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*.

authenticator

To configure authenticator parameters and to enter the authenticator configuration sub mode, use the **authenticator** command in dot1x profile configuration sub mode. To remove this configuration, use the **no** form of this command.

authenticator { **eap profile** *profile-name* | **host-mode** { **multi-auth** | **multi-host** | **single-host** } | **server dead action** { **auth-fail** | **auth-retry** } | **timer** { **mab-retry-time** *retry-timer-value* | **reauth-time** { *reauth-timer-value* | **server** } } }

Syntax Description

eap	Enables local Extensible Authentication Protocol (EAP) server for MACSec.
profile-name	Specifies the EAP profile name, in WORD.
host-mode	Sets the host mode for authentication. **Note** Only **single-host** mode is supported.
server dead action	Sets the action to be taken when the remote AAA server is unreachable. You can set it as either to retry the authentication or to consider it as authentication failure.
timer	Sets various timers for authentication.
mab-retry-time	Sets the interval, in seconds, after which the router re-initiates an authentication attempt for the MAC authentication bypass (MAB) clients, in scenarios where previous authentication failed or if the RADIUS server was unreachable. Range is 60 to 300, default being 60.
reauth-time	Sets the interval, in seconds, after which the router automatically initiates re-authentication process with the RADIUS server. Range is 60 to 5184000 (2 months).
server	Sets the re-authentication interval on the router as per the value specified by the RADIUS server. Minimum expected value is 60 seconds, default being 1 hour.

Command Default

None

Command Modes

Dot1x profile configuration mode

Command History

Release	Modification
Release 24.3.1	This command was modified to include the **mab-retry-time** timer option as part of the MAB feature.
Release 6.4.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
config-services	read, write

Examples

This example shows how to set the authenticator mode as **single-host**:

```
Router# configure
Router(config)# dot1x profile test_profile
Router(config-dot1x-test_profile)# authenticator host-mode single-host
Router(config-dot1x-test_profile)# commit
```

This example shows how to set the authenticator retry timer for MAB clients:

```
Router#configure
Router(config)#dot1x profile test_mab
Router(dot1xx-test_mab)#authenticator timer mab-retry-time 60
Router(dot1xx-test_mab)#commit
```

Related Commands

Command	Description
dot1x profile, on page 7	Configures IEEE 802.1X profile parameters and enters dot1x profile configuration sub mode.

clear mab

To clear the MAC authentication bypass (MAB) session or statistics, use the **clear mab** command in the XR EXEC mode.

clear mab { **session** *intf-type if-name* [**client** *mac-address*] | **statistics** { **interface** *intf-type if-name* | **location** *node* } }

Syntax Description

session	Clears MAB session related to a specific interface.
statistics	Clears MAB statistics

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 24.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
interface	read

The following example shows how to clear MAB statistics on an interface:

```
Router#clear mab statistics interface gigabitEthernet 0/0/0/0
```

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
```

dot1x profile

To configure IEEE 802.1X profile parameters and to enter dot1x profile configuration sub mode, use the **dot1x profile** command in XR Config mode. To remove this configuration, use the **no** form of this command.

dot1x profile *profile-name* { **authenticator** | **mab** | **pae** { **authenticator** | **both** | **supplicant** } | **supplicant eap** [**profile** *profile-name*] }

Syntax Description

profile-name	Specifies the dot1x profile name, in WORD, with a maximum of 63 characters.
authenticator	Enters the sub mode for authenticator.
mab	Enables MAC authentication bypass (MAB) feature.
pae	Sets 802.1X PAE type
supplicant	Enters the sub mode for supplicant.
eap	Configures EAP supplicant parameters.

Command Default

None

Command Modes

Global ConfigurationXR Config

Command History

Release	Modification
Release 24.3.1	This command was modified to include the **mab** option as part of MAC authentication bypass (MAB) feature.
Release 6.3.2	This command was introduced.

Usage Guidelines

Prior to the introduction of MAB feature, the dot1x configuration in these routers was only a key-provider for MACSec functionality, and not a mechanism for port control on the router.

See the *MACSec Using EAP-TLS Authentication* chapter and the *Implementing MAC Authentication Bypass* chapter in the *System Security Configuration Guide for Cisco NCS 5500 Series Routers*, for more details.

Task ID

Task ID	Operations
config-services	read, write

Examples

This example shows how to configure 802.1X profile on the router:

```
Router# configure
Router(config)# dot1x profile test_profile
Router(config-dot1x-test_profile)# pae both
Router(config-dot1x-test_profile)# authenticator timer reauth-time 3600
```

```
Router(config-dot1x-test_profile)# supplicant eap profile test-eap-profile
Router(config-dot1x-test_profile)# commit
```

This example shows how to enable MAB feature to implement port controlling:

```
Router#configure
Router(config)#dot1x profile test_mab
Router(dot1xx-test_mab)#mab
Router(dot1xx-test_mab)#commit
```

Related Commands

Command	Description
authenticator, on page 3	Configures authenticator parameters and enters the authenticator configuration sub 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
```

show mab

To display the MAC authentication bypass (MAB) feature status of the client, use the **show mab** command in the XR EXEC mode.

show mab { **detail** [**location** *node*] | **interface** *intf-type if-name* [**detail**] | **statistics** { **interface** *intf-type if-name* | **location** *node* } | **summary** [**location** *node*] }

Syntax Description

detail	Displays detailed MAB information.
interface	Displays MAB information of the interface.
statistics	Displays MAB statistics
summary	Displays summary of the MAB information.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 24.3.1	This command was introduced.

Usage Guidelines

Based on the client authorization status, the **show mab** command output displays one of these values in the authorization status field:

- Authorizing
- Authorized
- Authorized (Server unreachable)
- Authorized (Server send fail)
- Unauthorized (Server Reject)
- Unauthorized (Server unreachable)
- Unauthorized (Server send fail)

Task ID

Task ID	Operation
interface	read

The following examples show how to verify client MAB information at various levels:

```
Router#show mab summary
Fri Apr  1 16:37:32.340 IST
```

```
NODE: node0_0_CPU0
================================================================================
   Interface-Name        Client          Status
================================================================================
     Gi0/0/0/0         1122.3344.5566   Authorized

Router#


Router#show mab detail
Fri Apr  1 16:37:37.140 IST

NODE: node0_0_CPU0

MAB info for GigabitEthernet0/0/0/0
------------------------------------------------------------------
InterfaceName       : Gi0/0/0/0
InterfaceHandle     : 0x00000060
HostMode            : single-host
PortControl         : Enabled
PuntState           : Stop Success
PuntSummary         : Punt disabled
Client:
  MAC Address       : 1122.3344.5566
  Status            : Authorized
  SM State          : Terminate
  ReauthTimeout     : 60s, Remaining 0 day(s), 00:00:46
  RetryTimeout      : 60s, timer not started yet
  AuthMethod        : PAP (remote)
  LastAuthTime      : 2022 Apr 01 16:37:23.634
  ProgrammingStatus : Add Success

Router#


Router#show mab interface gigabitEthernet 0/0/0/0 detail
Fri Apr  1 16:38:31.543 IST
MAB info for GigabitEthernet0/0/0/0
------------------------------------------------------------------
InterfaceName       : Gi0/0/0/0
InterfaceHandle     : 0x00000060
HostMode            : single-host
PortControl         : Enabled
PuntState           : Stop Success
PuntSummary         : Punt disabled
Client:
  MAC Address       : 1122.3344.5566
  Status            : Authorized
  SM State          : Terminate
  ReauthTimeout     : 60s, Remaining 0 day(s), 00:00:51
  RetryTimeout      : 60s, timer not started yet
  AuthMethod        : PAP (remote)
  LastAuthTime      : 2022 Apr 01 16:38:23.640
  ProgrammingStatus : Add Success
Router#



Router#show mab statistics interface gigabitEthernet 0/0/0/0
Fri Apr  1 16:41:23.011 IST
InterfaceName         : GigabitEthernet0/0/0/0
------------------------------------------------------------------
MAC Learning:
  RxTotal             : 0
```

```
  RxNoSrcMac          : 0
  RxNoIdb             : 0
Port Control:
  EnableSuccess       : 1
  EnableFail          : 0
  UpdateSuccess       : 0
  UpdateFail          : 0
  PuntStartSuccess    : 0
  PuntStartFail       : 0
  PuntStopSuccess     : 1
  PuntStopFail        : 0
  AddClientSuccess    : 1
  AddClientFail       : 0
  RemoveClientSuccess : 0
  RemoveClientFail    : 0
Client                :
  MAC Address         : 1122.3344.5566
  Authentication:
    Success           : 1406
    Fail              : 0
    Timeout           : 0
    AAA Unreachable   : 0
Router#
```