CHAPTER

7

Cisco 900 Series Integrated Services Routers Software Configuration Guide

Configuring Identity Features on Layer 3 Interface

This chapter describes the identity features supported on the Onboard Gigabit Ethernet Layer 3 ports of the Cisco 900 Integrated Services Router (ISR).

This chapter contains the following sections:

• Authentication Methods, page 57
• Controlling Port Authorization State, page 59
• Flexible Authentication, page 61
• Host mode, page 61
• Open Access, page 62
• Control-Direction (Wake-on-LAN), page 62
• Preauthentication Access Control List, page 64
• Downloadable Access Control List, page 65
• Filter-ID or Named Access Control List, page 65
• IP Device Tracking, page 65

Note

Critical authentication, which is also known as Inaccessible Authentication Bypass or AAA Fail Policy, does not support the Identity features on the Onboard Gigabit Ethernet Layer 3 ports.

Authentication Methods

Identity features support various types of authentication methods that are suitable for different kinds of end hosts and users. The two methods that are mainly used are:

• IEEE 802.1X
• MAC Authentication Bypass (MAB)
Configuring the IEEE 802.1X

This example shows how to configure the IEEE 802.1X on the Cisco 900 ISR:

Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0
Router(config-if)# authentication port-control auto
Router(config-if)# dot1x pae authenticator
Router(config-if)# end
Router#

Use the `show authentication sessions` command to verify the configuration:

Router# show authentication sessions

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC Address</th>
<th>Method</th>
<th>Domain</th>
<th>Status</th>
<th>Session ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1</td>
<td>000d.e105.c771</td>
<td>dot1x</td>
<td>DATA</td>
<td>Authz Success</td>
<td>0303030300000000000BA04</td>
</tr>
</tbody>
</table>

```
Router# show authentication sessions interface Gi1

Interface: GigabitEthernet1
MAC Address: 0201.0201.0201
IP Address: Unknown
User-Name: testUser1
Status: Authz Success
Domain: DATA
Oper host mode: single-host
Oper control dir: both
Authorized By: Authentication Server
Vlan Group: N/A
AAA Policies: 
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0303030300000000000BA04
Acct Session ID: 0x00000001
Handle: 0x6D000001

Runnable methods list:
Method     State
dot1x      Authc Success
```

Router#

Configuring the MAC Authentication Bypass (MAB)

This example shows how to configure the MAB:

Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0
Router(config-if)# authentication port-control auto
Router(config-if)# mab
Router(config-if)# end
Router#

Use the `show authentication sessions` command to verify the configuration:

Router# show authentication sessions

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC Address</th>
<th>Method</th>
<th>Domain</th>
<th>Status</th>
<th>Session ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1</td>
<td>0201.0201.0201</td>
<td>mab</td>
<td>DATA</td>
<td>Authz Success</td>
<td>030303030000000004002500A8</td>
</tr>
</tbody>
</table>
Controlling Port Authorization State

You can control the port authorization by using the following methods:

- **Force-authorized** - This is the default setting that disables IEEE 802.1X and causes a port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without IEEE 802.1X-based authentication of the client.

- **Force-unauthorized** - This causes a port to remain in the unauthorized state, ignoring all the authentication attempts made by a client. A router cannot provide authentication services to clients through the interface.

- **Auto** - This enables IEEE 802.1X authentication and causes a port to start in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPoL) frames to be sent and received through a 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. The router requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the router with the help of the client's MAC address. If the client is successfully authenticated, the port state changes to authorized, and all the frames from the authenticated client are allowed through the port. If authentication fails, the port remains in the unauthorized state, but authentication can be retried.
Configuring the Controlling Port Authorization State

This example shows how to configure the Controlling Port Authorization state:

Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0
Router(config-if)# authentication port-control {auto | force-authorized | force-unauthorized}
Router(config-if)# mab
Router(config-if)# end
Router#

Use the show authentication sessions and show dot1x commands to verify the Controlling Port Authorization state:

Router# show authentication sessions

Interface       MAC Address     Method   Domain     Status           Session ID
Gi1            (unknown)       dot1x    DATA       Authz Success   030303030000000A002CFCBC

Router# show authentication sessions interface gi1

Interface:  GigabitEthernet1
MAC Address:  Unknown
IP Address:  Unknown
Status:  Authz Success
Domain:  DATA
Oper host mode:  single-host
Oper control dir:  both
Authorized By:  Authentication Server
Vlan Group:  N/A
Session timeout:  N/A
Idle timeout:  N/A
Common Session ID:  030303030000000A002CFCBC
Acct Session ID:  0x0000000D
Handle:  0x7C00000B

Runnable methods list:

<table>
<thead>
<tr>
<th>Method</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x</td>
<td>Authc Success</td>
</tr>
</tbody>
</table>

Router# show dot1x interface g0

Dot1x Info for GigabitEthernet0

-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = FORCEAUTHORIZED
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Router# show authentication sessions

Interface       MAC Address     Method   Domain     Status           Session ID
Gi1            (unknown)       dot1x    DATA       Authz Failed     0303030300000009002AB7FC

Router# show authentication sessions interface gi0

Interface:  GigabitEthernet0
Mac Address: Unknown  
IP Address: Unknown  
Status: Authz Failed  
Domain: DATA  
Oper host mode: single-host  
Oper control dir: both  
Session timeout: N/A  
Idle timeout: N/A  
Common Session ID: 030303030000009002AB7FC  
Acct Session ID: 0x0000000C  
Handle: 0x8B00000A

Runnable methods list:  
Method    State  
dot1x    Authc Failed  

Router#show dot1x interface g0  
Dot1x Info for GigabitEthernet0  
-------------------------------  
PAE              = AUTHENTICATOR  
PortControl      = FORCE_UNAUTHORIZED  
ControlDirection = Both  
HostMode         = SINGLE_HOST  
QuietPeriod      = 60  
ServerTimeout    = 0  
SuppTimeout      = 30  
ReAuthMax        = 2  
MaxReq           = 2  
TxPeriod         = 30

Flexible Authentication

Flexible Authentication sequencing allows a user to enable all or some authentication methods on a router port and specify the order in which the methods should be executed.

Configuring Flexible Authentication

For more information about configuring of Flexible Authentication, see:  

Host mode

Only single-host mode is supported for the Identity features on the Onboard Gigabit Ethernet Layer 3 ports. In single-host mode, only one client can be connected to the IEEE 802.1X-enabled router port. The router detects the client by sending an EAPol frame when the port link state changes to up state. If a client leaves or is replaced with another client, the router changes the port link state to down, and the port returns to the unauthorized state.
Open Access

The Open Access feature allows clients or devices to gain network access before authentication is performed. This is primarily required for the Preboot eXecution Environment (PXE) scenario where a device is required to access the network before PXE times out and downloads a bootable image, which contains a supplicant.

Configuring Open Access

This example shows how to configure Open Access:

Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0
Router(config-if)# authentication open
Router(config-if)# end
Router#

Control-Direction (Wake-on-LAN)

When the router uses IEEE 802.1X authentication with Wake-on-LAN (WoL), the router forwards traffic to the unauthorized IEEE 802.1X ports, including the magic packets. While the port is unauthorized, the switch continues to block ingress traffic other than EAPol packets. The host can receive packets, but cannot send packets to other devices in the network.

Configuring Control-Direction (Wake-on-LAN)

This example shows how to configure Control-Direction (Wake-on-LAN):

Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0
Router(config-if)# authentication control-direction both
Router(config-if)# end
Router#
Use the **show authentication sessions** and **show dot1x** commands to verify the default control-direction setting—both:

```
Router#show authentication sessions interface Gi0
Interface:  GigabitEthernet0
MAC Address:  0201.0201.0201
IP Address:  Unknown
User-Name:  testUser1
Status:  Authz Success
Domain:  DATA
Oper host mode:  single-host
Oper control dir:  both
Authorized By:  Authentication Server
Vlan Group:  N/A
AAA Policies:
Session timeout:  N/A
Idle timeout:  N/A
Common Session ID:  03030303000000000000BA04
Acct Session ID:  0x00000001
Handle:  0x6D000001

Runnable methods list:
Method   State
dot1x   Authc Success

Router#
```

```
Router#show dot1x int g0
Dot1x Info for GigabitEthernet0
-----------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```
Use the show authentication sessions and show dot1x commands to verify the authentication control-direction setting-in:

Router#show authentication sessions interface gi0
   Interface: GigabitEthernet0
   MAC Address: 0201.0201.0201
   IP Address: Unknown
   User-Name: testUser1
   Status: Authz Success
   Domain: DATA
   Oper host mode: single-host
   Oper control dir: in
   Authorized By: Authentication Server
   Vlan Group: N/A
   AAA Policies:
     Session timeout: N/A
     Idle timeout: N/A
     Common Session ID: 030303030000000C00310024
     Acct Session ID: 0x0000000F
     Handle: 0x8C00000D

Runnable methods list:
   Method   State
   dot1x    Authc Success

Router#show dot1x interface g0
Dot1x Info for GigabitEthernet0
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = In
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Preauthentication Access Control List

When Open-Access is installed, we recommend that a default port access control list (ACL) is configured on the authenticator. The ACL allows the end point to get a minimum access to the network to get its IP Address and running.

Configuring the Preauthentication Access Control List

For information about preconfiguring ACL, see:

Downloadable Access Control List

A Downloadable ACL is also referred to as dACL. For a dACL to work on a port, the ip device tracking feature should be enabled and the end point connected to the port should have an IP address assigned. After authentication on the port, use the `show ip access-list privileged EXEC` command to display the downloaded ACL on the port.

Filter-ID or Named Access Control List

Filter-Id also works as a dACL, but the ACL commands are configured on the authenticator. Authentication, authorization, and accounting (AAA) provides the name of the ACL to the authenticator.

IP Device Tracking

The IP Device Tracking feature is required for the dACL and Filter-ID features to function. To program a dACL or Filter-ID in a device, IP address is required. IP device tracking provides the IP address of the corresponding device to the Enterprise Policy Manager (EPM) module to convert the dACLs to each user by adding the IP address to them.