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

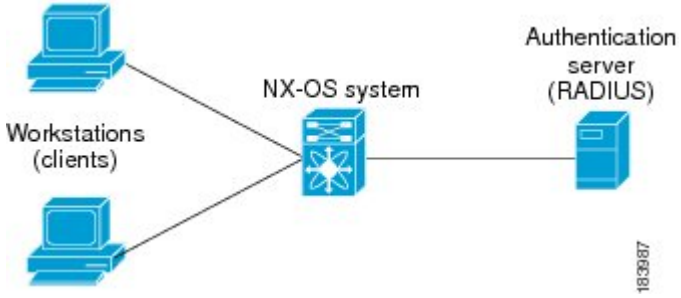
802.1X defines a client-server based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a Cisco NX-OS device port.

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

Device Roles

With 802.1X port-based authentication, the devices in the network have specific roles.

Figure 1: 802.1X Device Roles



The specific roles are as follows:

Supplicant

The client device that requests access to the LAN and Cisco NX-OS device services and responds to requests from the Cisco NX-OS device. The workstation must be running 802.1X-compliant client software such as that offered in the Microsoft Windows XP operating device.

Authentication server

The authentication server performs the actual authentication of the supplicant. The authentication server validates the identity of the supplicant and notifies the Cisco NX-OS device regarding whether the supplicant is authorized to access the LAN and Cisco NX-OS device services. Because the Cisco NX-OS device acts as the proxy, the authentication service is transparent to the supplicant. The Remote Authentication Dial-In User Service (RADIUS) security device with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server, version 3.0. RADIUS uses a supplicant-server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

Authenticator

The authenticator controls the physical access to the network based on the authentication status of the supplicant. The authenticator acts as an intermediary (proxy) between the supplicant and the authentication server, requesting identity information from the supplicant, verifying the requested identity information with the authentication server, and relaying a response to the supplicant. The authenticator includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server.

When the authenticator receives EAPOL frames and relays them to the authentication server, the authenticator strips off the Ethernet header and encapsulates the remaining EAP frame in the RADIUS format. This encapsulation process does not modify or examine the EAP frames, and the authentication server must support EAP within the native frame format. When the authenticator receives frames from the authentication server, the authenticator removes the server's frame header, leaving the EAP frame, which the authenticator then encapsulates for Ethernet and sends to the supplicant.

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

Authentication Initiation and Message Exchange

Either the authenticator (Cisco NX-OS device) or the supplicant (client) can initiate authentication. If you enable authentication on a port, the authenticator must initiate authentication when it determines that the port link state transitions from down to up. The authenticator then sends an EAP-request/identity frame to the

supplicant to request its identity (typically, the authenticator sends an initial identity/request frame followed by one or more requests for authentication information). When the supplicant receives the frame, it responds with an EAP-response/identity frame.

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

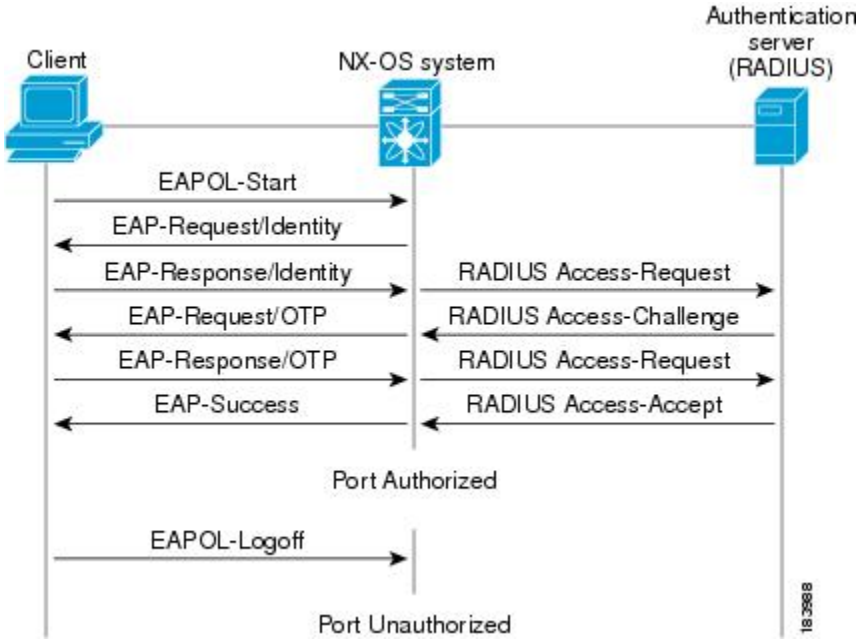
Note If 802.1X is not enabled or supported on the network access device, the Cisco NX-OS device drops any EAPOL frames from the supplicant. If the supplicant does not receive an EAP-request/identity frame after three attempts to start authentication, the supplicant transmits data as if the port is in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

When the supplicant supplies its identity, the authenticator begins its role as the intermediary, passing EAP frames between the supplicant and the authentication server until authentication succeeds or fails. If the authentication succeeds, the authenticator port becomes authorized.

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

Figure 2: Message Exchange

This figure 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.



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

Authenticator PAE Status for Interfaces

When you enable 802.1X on an interface, the Cisco NX-OS software creates an authenticator port access entity (PAE) instance. An authenticator PAE is a protocol entity that supports authentication on the interface. When you disable 802.1X on the interface, the Cisco NX-OS software does not automatically clear the authenticator PAE instances. You can explicitly remove the authenticator PAE from the interface and then reapply it, as needed.

Ports in Authorized and Unauthorized States

The authenticator port state determines if the supplicant is granted access to the network. The port starts in the unauthorized state. In this state, the port disallows 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 to flow normally.

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

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

Ports can have the following authorization states:

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.

If the supplicant is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated supplicant are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the 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.

MAC Authentication Bypass

You can configure the Cisco NX-OS device to authorize a supplicant based on the supplicant MAC address by using the MAC authentication bypass feature. For example, you can enable this feature on interfaces configured for 802.1X that are connected to devices such as printers.

If 802.1X authentication times out while waiting for an EAPOL response from the supplicant, the Cisco NX-OS device tries to authorize the client by using MAC authentication bypass.

When you enable the MAC authentication bypass feature on an interface, the Cisco NX-OS device uses the MAC address as the supplicant identity. The authentication server has a database of supplicant MAC addresses that are allowed network access. After detecting a client on the interface, the Cisco NX-OS device waits for an Ethernet packet from the client. The Cisco NX-OS device sends the authentication server a RADIUS-access/request frame with a username and password based on the MAC address. If authorization succeeds, the Cisco NX-OS device grants the client access to the network.

If an EAPOL packet is detected on the interface during the lifetime of the link, the Cisco NX-OS device determines that the device connected to that interface is an 802.1X-capable supplicant and uses 802.1X authentication (not MAC authentication bypass) to authorize the interface. EAPOL history is cleared if the interface link status goes down.

If the Cisco NX-OS device already authorized an interface by using MAC authentication bypass and detects an 802.1X supplicant, the Cisco NX-OS device does not unauthorize the client connected to the interface. When reauthentication occurs, the Cisco NX-OS device uses 802.1X authentication as the preferred reauthentication process.

Clients that were authorized with MAC authentication bypass can be reauthenticated. The reauthentication process is the same as that for clients that were authenticated with 802.1X. During reauthentication, the port remains in the previously assigned VLAN. If reauthentication is successful, the switch keeps the port in the same VLAN.

If reauthentication is based on the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute [29]) and if the Termination-Action RADIUS attribute (Attribute [29]) action is Initialize (the attribute value is DEFAULT), the MAC authentication bypass session ends, and connectivity is lost during reauthentication. If MAC authentication bypass is enabled and the 802.1X authentication times out, the switch uses the MAC authentication bypass feature to initiate reauthorization. For more information about these AV pairs, see RFC 3580, *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*.

MAC authentication bypass interacts with the following features:

- 802.1X authentication—You can enable MAC authentication bypass only if 802.1X authentication is enabled on the port.
- Port security—You cannot configure 802.1X authentication and port security on the same Layer 2 ports.
- Network admission control (NAC) Layer 2 IP validation—This feature takes effect after an 802.1X port is authenticated with MAC authentication bypass, including hosts in the exception list.

Dynamic VLAN Assignment based on MAC-Based Authentication (MAB)

The Cisco Nexus 9000 Series switches supports dynamic VLAN assignment. After the 802.1x authentication or MAB is completed; before bringing up the port, you may want to (as part of authorization) allow the peer/host to be placed into a particular VLAN based as a result of the authentication. The RADIUS server

typically indicates the desired VLAN by including tunnel attributes within the Access-Accept message. This procedure of getting the VLAN an binding it to the port constitutes to Dynamic VLAN assignment.

VLAN Assignment from RADIUS

After authentication is completed either through 802.1X or MAB, the response from the RADIUS server can have dynamic VLAN information, which can be assigned to a port. This information is present in response from RADIUS server in Accept-Access message in the form of tunnel attributes. For use in VLAN assignment, the following tunnel attributes are sent:

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

All the three parameters must be received for configuring access VLAN.

Single Host and Multiple Hosts Support

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 allows traffic from only one endpoint device on the 802.1X port. Once the endpoint device is authenticated, the Cisco NX-OS device puts the port in the authorized state. When the endpoint device leaves the port, the Cisco NX-OS device put the port back into the unauthorized state. A security violation in 802.1X is defined as a detection of frames sourced from any MAC address other than the single MAC address authorized as a result of successful authentication. In this case, the interface on which this security association violation is detected (EAPOL frame from the other MAC address) will be disabled. Single host mode is applicable only for host-to-switch topology and when a single host is connected to the Layer 2 (Ethernet access port) or Layer 3 port (routed port) of the Cisco NX-OS device.

Only the first host has to be authenticated on the 802.1X port configured with multiple host mode. The port is moved to the authorized state after the successful authorization of the first host. Subsequent hosts are not required to be authorized to gain network access once the port is in the authorized state. If the port becomes unauthorized when reauthentication fails or an EAPOL logoff message is received, all attached hosts are denied access to the network. The capability of the interface to shut down upon security association violation is disabled in multiple host mode. This mode is applicable for both switch-to-switch and host-to-switch topologies.

Supported Topology

The 802.1X port-based authentication supports point-to-point topology.

In this configuration, only one supplicant (client) can connect to the 802.1X-enabled authenticator (Cisco NX-OS device) port. The authenticator detects the supplicant when the port link state changes to the up state. If a supplicant leaves or is replaced with another supplicant, the authenticator changes the port link state to down, and the port returns to the unauthorized state.

About Per-User DACLs

From Cisco NX-OS Release 10.2(1)F, you can download per-user dynamic access control lists (DACLs) from the Cisco ISE Server as policy enforcement after authentication using IEEE 802.1X.

Per-user DACLs can be configured to provide different levels of network access and service to an 802.1X-authenticated user. When the RADIUS server authenticates a user that is connected to an 802.1X port, it retrieves the ACL attributes based on the user identity and sends them to the switch. The switch applies the attributes to the 802.1X port for the duration of the user session. The switch removes the per-user DACL configuration whenever the session is terminated or if the authentication failed.

RADIUS supports per-user attributes, including vendor-specific attributes. These vendor-specific attributes (VSAs) are in the octet-string format and are passed to the switch during the authentication process. The VSAs used for per-user DACLs are `inacl#<n>` for the ingress direction, where the value of `n` is from 1 to 32. The syntax is as follows:

`ip:inacl#<n>=`**`permit | deny`** [*protocol*] [*source_subnet*] [*dest_subnet*] [*operator*][*port*]

Example 1: `ip:inacl#1=permit udp any any eq 5555`

Example 2: `ip:inacl#2=deny udp any any eq 6666`

The switch supports VSAs only in the ingress direction.

Critical Authentication

From Cisco NX-OS Release 10.1(1), the 802.1X critical authentication on a port, accommodates 802.1X users that failed authentication when RADIUS servers in their ISP domain weren't reachable. The critical authentication feature is supported when 802.1X authentication is performed only through RADIUS or ISE servers. If an 802.1X user fails RADIUS authentication, it's still allowed to access the network. You can achieve this by using the **dot1x authentication event server dead action authorize** command. Use the **no** command to disable this feature.

About DACL

Dynamic ACL (DACL) is a single ACL that contains permissions of what users and groups can access. It restricts access to the dot1x MAB client. 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. A single DACL supports all blacklisted MAB clients.

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

Prerequisites for 802.1X

- Cisco Nexus Release 7.0(3)I7(1) software.

The following prerequisites are required for 802.1X Port-based Authentication with EAP-TLS profile:

- PKI Infra is responsible for providing the certificate management for EAP-TLS. This includes
  - Generating an RSA key-pair

- Creation of certificate trustpoint
- Authenticating the CA

- 802.1X needs a remote EAP server such as ISE on the device to provide the EAP-TLS. Local authentication server is not supported.
- Ensure that both the participating devices, the CA server, and Cisco Identity Services Engine (ISE) are synchronized using Network Time Protocol (NTP). If time is not synchronized on all your devices, certificates will not be validated.
- AAA server reachability: For the switches to mutually authenticate each other.
- As the switches do mutual authentication, both of them must have proper AAA configurations and AAA connectivity.

802.1X Guidelines and Limitations

802.1X port-based authentication has the following guidelines and limitations:

- When you upgrade the Cisco Nexus Series switch to Cisco NX-OS Release 9.2(1) using the (dispruptive/non-disruptive) In-Service Software Upgrades (ISSU), you must first disable 802.1x using the **no feature dot1x** command and then enable it using the **feature dot1x** command for multi-authentication to work.
- Beginning with Cisco NX-OS Release 9.2(1), multi-authentication mode is enabled on an 802.1X port. Dynamic VLAN assignment occurs successfully for the first authenticated host. Subsequent authorized (based on user credentials) data hosts are considered successfully authenticated, provided either they have no VLAN assignment or have a VLAN assignment matching the first successfully authenticated host on the port. This ensures that all successfully authenticated hosts on a port are members of the same VLAN. Flexibility of Dynamic VLAN assignment is only provided to the first authenticated host.
- Beginning with Cisco NX-OS Release 9.2(3), 802.1X port-based authentication is supported on FEX-ST and host interface (HIF) ports. IEEE 802.1X port-based authentication support applies to both straight-through and dual-homed FEX.
- Cisco Nexus 9000 Series switches do not support 802.1X on the following:
  - Transit topology set ups
  - vPC ports
  - PVLAN ports
  - L3 (routed) ports
  - Port security
  - Ports that are enabled with CTS and MACsec PSK.
  - 802.1X with LACP port-channels.

Note 802.1X supports static port-channels.

Note Disable 802.1X on vPC ports and all unsupported features.

- The Cisco NX-OS software supports 802.1X authentication only on physical ports.
- Dynamic VLAN assignment is supported only on Cisco Nexus 9300-FX/EX/FX2 Platform switches.
- The Cisco NX-OS software does not work with the CTS or the MACsec PSK features. Global "mac-learn disable" and 802.1X feature are mutually exclusive and cannot be configured together.
- 802.1X is mutually exclusive with the IP Source Guard and uRPF features and cannot be configured together. When you upgrade the Cisco Nexus Series switch to Cisco NX-OS Release 9.2(3), you must disable one of these features.
- During a switch reload, 802.1X does not generate RADIUS accounting stops.
- The Cisco NX-OS software does not support the following 802.1X protocol enhancements:
  - One-to-many logical VLAN name to ID mapping
  - Web authorization
  - Dynamic domain bridge assignment
  - IP telephony
  - Guest VLANs
- In order to prevent reauthentication of inactive sessions, use the authentication timer inactivity command to set the inactivity timer to an interval shorter than the reauthentication interval set with the authentication timer reauthenticate command.
- 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 the error messages.
- In Cisco Nexus Release 9.2(1), tagged EAPOL frames are processed although the VLAN is not configured on the interface and the authentication is successful on the interface for the client.
- Secure mac learned on the orphan port is not synced on the vPC peer.
- Beginning with Cisco NX-OS Release 9.2(1), the MAC authentication bypass is supported on Cisco Nexus 9300-EX/FX/FX2 TOR switches.
- Beginning with Cisco NX-OS Release 9.3(5), 802.1X is supported on Cisco Nexus 9300-FX3 platform switches.
- Beginning with Cisco NX-OS Release 10.1(2), 802.1X is supported on Cisco Nexus 9300-GX platform switches.
- Beginning with Cisco NX-OS Release 10.2(1)F, 802.1X is supported on the N9K-C9364D-GX2A and N9K-C9332D-GX2B switches.
- Beginning with Cisco NX-OS 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.

- The Cisco Nexus C9508 switches with N9K-X9788TC-FX, and N9K-X97160YC-EX line cards does not support the following features with 802.1X :
  - DVLAN
  - DACL
  - FEX-AA
  - VXLAN and mac-move
  - CoA
  - Only MAB supported as authentication method and no EAP
  - Support is for access port with single access VLAN.
- The following platform limitation is applicable only for Cisco Nexus 9000 PX/TX/PQ EoR or ToR switches:
  - When feature 802.1X is configured on a vPC domain, the 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.
- Beginning with Cisco NX-OS 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 9700-EX/FX/GX line cards.
- Beginning with Cisco NX-OS Release 10.4(1)F, Cisco Nexus 9336C-FX2, 93180YC-FX3, 93108TC-FX3P switches and Cisco Nexus 9500 switches with X9716D-GX line cards supports 802.1X port-based authentication using EAP/EAP-TLS (to carry certificates) for uplink ports where MACSec is required with the following limitations:
  - EAP-TLS supported TLS version is 1.2.
  - Support for Single EAP profile per switch and multiple interfaces can use the same EAP profile.
  - No support for MAC Move profiles of supplicants.
  - Authenticator profile will be enabled for L3 ports, trunks ports, vPC for only MACsec EAP-TLS.

Note 802.1X authenticator functionality for MAB/EAP clients will not be supported for L3 or Trunk and vPC ports.

  - EAP-TLS is supported for only EAP on MACsec configured interfaces.
  - EAP-TLS is supported only on Multi-Host mode.
  - DACL/Critical AUTH/FEX-AA and other 802.1X features on 802.1X MACsec enabled interfaces is not supported.
  - EAP-TLS is supported for only remote authentication (ISE/RADIUS – ISE 3.0 and above), local authentication is not supported.
  - The following order must be followed for EAP-TLS configuration to function properly:

- The **macsec eap policy** command must be configured first and then the **dot1x supplicant eap profile TLS** command.
- For the **no** form of the EAP profile command, the **dot1x supplicant eap profile TLS** command must be removed first and then the **macsec eap policy** command.
- For **no feature** command, We recommend to remove the 802.1X feature first and then MACsec feature to avoid DME DB inconsistencies.

- Single EAP profile which is configured across the switch can be applied on different interface.
- If **macsec eap policy** is configured on interfaces, the regular 802.1X authenticator function or commands are not supported.
- Peer to peer MACsec enabled switches must have same 802.1X or MACsec configurations.
- If the commands are different (like one side should-secure and another side must-secure), the behavior will be undefined and must trigger shut/no-shut to recover.
- Once MACsec secure session is created with a trust point and eap profile is added to interface:
  - Removal of trustpoint configuration will not delete MACsec session.
  - Removal of 802.1X supplicant command will not delete MACsec session.
  - MACsec session will be deleted only on MACsec interface specific command removal.
- MACsec PKI is supported on switches without any intermediate switches or hops and should be directly connected.
- MACsec PKI (802.1X EAP-TLS) mode does not support EoR Stateful Switch Over (SSO).
- EAP-TLS is supported only on the following interface types:
  - L2/L3 ports, Port-channel member ports, trunk ports and breakout ports
  - Unsupported interface types – there is no command level restriction.
- Number of MACsec sessions supported depends on the physical interface scale.

- Beginning with Cisco NX-OS Release 10.4(3)F, EAP-TLS supports Transport Layer Security version 1.3 and 1.2 on Cisco Nexus switches.

Note If the RADIUS server is not capable of TLS v1.3, then TLS v1.2 is used, as it is the minimum supported version.

Guidelines and Limitations for Per-User DACL Support for 802.1X

- The following switch platforms support this feature:
  - Cisco Nexus 9300-EX platform switches

  - Cisco Nexus 9300-FX platform switches
  - Cisco Nexus 9300-FX2 platform switches

- Per-user DACL supports the IPv4 TCP, UDP, and ICMP ACL rules, but doesn't support IPv6 ACL rules.
- Per-user DACLs are limited to single RADIUS response which is less than 4KB and maximum number of ACEs supported is 32.
- This feature doesn't support standard ACLs on the switch port.
- Only one DACL per port is supported. The maximum number of DACLs supported across a switch is same as the number of ports in that switch.
- DACL and dynamic VLAN aren't supported together on the same port.
- Dynamically modifying DACL content from ISE is not supported. To achieve this, clear the previously applied DACL from the port using the **clear dot1x interface** command and then the new one from ISE is applied. With that, all the clients on this port will have transient traffic disruption.
- Cisco Nexus 9000 series switches in AA FEX mode do not support the per-user DACL.
- Per-user DACL supports only MAB and multi-auth host mode.
- Like all other Nexus 9000 802.1x features, per-User DACL is also supported only on physical ports, that is, regular L2 access ports and not supported on trunk, vPC, port-channel and its members, and subinterfaces.
- Like all other Nexus 9000 ACLs applied on the switch, the maximum limit of the per-user DACL is 4000 ASCII characters.
- MAC-move profiles for the per user DACL feature isn't supported.
- Beginning with Cisco NX-OS Release 10.2(1), the DACL feature is supported on Cisco Nexus 9300-FX/FX2/EX TOR switches.

Guidelines and Limitations for Critical Authentication

- Critical authentication supports only for basic MAB clients and not supported on topologies like FEX-AA and VxLAN.
- Enabling the **authentication event server dead action authorize** command all the time is a security risk because all the unauthorized client traffic is allowed.
- Beginning with Cisco NX-OS Release 10.1(2), the critical authentication feature is supported on Cisco Nexus 9300-EX/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

This table lists the default settings for 802.1X parameters.

Table 1: 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

This section describes how to configure the 802.1X feature.

Process for Configuring 802.1X

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.

Enabling the 802.1X Feature

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

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(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.

Configuring 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

	Command or Action	Purpose

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.

Controlling 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

	Command or Action	Purpose

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)# 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:**	Displays 802.1X feature status and configuration information for an interface.

	Command or Action	Purpose
	`switch# show dot1x interface ethernet 2/1`	
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring EAP-TLS

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**. For configuring MACsec EAP policy, see Configuring MACsec EAP section.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

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*
	Example:
	`switch(config-eap-profile)# method TLS`
	`switch(config-eap-profile)#`
		Enters global configuration mode.
		Specifies the EAP method to be used.

Step 5	**interface ethernet** *slot / port* **Example:**	Selects the interface to configure and enters interface configuration mode.

	Command or Action	Purpose
	`switch(config-eap-profile)# interface ethernet 1/30` `switch(config-if)#`	
Step 6	**[no] dot1x supplicant eap profile** *eap profile name* **Example:** `switch(config-if)# dot1x supplicant eap profile`	Enters global configuration mode. Configures the 802.1X supplicant to the EAP profile.

Creating or Removing an Authenticator PAE 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

	Command or Action	Purpose

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.

	Command or Action	Purpose
		Note If an authenticator PAE already exists on the interface the **dot1x pae authentication** command does not change the configuration on the interface.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Enabling Critical Authentication

Before you begin

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

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**radius-server test idle-time** *minutes* **Example:** `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 3	**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.

	Command or Action	Purpose
		Note Set the dead time to a value greater than 0 to enable monitoring.
Step 4	**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 Configuring the Shared Secret for RADIUS or TACACS+.
Step 5	**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 6	**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 7	**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.

	Command or Action	Purpose
Step 8	**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 9	**source-interface** *interface* **Example:** `switch(config-radius)# source-interface mgmt 0`	Configures the global source interface for all RADIUS server groups configured on the device.

Step 10	**exit**
	Example:
	`switch(config-radius)# exit`
	`switch(config)#`
		Exits the RADIUS server group configuration submode.

Step 11	**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.

Enabling 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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot/port* **Example:**	Selects the interface to configure and enters interface configuration mode.

	Command or Action	Purpose
	`switch(config)# interface ethernet 2/1` `switch(config-if)#`	
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(config)# show dot1x all`	Displays all 802.1X feature status and configuration information.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Manually Reauthenticating 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

	Command or Action	Purpose
Step 1	**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.

Changing 802.1X Authentication Timers for an Interface

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 it that 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

	Command or Action	Purpose

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	(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 4	(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 5	(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 6	(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 7	(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 8	(Optional) **dot1x timeout inactivity-period** *seconds* **Example:**	Sets the number of seconds the switch can remain inactive. The recommended minimum value is1800 seconds.

	Command or Action	Purpose
	`switch(config-if)# dot1x timeout inactivity-period 1800`	

Step 9	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 10	(Optional) **show dot1x all** **Example:** `switch# show dot1x all`	Displays the 802.1X configuration.
Step 11	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Enabling 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

	Command or Action	Purpose

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:**	Exits configuration mode.

	Command or Action	Purpose
	`switch(config-if)# exit` `switch(config)#`	
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(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring the Default 802.1X Authentication Method - MAB

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

	Command or Action	Purpose

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.

	Command or Action	Purpose

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(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Creating Dynamic Access Lists

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

	Command or Action	Purpose

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(config)# hardware access-list tcam region ing-dacl 256`
	`switch(config)#`
		Specifies the TCAM size. The range is between 0 to 2147483647.

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.

	Command or Action	Purpose
Step 4	(Optional) **show ip access-list** **Example:** `switch(config)# ip access-list creative_blacklist1`	Displays the configured IP access list.

Step 5	(Optional) **show ip access-list dynamic**
	Example:
	`switch(config)# 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 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(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring 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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**hardware access-list tcam region ing-dacl** **Example:** `switch(config)# hardware access-list tcam region ing-dacl`	Configures TCAM on the switch to create a new DACL-TCAM region.

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

	Command or Action	Purpose
Step 4	**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*.

Enabling 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

	Command or Action	Purpose

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.

	Command or Action	Purpose
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(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Disabling 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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose
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.

Disabling the 802.1X Feature

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

	Command or Action	Purpose

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.

	Command or Action	Purpose

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.

Resetting 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:
	`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 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(config)# show dot1x all`	Displays all 802.1X feature status and configuration information.

	Command or Action	Purpose
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Setting 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

	Command or Action	Purpose

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.

	Command or Action	Purpose
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Enabling 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

	Command or Action	Purpose

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.

Configuring 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

	Command or Action	Purpose
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.

Example

This example shows how to enable the 802.1x feature:

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

Setting 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

	Command or Action	Purpose

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(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Verifying the 802.1X Configuration

To display 802.1X information, perform one of the following tasks:

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.

Command	Purpose
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.

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

```
switch(config)# 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 = C4:B2:39:2C:EE:50
                   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 = C4:B2:39:2C:EE:50
        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

The following are the guidelines and limitations for 802.1X support for VXLAN EVPN:

- 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.
- 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, we cannot prevent the move across EVPN 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.
- You cannot configure static and secure MAC together.
- Cisco Nexus 9504 and Cisco Nexus 9508 platform switches with -R line cards does not support multi-authentication and multi-authentication with VXLAN.
- 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.
- 802.1X is not supported with Fabric Peering

Configuring 802.1X Support for VXLAN EVPN

This procedure configures 802.1X for VXLAN EVPN.

Procedure

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

	Command or Action	Purpose
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:**	Displays the 802.1X configuration.

```
switch(config)# 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
```

Verifying the 802.1X Support for VXLAN EVPN

To display the 802.1X support for VXLAN EVPN configuration information, enter one of the following 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   00:16:5A:4C:00:07      AUTHORIZED
                                00:16:5A:4C:00:06      AUTHORIZED
                                00:16:5A:4C:00:05      AUTHORIZED
                                00:16:5A:4C:00:04      AUTHORIZED
switch#
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#
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#
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(67.67.67.67)
C   10     0016.5a4c.0005   dynamic  0         F      F    nve1(67.67.67.67)
C   10     0016.5a4c.0006   dynamic  0         F      F    nve1(67.67.67.67)
C   10     0016.5a4c.0007   dynamic  0         F      F    nve1(67.67.67.67)
```

Example of the show dot1x command

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

Verifying Critical Authentication

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

```
switch(config)# 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.

Monitoring 802.1X

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

	Command or Action	Purpose
Step 1	**show dot1x** {**all** | **interface ethernet** *slot*/*port*} **statistics** **Example:** `switch# show dot1x all statistics`	Displays the 802.1X statistics.

Configuration Example for 802.1X

The following example shows how to 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
```

The following example shows how to 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.

Configuration Example for Per-User DACL

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       36:12:61:51:21:52    AUTHORIZED
                          36:12:61:51:21:53    AUTHORIZED

switch# show dot1x all details
------------------------------

Supplicant = 36:12:61:51:21:52
Domain = DATA
```

```
Auth SM State = AUTHENTICATED
DACL-Applied = False
------------------------------
Supplicant = 36:12:61:51:21:53
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.

Related Documents

Related Topic	Document Title
Cisco NX-OS Licensing	*Cisco NX-OS Licensing Guide*
Command reference	
VRF configuration	

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*