Restrictions for IEEE 802.1X Port-Based Authentication

The following restrictions are applicable for IEEE 802.1X port-based authentication:

- 802.1X multi-host and 802.1X multi-auth are not supported.
- 802.1X VLAN assignment is not supported.
- Walled-garden VLAN and policies on authentication failures are not supported.
- Subinterfaces and VLAN-tagged traffic are not supported on the ports on which 802.1X port-based authentication is configured.

Communication with the RADIUS server that is initiated by the 802.1x authenticator (RADIUS client) must happen through the built-in management interface on the route processor (RP). Currently, the scenario in which the 802.1x authenticator (RADIUS client) uses a line card port to communicate with the RADIUS server is not supported.

IEEE 802.1X Device Roles

The devices in the network have the following specific roles with IEEE 802.1X authentication:

- **Authenticator** - An entity that facilitates authentication of other entities attached to the same LAN.
- **Supplicant** - An entity at one end of a point-to-point LAN segment that seeks to be authenticated by an Authenticator attached to the other end of that link.
- **Authentication Server** - An entity that provides an authentication service to an Authenticator. Based on the credentials provided by the Supplicant, the server determines whether the Supplicant is authorized to access the services provided by the system in which the Authenticator resides.
Understanding 802.1X Port-Based Authentication

IEEE 802.1X port-based authentication is configured on Cisco NCS 540 Series Router to prevent unauthorized routers (supplicants) from gaining access to the network. An authentication server validates the supplicant that is connected to an authenticator port, before the services offered by the client or the network is made available to the supplicant.

Until the supplicant is authenticated, the port is in Unauthorized state, and 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPoL) packets through the port. EAPoL frames can have either default EtherType of 0x888E or Cisco-defined EtherType of 0x876F. After successful authentication of the supplicant, the port transitions to Authorized state, and normal traffic passes through the port for the authenticated client.

Periodic reauthentication can be enabled to use either the port-configured value or from authentication server. The authentication server communicates the reauthentication-timer value in Session-Timeout attribute, with the final RADIUS Access-Accept message. On 802.1X reauthentication failure, the port is blocked and moved back to the Unauthorized state.

If the link state of a port changes from up to down, or if an EAPOL-logoff frame is received, the port returns to the Unauthorized state.

The following figure shows the topology for IEEE 802.1X port-based authentication:

Figure 1: Topology for IEEE 802.1X Port-Based Authentication

Configure 802.1X Port-Based Authentication

To configure 802.1X port-based authentication, perform the following tasks:

1. Configure RADIUS server
2. Configure 802.1X authentication method
3. Create a 802.1X profile
4. Apply 802.1X profile on an interface

**Configure RADIUS Server**

To configure RADIUS server pre-shared keys, obtain the pre-shared key values for the remote RADIUS server and perform this task.

```
Router# configure terminal
Router(config)# radius-server host {ipv4-address|ipv6-address|host-name} key [0 Line 7]
   Key-value
Router(config)# radius-server vsa attribute ignore unknown
Router(config)# commit
```

**Running Configuration**

```
Router# show run radius
radius-server host 209.165.200.225 auth-port 1646
   key 7 094F471A1A0A57
   radius-server vsa attribute ignore unknown
```

**Configure 802.1X Authentication Method**

You can configure 802.1X authentication method using RADIUS as the protocol. Only default AAA method is supported for 802.1X authentication.

```
Router# configure terminal
Router(config)# aaa authentication dot1x default group radius
Router(config)# commit
```

**Running Configuration**

```
Router# show run aaa
configure
   aaa authentication dot1x default group radius
```

**Create 802.1X Profile**

You can create multiple 802.1X profiles. The role of the node running 802.1X profile must be an authenticator.

```
Router# configure terminal
Router(config)# dot1x profile {name}
Router(config-dot1x-prof)# pae {authenticator}
Router(config-dot1x-prof)# authenticator timer reauth-time {reauth-time | server}
Router(config-dot1x-prof-auth)# commit
```

**Running Configuration**

```
Router# show run dot1x profile test_prof
dot1x profile test_prof
   pae authenticator
   authenticator
      timer reauth-time 3600
```
Apply 802.1X Profile on Interface

You can attach one of the 802.1X profiles on an interface.

Router# configure
Router(config)# interface interface-name
Router(config-if)# dot1x profile profile-name
Router(config-if)# commit

Running Configuration

Router# show run interface HundredGigE 0/0/1/0
interface HundredGigE 0/0/1/0
dot1x profile test_prof

Verify 802.1X Port-Based Authentication

The 802.1X authentication can be verified using the following:

- Show command outputs
- Syslog messages

Show Command Outputs

The `show dot1x interface` command verifies whether the 802.1X port-based authentication is successful or not. If the authentication is successful, the traffic is allowed on the configured interface.

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

Dot1x info for HundredGigE 0/0/1/0
dot1x profile test_prof

Dot1x Port Status:
- AUTHORIZED

Restrictions for IEEE 802.1X Port-Based Authentication

Restrictions for IEEE 802.1X Port-Based Authentication
Syslog Messages

When 802.1x configuration is applied on an interface, the port becomes 802.1X controlled, and the following syslog message is displayed:

%L2-DOT1X-5-PORT_CONTROL_ENABLE_SUCCESS : Hu0/0/1/0 : Port Control Enabled

After successful authentication of supplicant, the following syslog messages are displayed:

%L2-DOT1X-5-AUTH_SUCCESS : Hu0/0/1/0 : Authentication successful for client 027E.15F2.CAE7

%L2-DOT1X-5-PORT_CONTROL_ADD_CLIENT_SUCCESS : Hu0/0/1/0 : Port Access Enabled For Client 027E.15F2.CAE7

When 802.1X port-based configuration is removed from an interface, the following syslog message is displayed:

%L2-DOT1X-5-PORT_CONTROL_DISABLE_SUCCESS : Hu0/0/1/0 : Port Control Disabled

When authentication fails, the following syslog messages are displayed:

%L2-DOT1X-5-AUTH_FAIL : Hu0/0/1/0 : Authentication fail for client 027E.15F2.CAE7

%L2-DOT1X-5-PORT_CONTROL_REMOVE_CLIENT_SUCCESS : Hu0/0/1/0 : Port Access Disabled For Client 027E.15F2.CAE7

When authentication server is unreachable, the following syslog message is displayed:

%L2-DOT1X-5-AAA_UNREACHABLE : Hu0/0/1/0 : AAA server unreachable for client 027E.15F2.CAE7, Retrying Authentication

When authentication method is not configured, the following syslog message is displayed:

%L2-DOT1X-4-NO_AUTHENTICATION_METHOD : Hu0/0/1/0 : No authentication method configured