.0000.0000 any eq 6666 vlan 100 [match=0]
  30 deny ip any 3612.6151.2153 0000.0000.0000 any vlan 100 [match=0]
```

Additional references for 802.1x

This section includes additional information related to implementing 802.1X.

Standards

Table 6: Standards

Standards	Title
IEEE Std 802.1X- 2004 (Revision of IEEE Std 802.1X-2001)	*802.1X IEEE Standard for Local and Metropolitan Area Networks Port-Based Network Access Control*
RFC 2284	*PPP Extensible Authentication Protocol (EAP)*
RFC 3580	*IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*