Configuring 802.1X

This chapter contains the following sections:

Information 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.

The specific roles are as follows:

Supplicant

The client device that requests access to the LAN and Cisco Nexus 1000v device services and responds to requests from the Cisco Nexus 1000v device. The workstation must be running 802.1X-compliant client software such as that offered in the Microsoft Windows operating device.

Note To resolve Windows XP network connectivity and Cisco 802.1X port-based authentication issues, read the Microsoft Knowledge Base article at this URL: http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

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 Nexus 1000v device regarding whether the supplicant is authorized to access the LAN and Cisco Nexus 1000v device services. Because the Cisco Nexus 1000v 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 vEthernet 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 vEthernet and sends to the supplicant.

Note The Cisco Nexus 1000v device can only be an 802.1X authenticator.

Authentication Initiation and Message Exchange

Either the authenticator (Cisco Nexus 1000v 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.

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.

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

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.

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 Nexus 1000v device puts the port in the authorized state. When the endpoint device leaves the port, the Cisco Nexus 1000v 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 (vEthernet access port) of the Cisco Nexus 1000v 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 host-to-switch topologies.

Licensing Requirements for 802.1X

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	802.1X requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you.

Prerequisites for 802.1X

802.1X Guidelines and Limitations

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

- All the Dot1x configurations are supported only in the port-profile mode.
- Use of **dot1x pae authenticator** command in any form is not recommended. Use of this command might result in undefined behavior in Dot1x state machine. You can use **dot1x port-control auto** command in the port-profile to control Dot1x configuration.
- The Cisco Nexus 1000v software supports 802.1X authentication only on vEthernet ports.
- The Cisco Nexus 1000v software does not support 802.1X authentication on port channels or subinterfaces.
- When you enable 802.1X authentication, supplicants are authenticated before any other Layer 2 or Layer 3 features are enabled on an vEthernet interface.
- The Cisco NX-OS software supports 802.1X authentication only on vEthernet interfaces that are in a port channel, a trunk, or an access port.
- The Cisco NX-OS software does not support single host mode on trunk interfaces .
- The Cisco NX-OS software does not support MAC address authentication bypass.

- 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
  - Mac authentication bypass
  - 802.1x specific SNMP MIBs
- For RADIUS Accounting, only the start and stop messages with basic attributes such as Username, Network Device Name, Calling Station ID(MAC Address), NAS IP Address (Network device IP address), and AAA Session ID are supported.
- Configuring VSM as SXP speaker with CTS device tracking option populates the ISE server with IP-SGT mapping that can be used instead of the Framed IP address for Radius Accounting.

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)

Parameters	Default
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 vEthernet interfaces.

Enabling the 802.1X Feature

You must enable the 802.1X feature on the Cisco Nexus 1000v 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.

	Command or Action	Purpose

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. **Note** The **show dot1x** command is available if the 802.1X feature is enable. You can also use the **show feature** command to verify the status of the 802.1X feature.
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 Nexus 1000v 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.

	Command or Action	Purpose

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 Nexus 1000v device.

Procedure

	Command or Action	Purpose

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

Step 2	**port-profile type vethernet** *port_profile_name* **Example:**	Selects the port-profile to configure and enters port-profile configuration mode.

	Command or Action	Purpose
	`switch(config)# port-profile type vethernet SAMPLE_PORT_PROFILE_1` `switch(config-port-prof)#`	
Step 3	**dot1x port-control** {**auto** | **force-authorized** | **forced-unauthorized**} **Example:** `switch(config-port-prof)# dot1x port-control auto`	Changes the 802.1X authentication state on the interface. The default is force-authorized.

Step 4	**exit**
	Example:
	`switch(config-port-prof)# 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 vethernet** *port* **Example:** `switch# show dot1x interface vethernet 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.

Enabling Periodic Reauthentication for Port-Profile

You can enable periodic 802.1X reauthentication on a Virtual Ethernet (virtual 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 Nexus 1000v device.

Procedure

	Command or Action	Purpose

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

Step 2	**port-profile type vethernet** *port_profile_name*
	Example:
	`Switch(config)# port-profile type vethernet SAMPLE_PORT_PROFILE_1`
	`switch(config-port-prof)#`
		Selects the port-profile to configure and enters port-profile configuration mode.

Step 3	**dot1x re-authentication** **Example:** `switch(config-port-prof)# dot1x re-authentication`	Enables periodic reauthentication of the supplicants connected to the virtual interface. By default, periodic authentication is disabled.
Step 4	(Optional) **dot1x timeout re-authperiod** *seconds* **Example:** `switch(config-port-prof)# 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 Nexus 1000v device only if you enable periodic reauthentication on the virtual interface.

Step 5	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config-port-prof)#`
		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 Reauthenticating Supplicants

You can manually reauthenticate the supplicants for the entire Cisco Nexus 1000v device or for a virtual 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 Nexus 1000v device.

Procedure

	Command or Action	Purpose
Step 1	**dot1x re-authenticate** [**vethernet** *port*] **Example:** `switch# dot1x re-authenticate vethernet 1`	Reauthenticates the supplicants on the Cisco Nexus 1000v device or on a virtual interface.

Manually Initializing 802.1X Authentication

You can manually initialize the authentication for all supplicants on a Cisco Nexus 1000v device or for a specific interface.

Note Initializing the authentication clears any existing authentication status before starting the authentication process for the client.

Before you begin

Enable the 802.1X feature on the Cisco Nexus 1000v device.

Procedure

	Command or Action	Purpose
Step 1	**dot1x initialize** [**interface vethernet** *port*] **Example:** `switch# dot1x initialize interface vethernet 1`	Initializes 802.1X authentication on the Cisco Nexus 1000v device or on a specified interface.

Changing 802.1X Authentication Timers for a Port-Profile

You can change the following 802.1X authentication timers on the Cisco Nexus 1000v switch interfaces:

Quiet-period timer
When the Cisco Nexus 1000v switch 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.

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 Nexus 1000v switch 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 Nexus 1000v switch 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 Nexus 1000v switch 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.

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 Nexus 1000v switch.

Procedure

	Command or Action	Purpose

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

Step 2	**port-profile type vethernet** *port_profile_name*
	Example:
	`switch(config)# port-profile type vethernet SAMPLE_PORT_PROFILE_1`
	`switch(config-port-prof)#`
		Selects the port-profile to configure and enters port-profile configuration mode.

Step 3	(Optional) **dot1x timeout quiet-period** *seconds* **Example:** `switch(config-port-prof)# 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*	Sets the number of seconds that the authenticator ignores EAPOL-Start packets

	Command or Action	Purpose
	Example: `switch(config-port-prof)# dot1x timeout ratelimit-period 10`	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-port-prof)# dot1x timeout server-timeout 60`	Sets the number of seconds that the Cisco Nexus 1000v switch 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-port-prof)# dot1x timeout supp-timeout 20`	Sets the number of seconds that the Cisco Nexus 1000v switch waits for the supplicant to respond to an EAP request frame before the Cisco Nexus 1000v switch 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-port-prof)# 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	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 9	(Optional) **show dot1x all** **Example:** `switch# show dot1x all`	Displays the 802.1X configuration.
Step 10	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Enabling Single Host or Multiple Hosts Mode

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

Before you begin

Enable the 802.1X feature on the Cisco Nexus 1000v switch.

Procedure

	Command or Action	Purpose

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

Step 2	**port-profile type vethernet** *port_profile_name*
	Example:
	`switch(config)# port-profile type vethernet SAMPLE_PORT_PROFILE_1`
	`switch(config-port-prof)#`
		Selects the port-profile to configure and enters port-profile configuration mode.

Step 3	**dot1x host-mode** {**multi-host** | **single-host**} **Example:** `switch(config-port-prof)# dot1x host-mode multi-host`	Configures the host mode. The default is single-host. **Note** Make sure that the **dot1x port-control** port-profile configuration command is set to **auto** for the specified virtual port-profile.

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.

Enabling 802.1x Guest VLAN

Guest VLAN configuration is used to provide limited network accessibility to a VM user when the VM does not have 802.1x capability or when the VSM is not available (Headless mode).

Before you begin

Enable the 802.1X feature on the Cisco Nexus 1000v switch.

Procedure

	Command or Action	Purpose

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

Step 2	**port-profile type vethernet** *port_profile_name*
	Example:
	`switch(config)# port-profile type vethernet SAMPLE_PORT_PROFILE_1`
	`switch(config-port-prof)#`
		Selects the port-profile to configure and enters port-profile configuration mode.

Step 3	**authentication event no-response action authorize vlan** *vlan-id* **Example:** `switch(config-port-prof)#authentication event no-response action authorize vlan 1309`	Configures and enables a guest VLAN on a particular port-profile. **Note** To disable the guest VLAN feature on a particular port-profile, use the no form of this command.

Step 4	**exit**
	Example:
	`switch(config-port-prof)# 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) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Disabling 802.1X Authentication

You can disable 802.1X authentication on the Cisco Nexus 1000v switch device. By default, the Cisco Nexus 1000v 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 Nexus 1000v switch. The Cisco Nexus 1000v 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 Nexus 1000v software restores the configured port mode on the interfaces.

Before you begin

Enable the 802.1X feature on the Cisco Nexus 1000v switch.

Procedure

	Command or Action	Purpose

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 Nexus 1000v switch. The default is enabled. **Note** Use the **dot1x system-auth-control** command to enable 802.1X authentication on the Cisco Nexus 1000v switch.

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.
Step 5	(Optional) **show dot1x** **Example:** `switch(config-port-profile)# show dot1x`	Displays the 802.1X feature status.

Disabling the 802.1X Feature

You can disable the 802.1X feature on the Cisco Nexus 1000v switch.

When you disable 802.1X, all related configurations are automatically discarded. The Cisco Nexus 1000v 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 Nexus 1000V for VMware vSphere System Management Configuration Guide, Release 5.x* for your platform.

Before you begin

Enable the 802.1X feature on the Cisco Nexus 1000v switch.

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.

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 Port-Profile Configuration to the Default Values

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

Before you begin

Enable the 802.1X feature on the Cisco Nexus 1000v switch.

Procedure

	Command or Action	Purpose

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

Step 2	**port-profile type vethernet** *port_profile_name*
	Example:
	`switch(config)# port-profile type vethernet SAMPLE_PORT_PROFILE_1`
	`switch(config-port-prof)#`
		Selects the port-profile to configure and enters port-profile configuration mode.

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

	Command or Action	Purpose

Step 4	**exit**
	Example:
	`switch(config-port-prof)# 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.

Setting the Maximum Authenticator-to-Supplicant Frame Retransmission Retry Count for a Port-Profile

You can set the maximum number of times that the Cisco Nexus 1000v switch retransmits authentication requests to the supplicant on a virtual 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 Nexus 1000v switch.

Procedure

	Command or Action	Purpose

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

Step 2	**port-profile type vethernet** *port_profile_name*
	Example:
	`switch(config)# port-profile type vethernet SAMPLE_PORT_PROFILE_1`
	`switch(config-port-prof)#`
		Selects the port-profile to configure and enters port-profile configuration mode.

Step 3	**dot1x max-req** *count* **Example:** `switch((config-port-prof))# dot1x max-req 3`	Changes the maximum authorization request retry count. The default is 2 times and the range is from 1 to 10.

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

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

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

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 Nexus 1000v switch.

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.

	Command or Action	Purpose
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.
Step 5	(Optional) **show dot1x** **Example:** `switch# show dot1x`	Displays the 802.1X 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 Nexus 1000v switch.

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 a Port-Profile

You can set the maximum number of times that the Cisco Nexus 1000v switch retransmits reauthentication requests to the supplicant on a virtual 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 Nexus 1000v switch.

Procedure

	Command or Action	Purpose

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

Step 2	**port-profile type vethernet** *port_profile_name*
	Example:
	`switch(config)# port-profile type vethernet SAMPLE_PORT_PROFILE_1`
	`switch(config-port-prof)#`
		Selects the port-profile to configure and enters port-profile configuration mode.

Step 3	**dot1x max-reauth-req** *retry-count* **Example:** `switch(config-port-prof)# 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) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.
Step 6	(Optional) **show dot1x all** **Example:** `switch# show dot1x all`	Displays all 802.1X feature status and configuration information.

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 vethernet *port* [**details** | **statistics** | **summary**]	Displays the 802.1X feature status and configuration information for an vEthernet 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 Nexus 1000V for VMware vSphere Command Reference, Release 5.x* for your platform.

Monitoring 802.1X

You can display the statistics that the Cisco Nexus 1000v switch maintains for the 802.1X activity.

Before you begin

Enable the 802.1X feature on the Cisco Nexus 1000v switch.

Procedure

	Command or Action	Purpose
Step 1	**show dot1x** {**all** | **interface vethernet** *port*} **statistics** **Example:** `switch(config-port-prof)# show dot1x all statistics`	Displays the 802.1X statistics.

Configuration Example for 802.1X

The following example shows how to configure 802.1X on the port-profile for a port-profile:

```
configure terminal
feature dot1x
aaa authentication dot1x default group SAMPLE_RADIUS_USERS_GROUP_1
port-profile type vethernet SAMPLE_PORT_PROFILE_1
```

```
dot1x port-control auto
```

Note Repeat **dot1x port-control auto** command for all the port-profiles that requires 802.1X authentication.

802.1X integration with Cisco Trustsec

With this release, 802.1X can function with Cisco Trustsec (CTS) feature. For detailed information about Cisco Trustsec, see Configuring Cisco Trustsec. You need advanced license for Nexus 1000v to enable CTS feature. When you configure CTS with 802.1X:

- If dot1x port-control is configured together with CTS, dot1x SGT is obtained from radius server and it takes priority.
- Ensure that the **cts manual** command is configured before configuring the **dot1x port-control auto** command while configuring port-profile for CTS.

The following is a sample configuration to integrate 802.1X feature with CTS.

```
Before enabling 802.1X and CTS commands on a port-profile:
------------------------------------------------------------
port-profile type vethernet SAMPLE_PORT_PROFILE_1
switchport mode access
switchport access vlan 1309
no shutdown
state enabled
vmware port-group

Enabling 802.1X and CTS on a port-profile:
----------------------------------------
First configure 'cts manual' and then configure 'dot1x port-control auto' as below:
switch# configure terminal
switch(config)# port-profile type vethernet SAMPLE_PORT_PROFILE_1
switch(config-port-prof)# cts manual
switch(config-port-prof-cts-manual)# exit
switch(config-port-prof)# dot1x port-control auto
switch(config-port-prof)# end
switch#
```