Configuring Identity Features on Layer 3 Interface

This chapter describes the identify features supported on the Onboard Gigabit Ethernet Layer 3 ports of the Cisco 1921 Integrated Services Router (ISR).

This chapter contains the following sections:

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

Perform these steps to configure the IEEE 802.1X on the Cisco 1921 ISR.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot / port*
4. **authentication port-control auto**
5. **dot1x pae authenticator**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** *slot/port* **Example:** `Router(config)# interface gigabitethernet 0/0`	Enters interface configuration mode.
Step 4	**authentication port-control auto** **Example:** `Router(config-if)# authentication port-control auto`	Enables the manual control of the port authorization state.
Step 5	**dot1x pae authenticator** **Example:** `Router(config-if)#dot1x pae authenticator`	Configures the port as an IEEE 802.1x Port Access Entity (PAE) authenticator.

Step 6	**end**
	
	Example:
	`Router(config-if)# end`
	`Router#`
		Returns to privileged EXEC mode.

Verifying the IEEE 802.1X

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

```
c1921#show authentication sessions
```

```
Interface      MAC Address     Method   Domain   Status         Session ID
Gi0/1          000d.e105.c771  dot1x    DATA     Authz Success  0303030300000000000BA04

c1921#show authentication sessions interface Gi0/1
            Interface:  GigabitEthernet0/1
          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

c1921#
```

Configuring the MAC Authentication Bypass (MAB)

Perform these steps to configure the MAB.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot / port*
4. **authentication port-control auto**
5. **mab**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** *slot/port* **Example:** `Router(config)# interface gigabitethernet 0/0`	Enters interface configuration mode.
Step 4	**authentication port-control auto** **Example:** `Router(config-if)# authentication port-control auto`	Enables the manual control of the port authorization state.
Step 5	**mab** **Example:** `Router(config-if)# mab`	Enables MAC-based authentication on a port.

Step 6	**end**
	
	Example:
	`Router(config-if)# end`
	`Router#`
		Returns to privileged EXEC mode.

Verifying the MAB

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

```
c1921#show authentication sessions

Interface      MAC Address     Method   Domain   Status         Session ID
Gi0/1          0201.0201.0201  mab      DATA     Authz Success  0303030300000004002500A8

c1921#show authentication sessions interface Gi0/1
            Interface:  GigabitEthernet0/1
          MAC Address:  0201.0201.0201
           IP Address:  Unknown
            User-Name:  02-01-02-01-02-01
               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:  03030303000000004002500A8
      Acct Session ID:  0x00000007
               Handle:  0x3D000005

Runnable methods list:
       Method   State
       mab      Authc Success

c1921#
```

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

Perform these steps to configure the Controlling Port Authorization state.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot / port*
4. **authentication port-control auto**
5. **mab**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** *slot/port* **Example:** `Router(config)# interface gigabitethernet 0/0`	Enters interface configuration mode.
Step 4	**authentication port-control** {*auto* | *force-authorized* | *force-unauthorized*} **Example:** `Router(config-if)# authentication port-control {auto | force-authorized | force-unauthorized}`	Enables the manual control of the port authorization state. **auto**-Allows only EAPol traffic until successful authentication. **force-authorized**-Allows all traffic, requires no authentication. **force-unauthorized**-Allows no traffic.
Step 5	**mab** **Example:** `Router(config-if)# mab`	Enables MAC-based authentication on a port.

Step 6	**end**
	
	Example:
	`Router(config-if)# end`
	`Router#`
		Returns to privileged EXEC mode.

Verifying the Controlling Port Authorization State

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

```
c1921#show authentication sessions

Interface      MAC Address     Method   Domain   Status         Session ID
Gi0/1          (unknown)       dot1x    DATA     Authz Success  030303030000000A002CFCBC

c1921#show authentication sessions interface gi0/1
            Interface:  GigabitEthernet0/1
          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:
       Method   State
       dot1x    Authc Success

c1921#show dot1x interface g0/1
Dot1x Info for GigabitEthernet0/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = FORCE_AUTHORIZED
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

c1921#show authentication sessions

Interface      MAC Address     Method   Domain   Status         Session ID
Gi0/1          (unknown)       dot1x    DATA     Authz Failed   0303030300000009002AB7FC

c1921#show authentication sessions interface gi0/1
            Interface:  GigabitEthernet0/1
          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:  03030303000000009002AB7FC
       Acct Session ID:  0x0000000C
               Handle:  0x8B00000A

Runnable methods list:
       Method   State
       dot1x    Authc Failed

c1921#show dot1x interface g0/1
Dot1x Info for GigabitEthernet0/1
-----------------------------------
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:

http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-service/application_note_c27-573287.html

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

Perform these steps to configure Open Access.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot / port*
4. **authentication open**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** *slot/port* **Example:** `Router(config)# interface gigabitethernet 0/0`	Enters interface configuration mode.
Step 4	**authentication open** **Example:** `Router(config-if)# authentication open`	Enables open access on a port.

Step 5	**end**
	
	Example:
	`Router(config-if)# end`
	`Router#`
		Returns to privileged EXEC mode.

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)

Perform these steps to configure Control-Direction (Wake-on-LAN).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot / port*
4. **authentication control-direction {in|both}**

5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** *slot/port* **Example:** `Router(config)# interface gigabitethernet 0/0`	Enters interface configuration mode.

Step 4	**authentication control-direction {*in*|*both*}**
	
	Example:
	`Router(config-if)# authentication control-direction in`
	`Router(config-if)# authentication control-direction both`
		Configures the port mode as unidirectional or bidirectional.
		
		in-The port can send packets to the host, but cannot receive packets from the host.
		
		both-The port cannot receive packets from or send packets to the host. This is the default value.

Step 5	**end**
	
	Example:
	`Router(config-if)# end`
	`Router#`
		Returns to privileged EXEC mode.

Verifying Default Control-Direction Setting-Both

Use the **show authentication sessions** and **show dot1x** commands to verify the default control-direction setting-both:

```
c1921#show authentication sessions interface Gi0/1
            Interface:  GigabitEthernet0/1
          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

c1921#

c1921#sh dot1x int g0/1
Dot1x Info for GigabitEthernet0/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

Verifying Authentication Control-Direction Setting-in

Use the **show authentication sessions** and **show dot1x** commands to verify the authentication control-direction setting-in:

```
c1921#show authentication sessions interface gi0/1
            Interface:  GigabitEthernet0/1
          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

c1921#show dot1x interface g0/1
Dot1x Info for GigabitEthernet0/1
-----------------------------------
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:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SY/configuration/guide/sy_swcg/port_acls.html#wp1039754

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.