

# 802.1X and Port Control Commands

This module describes the 802.1X and port control commands.

For detailed information about port control using MAC Authentication Bypass (MAB), the related configuration tasks, and examples, see the *Implementing MAC Authentication Bypass* chapter in the *System Security Configuration Guide for Cisco ASR 9000 Series RoutersSystem Security Configuration Guide for Cisco 8000 Series Routers*.


- authenticator, on page 2
- clear mab, on page 4
- dot1x profile, on page 5
- show mab, on page 7
- show dot1x port authentication, on page 10

# 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.<br>**Note**<br>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.<br>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.<br>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.<br>Minimum expected value is 60 seconds, default being 1 hour. |

## Command Default

None

## Command Modes

Dot1x profile configuration mode

## Command History

| Release | Modification |
|---|---|
| Release 7.3.4<br>Release 7.5.2 | This command was modified to include the **mab-retry-time** timer option as part of the MAB feature. |
| Release 7.0.12 | 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 5 | 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 EXEC modeXR 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

EXEC modeXR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 7.3.4 | This command was introduced. |
| Release 7.5.2 | |

## 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 profile

To configure IEEE 802.1X profile parameters and to enter dot1x profile configuration sub mode, use the **dot1x profile** command in Global Configuration modeXR 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 7.3.4<br>Release 7.5.2 | This command was modified to include the **mab** option as part of MAC authentication bypass (MAB) feature. |
| Release 7.0.12 | 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 Port Control* chapter in the *System Security Configuration Guide for Cisco ASR 9000 Series RoutersSystem Security Configuration Guide for Cisco 8000 Series Routers* respectively, for details of 802.1X profile and MAB feature.

## 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 2 | Configures authenticator parameters and enters the authenticator configuration sub mode. |

# show mab

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

EXEC modeXR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 7.3.4 | This command was introduced. |
| Release 7.5.2 | |

## 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#
```

# show dot1x port authentication

To view the 802.1X authentication information for ports on the router, use the **show dot1x port authentication** command in the EXEC modeXR EXEC mode.

**show dot1x port authentication** [ **detail** [ **location** *node* ] | **interface** *intf-type port* [ **detail** | **statistics** ] | **statistics** [ **location** *node* ] | **summary** [ **location** *node* ] ]

## Syntax Description

| | |
|---|---|
| **detail** | Displays details of all 802.1X or MAB-enabled interfaces and respective clients. |
| **interface** | Specifies the name of the interface configured for 802.1X or MAB. |
| **statistics** | Displays a location-based port authentication statistics. |
| **summary** | Displays summary of all 802.1X or MAB-enabled interfaces and respective clients. |
| **location** *node* | Specifies card location of the 802.1X process instance. |

## Command Default

None

## Command Modes

EXEC modeXR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 25.3.1 | This command was modified to include the **statistics** option. |

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

| Task ID | Operation |
|---|---|
| interface | read |

```
Router#show dot1x port authentication
Thu Feb  6 05:50:00.086 UTC

NODE: node0_2_CPU0
======================================================================
     Interface           Client         Method        Status
======================================================================
     Hu0/2/0/6         ac4a.6730.0620     mab        Authorized
```

This example shows that the authentication falls back to MAB when 802.1X authentication fails.

```
Router#show dot1x port authentication detail
Thu Feb  6 05:50:32.509 UTC

NODE: node0_2_CPU0
```

```
Port Authentication Info for Hu0/2/0/6
------------------------------------------------------------------
Interface Handle         : 0x80001c0
Interface State          : Up
Port Status              : Authorized (1/1)
Profile                  : test_auth_mab
Method List              : dot1x, mab
Client :
 MAC Address             : ac4a.6730.0620
 Status                  : Authorized
 Programming Status      : Add Success
 Unauthorized Timer      : 60s, timer off
 Method:
  dot1x                  : Failed
  mab                    : Success
```

This example shows how to display the 802.1X port authentication statistics on you router.

```
Router#show dot1x port authentication statistics

NODE: node0_RP0_CPU0
 COA:
  Total             :   Req: 1     ACK: 1     NAK: 0
  Reauth-last       :   Req: 1     ACK: 1     NAK: 0
  Reauth-rerun      :   Req: 0     ACK: 0     NAK: 0
  Internal-IPC      :   Req: 0     ACK: 0     NAK: 0
                        ClientNotFound: 0     RspTimeout : 0
  CMD Handler:
   CtxNotFound      : 0
   TidMismatch      : 0
  RateLimit:
   ActiveCtxCount   : 0
   MaxCtxCount      : 128
  NAK ClientNotFound: 0
  NAK RateLimit     : 0
  ACK send fail     : 0
  NAK send fail     : 0
  Invalid CSID      : 0
  Invalid NASportID : 0
  Invalid CMD       : 0
  Internal Error    : 0
```