

802.1X and Port Control Commands

This module describes the commands used for 802.1X Authentication.

Note All commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router that is introduced from Cisco IOS XR Release 6.3.2. References to earlier releases in Command History tables apply to only the Cisco NCS 5500 Series Router.

Note

- Starting with Cisco IOS XR Release 6.6.25, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 560 Series Routers.
- Starting with Cisco IOS XR Release 6.3.2, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router.
- References to releases before Cisco IOS XR Release 6.3.2 apply to only the Cisco NCS 5500 Series Router.
- Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:
  - N540-28Z4C-SYS-A
  - N540-28Z4C-SYS-D
  - N540X-16Z4G8Q2C-A
  - N540X-16Z4G8Q2C-D
  - N540X-16Z8Q2C-D
  - N540-12Z20G-SYS-A
  - N540-12Z20G-SYS-D
  - N540X-12Z16G-SYS-A
  - N540X-12Z16G-SYS-D

This module provides command line interface (CLI) commands for 802.1X Authentication Commands.

For detailed information about 802.1X authentication commands, configuration tasks, and examples, see the *802.1X Port-Based Authentication* chapter in the *System Security Configuration Guide for Cisco NCS 5500 Series Routers*.

- dot1x host-mode, on page 3
- show dot1x, on page 4

dot1x host-mode

To allow multiple hosts or MAC addresses on a single port, use the `host-mode` command under authenticator mode in dot1x profile.

host-mode { **multi-auth** | **multi-host** | **single-host** }

Syntax Description

multi-auth	Multiple authentication mode
multi-host	Multiple host mode
single-host	Single host mode

Command Default

The default is `multi-auth` mode.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.2.1	This command was introduced.

Use the following steps to configure 802.1X host-modes:

```
Router# configure terminal
Router(config)# dot1x profile {name}
Router(config-dot1x-auth)# pae {authenticator}
Router(config-dot1x-auth-auth)# host-mode
multi-auth multiple authentication mode
multi-host multiple host mode
single-host single host mode
```

show dot1x

To display whether 802.1X authentication has been configured on the device, use the **show dot1x** command in privileged EXEC mode.

show dot1x [**interface** *interface-type interface-id* | **detail**]

Syntax Description

interface *interface-type interface-id*	Displays the information for the specified interface ID.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
dot1x	read

Example

The **show dot1x interface** command verifies whether the 802.1X port-based authentication is successful or not for the supplicant to proceed with the traffic flow on the configured interface.

```
Router# show dot1x interface HundredGigE 0/0/1/0 detail

Dot1x info for HundredGigE 0/0/1/0
------------------------------------------------------------
Interface short name      : Hu0/0/1/0
Interface handle          : 0x4080
Interface MAC             : 021a.9eeb.6a59
Ethertype                 : 888E
PAE                       : Authenticator
Dot1x Port Status         : AUTHORIZED
Dot1x Profile             : test_prof
L2 Transport              : FALSE
Authenticator:
   Port Control           : Enabled
   Config Dependency      : Resolved
   Eap profile            : None
   ReAuth                 : Disabled
Client List:
      Supplicant          : 027E.15F2.CAE7
 Programming Status       : Add Success
      Auth SM State       : Authenticated
      Auth Bend SM State  : Idle
      Last authen time    : 2018 Dec 11 17:00:30.912
```

```
      Last authen server  : Remote radius server
      Time to next reauth : reauth not enabled
MKA Interface:
   Dot1x Tie Break Role   : NA (Only applicable for PAE role both)
   EAP Based Macsec       : Disabled
   MKA Start time         : NA
   MKA Stop time          : NA
   MKA Response time      : NA
```