Configuring IEEE 802.1X and IEEE 802.11i Authentication

IEEE 802.1X is a port-based network access control (PNAC) protocol that prevents unauthorized network devices from gaining access to wired networks (WANs), by providing authentication for devices that want to connect to a WAN.

IEEE 802.11i prevents unauthorized network devices from gaining access to wireless networks (WLANs). 802.11i implements WiFi Protected Access II (WPA2) to provide authentication for devices that want to connect to a WLAN on a vEdge 100wm router.

A RADIUS authentication server must authenticate each client connected to a port before that client can access any services offered by network.

This article describes how to configure RADIUS servers to use for 802.1X and 802.11i authentication. It describes how to enable 802.1X on vEdge router interfaces to have the router act as an 802.1X authenticator, responsible for authorizing or denying access to network devices on a WAN. Finally, it describes how to enable 802.11i on vEdge 100wm routers to control access to WLANs.

Configure RADIUS Authentication Servers

Authentication services for IEEE 802.1X and IEEE 802.11i are provided by RADIUS authentication servers. You configure the RADIUS servers to use for 802.1X and 802.11i authentication on a system-wide basis:

```
  vEdge(config)# system radius
  vEdge(config-radius)# server ip-address
```

Specify the IP address of the RADIUS server. You can configure one or two RADIUS servers to perform 802.1X and 802.11i authentication. (Note that for AAA authentication, you can configure up to eight RADIUS servers.)

For each RADIUS server, you can configure a number of optional parameters.

You can configure the VPN through which the RADIUS server is reachable and the router interface to use to reach the server:

```
  vEdge(config-server)# vpn vpn-id
  vEdge(config-server)# source-interface interface-name
```

If you configure two RADIUS servers, they must both be in the same VPN, and they must both be reachable using the same source interface.

You must configure a tag to identify the RADIUS server:

```
  vEdge(config-server)# tag tag
```

The tag can be from 4 through 16 characters. You use this tag when configuring the RADIUS servers to use with IEEE 802.1X authentication and with IEEE 802.11i WPA enterprise authentication (discussed later in this article).

For authentication between the router and the RADIUS server, you can authenticate and encrypt packets sent between the vEdge router and the RADIUS server, and you can configure a destination port for authentication requests. To authenticate and encrypt packets, configure a key:
Enter the password as clear text, which is immediately encrypted, or as an AES 128-bit encrypted key. The key must match the AES encryption key used on the RADIUS server.

By default, UDP port 1812 is used as the destination port on the RADIUS server to use for authentication requests. You can change the port number to a number from 1 through 65535. To disable authentication, set the port number to 0.

You can set the priority of a RADIUS server, to choose which one to use first when performing 802.1X authentication:

The priority can be a value from 0 through 7. The server with the lower priority number is given priority. If you do not include this command in the RADIUS server configuration, the priority is determined by the order in which you enter the IP addresses in the `system radius server` command.

By default, accounting is enabled for 802.1X and 802.11i interfaces. Accounting information is sent to UDP port 1813 on the RADIUS server. To change this port:

The port number can be from 1 through 65535.

---

**Configure IEEE 802.1X Port Security**

To enable basic 802.1X port security on an interface, configure it and at least one RADIUS server to use for 802.1X authentication. The 802.1X interface must be in VPN 0.

For 802.1X authentication to work, you must also configure the same interface under an untagged bridge:

The interface name in the `vpn 0 interface` and `bridge interface` commands must be the same. Do not configure a VLAN ID for this bridge so that it remains untagged.

You can enable 802.1X on a maximum of four wired physical interfaces. The interface cannot also be configured as a tunnel interface.

Configure the tags associated with one or two RADIUS servers to use for 802.1X client authentication and accounting. (You configure the tags with the `system radius server tag` command.) If you specify tags for two RADIUS servers, they must both be reachable in the same VPN. If you do not configure a priority value when you configure the RADIUS server with the `system radius server priority` command, the order in which you list the IP addresses is the order in which the RADIUS servers are tried.
Enable RADIUS Accounting

By default, the vEdge router never sends interim accounting updates to the 802.1X RADIUS accounting server. Accounting updates are sent only when the 802.1X session ends.

To enable the sending of interim accounting updates, configure the interval at which to send the updates:

```bash
vEdge(config-dot1x)# accounting-interval seconds
```

The time can be from 0 through 7200 seconds.

Enable MAC Authentication Bypass

IEEE 802.1X authentication is accomplished through an exchange of Extensible Authentication Protocol (EAP) packets. After 802.1X-compliant clients respond to the EAP packets, they can be authenticated and granted access to the network. Enabling MAC authentication bypass (MAB) provides a mechanism to allow non-802.1X–compliant clients to be authenticated and granted access to the network.

The vEdge router determines that a device is non-802.1X–compliant clients when the 802.1X authentication process times out while waiting for an EAPOL response from the client.

To enable MAC authentication bypass for an 802.1X interface on the vEdge router:

```bash
vEdge(config)# vpn 0 interface interface-name dot1x
vEdge(config-dot1x)# mac-authentication-bypass
```

With this configuration, the vEdge router authenticates non-802.1X–compliant clients using the configured RADIUS servers. The RADIUS server must be configured with the MAC addresses of non-802.1X–compliant clients that are allowed to access the network.

To enable MAB on the RADIUS server:

```bash
vEdge(config-dot1x)# mac-authentication-bypass server
```

To allow authentication to be performed for one or more non-802.1X–compliant clients before performing an authentication check with the RADIUS server, list their MAC addresses in the following command:

```bash
vEdge(config-dot1x)# mac-authentication-bypass allow mac-addresses
```

You can configure up to eight MAC addresses for MAC authentication bypass. For these devices, the vEdge router grants immediate network access based on their MAC addresses, and then sends a request to the RADIUS server to authenticate the devices.

Configure VLANs for Authenticated and Unauthenticated Clients

For clients that cannot be authenticated but that you want to provide limited network services to, you create VLANs to handle network access for these clients. You also create VLANs to handle authenticated clients.

You can create the following kinds of VLAN:

- Guest VLAN—Provide limited services to non-802.1X–compliant clients.
• Authentication Reject VLAN—Provide limited services to 802.1X-compliant clients that failed RADIUS authentication. An authentication-reject VLAN is similar to a restricted VLAN.

• Authentication Fail VLAN—Provide network access when RADIUS authentication or the RADIUS server fails. An authentication-fail VLAN is similar to a critical VLAN.

• Default VLAN—Provide network access to 802.1X–compliant clients that are successfully authenticated by the RADIUS server. If you do not configure a default VLAN on the vEdge router, successfully authenticated clients are placed into VLAN 0, which is the VLAN associated with an untagged bridge.

To configure the VLANS for authenticated and unauthenticated clients, first create the VLAN in a bridging domain, and then create the 802.1X VLANS for the unauthenticated clients by associating the bridging domain VLAN with an 802.1X VLAN.

To create the VLAN, configure a bridging domain to contain the VLAN:

```bash
vEdge(config)# bridge bridge-id
vEdge(config-bridge)# name text
vEdge(config-bridge)# vlan vlan-id
vEdge(config-bridge)# interface interface-name
vEdge(config-interface)# no shutdown
```

The bridging domain identifier is a number from 1 through 63. A best practice is to have the bridge domain ID be the same as the VLAN number.

The name is optional, but it is recommended that you configure a name that identifies the 802.1X VLAN type, such as Guest-VLAN and Default-VLAN.

The VLAN number can be from 1 through 4095. This is the number that you associate with an 802.1X VLAN.

The interface name is the interface that is running 802.1X.

Then configure the 802.1X VLANS to handle unauthenticated clients.

A guest VLAN provides limited services to non-802.1X–compliant clients, and it can be used to allow clients to download 802.1X client software. An interface running 802.1X assigns clients to a guest VLAN when the interface does not receive a response to EAP request/identity packets that it has sent to the client, or when the client does not send EAPOL packets and MAC authentication bypass is not enabled. To configure a guest VLAN:

```bash
vEdge(config)# vpn 0 interface interface-name interface dot1x
vEdge(config-dot1x)# guest-vlan vlan-id
```

The VLAN number must match one of the VLANS you configured in a bridging domain. A best practice is to have the VLAN number be the same as the bridge domain ID.

An authentication-reject VLAN provides limited services to 802.1X-compliant clients that have failed RADIUS authentication. To configure an authentication-reject VLAN:

```bash
vEdge(config-dot1x)# auth-reject-vlan vlan-id
```

The VLAN number must match one of the VLANS you configure in a bridging domain. A best practice is to have the VLAN number be the same as the bridge domain ID.

When the RADIUS authentication server is not available, 802.1X-compliant clients attempting to authenticate are placed in an authentication-fail VLAN if it is configured. If this VLAN is not configured, the authentication request is eventually dropped. To configure the authentication-fail VLAN:
The VLAN number must match one of the VLANs you configure in a bridging domain. A best practice is to have the VLAN number be the same as the bridge domain ID.

The following configuration snippet illustrates the interrelationship between the 802.1X configuration and the bridging domain configuration. This snippet shows that the bridging domain numbers match the VLAN numbers, which is a recommended best practice. Also, the bridging domain name identifies the type of 802.1X VLAN.

```

vEdge(config-dot1x)# auth-fail-vlan vlan-id

The VLAN number must match one of the VLANs you configure in a bridging domain. A best practice is to have the VLAN number be the same as the bridge domain ID.

The following configuration snippet illustrates the interrelationship between the 802.1X configuration and the bridging domain configuration. This snippet shows that the bridging domain numbers match the VLAN numbers, which is a recommended best practice. Also, the bridging domain name identifies the type of 802.1X VLAN.

```
```
ip address 10.1.19.15/24
no shutdown !
interface ge0/4
ip address 10.20.24.15/24
no shutdown !
interface ge0/5
dot1x
 auth-reject-vlan 40
 auth-fail-vlan 30
 guest-vlan 20
 default-vlan 10
 radius-servers freerad1
 no shutdown !
interface ge0/7
ip address 10.0.100.15/24
no shutdown !
!
vpn 1
interface ge0/2.1
ip address 10.2.19.15/24
mtu 1496
no shutdown !
interface irb1
ip address 56.0.1.15/24
mac-address 00:00:00:00:aa:01
no shutdown
dhcp-server
address-pool 56.0.1.0/25
offer-time 600
lease-time 86400
admin-state up
options
default-gateway 56.0.1.15
!
!
vpn 10
interface ge0/2.10
ip address 10.10.19.15/24
mtu 1496
no shutdown !
interface irb10
ip address 56.0.10.15/24
mac-address 00:00:00:00:aa:10
no shutdown
dhcp-server
address-pool 56.0.10.0/25
offer-time 600
lease-time 86400
admin-state up
options
default-gateway 56.0.10.15
!
!
vpn 20
interface ge0/2.20
ip address 10.20.19.15/24
mtu 1496
no shutdown !
interface irb20
ip address 56.0.20.15/24
mac-address 00:00:00:00:aa:20
no shutdown !
vpn 30
interface ge0/2.30
ip address 10.30.19.15/24
mtu 1496
no shutdown !
interface irb30
ip address 56.0.30.15/24
mac-address 00:00:00:00:aa:30
no shutdown
Configure Control Direction

To configure how the 802.1X interface handles traffic when the client is unauthorized, set the control direction:

```plaintext
vEdge(config-dot1x)# configuration
```

The direction can be one of the following:

- **in-and-out**—The 802.1X interface can both send packets to and receive packets from the authorized client. Bidirectional control is the default behavior.
- **in-only**—The 802.1X interface can send packets to the unauthorized client, but cannot receive packets from that client.

Configure Authentication with Wake on LAN

IEEE 802.1X authentication wake on LAN (WoL) allows dormant clients to be powered up when the vEdge router receives a type of Ethernet frame called the magic packet. Administrators can use wake on LAN when to connect to systems that have been powered down.

When a client that uses wake on LAN and that attaches through an 802.1X port powers off, the 802.1X port becomes unauthorized. The port can only receive and send EAPOL packets, and wake-on-LAN magic packets cannot reach the client. When the device is powered off, it is not authorized, and the switch port is not opened.

Without wake on LAN, when an 802.1X port is unauthorized, the router's 802.1X interface block traffic other than EAPOL packets coming from unauthorized clients.

When you enable wake on LAN on an 802.1X port, the vEdge router is able to send magic packets even if the 802.1X port is unauthorized.

To enable wake on LAN on an 802.1X interface, use the following command:

```plaintext
vEdge(config)# vEdge(config)# vEdge(config-dot1x)# configuration
vEdge(config-dot1x)# configuration
```

Configure 802.1X Host Mode

The host mode of an 802.1X interfaces determines whether the interface grants access to a single client or to multiple clients. Three host modes are available:
• Single-host mode—The 802.1X interface grants access only to the first authenticated client. All other clients attempting access are denied and dropped.

• Multiple-host mode—A single 802.1X interface grants access to multiple clients. In this mode, only one of the attached clients must be authorized for the interface to grant access to all clients. If the interface becomes unauthorized, the vEdge router denies network access to all the attached clients.

• Multiple-authentication mode—A single 802.1X interface grants access to multiple authenticated clients on data VLANs.

To configure the host mode of the 802.1X interface, use the following command:

```bash
vEdge(config)# vpn 0 interface interface-name dotlx
vEdge(config-dotlx)# host-mode (multi-auth | multi-host | single-host)
```

### Set the Timeout for Inactive Clients

By default, when a client has been inactive on the network for 1 hour, its authentication is revoked, and the client is timed out. To change the timeout interval, use the following command:

```bash
vEdge(config)# vpn 0 interface interface-name dotlx
vEdge(config-dotlx)# timeout inactivity minutes
```

The timeout interval can be from 0 through 1440 minutes (24 hours).

### Enable Periodic Client Reauthentication

By default, once a client session is authenticated, that session remains functional indefinitely. To enable the periodic reauthentication of 802.1X clients, configure the number of minutes between reauthentication attempts:

```bash
vEdge(config)# vpn 0 interface interface-name dotlx
vEdge(config-dotlx)# reauthentication minutes
```

The time can be from 0 through 1440 minutes (24 hours).

### Configure Dynamic Authorization Service for RADIUS Change of Authorization

Dynamic authorization service (DAS) allows an 802.1X interface on a vEdge router to accept change of authorization (CoA) requests from a RADIUS or other authentication server and to act on the requests. The Viptela implementation of DAS supports disconnect packets, which immediately terminate user sessions, and reauthentication CoA requests, which modify session authorization attributes.

DAS, defined in [RFC 5176](https://tools.ietf.org/html/rfc5176), is an extension to RADIUS that allows the RADIUS server to dynamically change 802.1X session information without requiring the vEdge router to initiate the change request. When you enable DAS on the vEdge router, the router opens a socket to listen for CoA requests from the RADIUS server. If the network administrator of a RADIUS server modifies the authentication of an 802.1X client, the RADIUS server sends a CoA request to inform the router about the change of authorization. When the router receives the CoA request, it processes the requested change.
To enable DAS for an 802.1X interface, you configure information about the RADIUS server from which the interface can accept CoA requests. In the context of configuring DAS, the vEdge router is the server and the RADIUS server (or other authentication server) is the client.

To configure the RADIUS server from which to accept CoA requests, configure the server’s IP address and the password that the RADIUS server uses to access the router’s 802.1X interface:

```
vEdge(config)# vpn 0 interface interface-name dot1x
vEdge(config-dot1x)# das
vEdge(config-das)# client ip-address
vEdge(config-das)# secret-key password
```

You can configure the VPN through which the RADIUS server is reachable:

```
vEdge(config-das)# vpn vpn-id
```

By default, the 802.1X interface uses UDP port 3799 to listen for CoA request from the RADIUS server. You can change the port number:

```
vEdge(config-das)# port port-number
```

The port number can be a value from 1 through 65535. If you configure DAS on multiple 802.1X interfaces on a vEdge router, you must configure each interface to use a different UDP port.

By default, the CoA requests that the vEdge router receives from the DAS client are all honored, regardless of when the router receives them. To have the router handle CoA within a specified time, you require that the DAS client timestamp all CoA requests:

```
vEdge(config-das)# require-timestamp
```

With this configuration, the vEdge router processes only CoA requests that include an event timestamp. Non-timestamped CoA requests are dropped immediately.

When timestamping is configured, both the vEdge router and the RADIUS server check that the timestamp in the CoA request is current and within a specific time window. The default time window is 300 seconds (5 minutes). This behavior means that if the DAS timestamps a CoA at 15:00 and the router receives it at 15:04, the router honors the request. However, if the router receives the request at 15:10, the router drops the CoA request. You can change the time window to a time from 0 through 1000 seconds:

```
vEdge(config-das)# time-window seconds
```

---

**Configure RADIUS Authentication and Accounting Attributes**

For IEEE 802.1X authentication and accounting, the vEdge router, acting as a network access server (NAS), sends RADIUS attribute–value (AV) pairs to the RADIUS server. These AV pairs are defined in RFC 2865, RADIUS, RFC 2866, RADIUS Accounting, and RFC 2869, RADIUS Extensions. The AV pairs are placed in the Attributes field of the RADIUS packet.

By default, when you enable IEEE 802.1X port security, the following authentication attributes are included in messages sent to the RADIUS server:
### Attribute Details

<table>
<thead>
<tr>
<th>Attribute Number</th>
<th>Attribute Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User-Name</td>
<td>Name of the user to be authenticated.</td>
</tr>
<tr>
<td>5</td>
<td>NAS-Port</td>
<td>Physical port number on the vEdge router that is authenticating the user.</td>
</tr>
<tr>
<td>12</td>
<td>Framed-MTU</td>
<td>Maximum MTU configured for the user.</td>
</tr>
<tr>
<td>30</td>
<td>Called-Station-Id</td>
<td>Phone number that the user called, using dialed number identification (DNIS) or similar technology used to access the RADIUS server.</td>
</tr>
<tr>
<td>31</td>
<td>Calling-Station-Id</td>
<td>Phone number that the call came in to the server, using automatic number identification (ANI) or similar technology.</td>
</tr>
<tr>
<td>44</td>
<td>Acct-Session-Id</td>
<td>Unique session identifier.</td>
</tr>
<tr>
<td>61</td>
<td>NAS-Port-Type</td>
<td>Type of physical port on the vEdge router that is authenticating the user.</td>
</tr>
<tr>
<td>77</td>
<td>Connect-Info</td>
<td>Nature of the user's connection.</td>
</tr>
<tr>
<td>79</td>
<td>EAP-Message</td>
<td>Encapsulate Extended Access Protocol (EAP) packets, to allow the vEdge router to authenticate dial-in users via EAP without having to run EAP.</td>
</tr>
<tr>
<td>80</td>
<td>Message-Authenticator</td>
<td>Sign RADIUS Access-Requests to prevent these requests from being spoofed by ARAP, CHAP, or EAP.</td>
</tr>
</tbody>
</table>

### Accounting Attributes

When you enable RADIUS accounting, the following accounting attributes are included, by default, in messages sent to the RADIUS server:

<table>
<thead>
<tr>
<th>Attribute Number</th>
<th>Attribute Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User-Name</td>
<td>Name of the user to be authenticated.</td>
</tr>
<tr>
<td>5</td>
<td>NAS-Port</td>
<td>Physical port number on the vEdge router that is authenticating the user.</td>
</tr>
<tr>
<td>30</td>
<td>Called-Station-Id</td>
<td>Phone number that the user called, using dialed number identification (DNIS) or similar technology used to access the RADIUS server.</td>
</tr>
<tr>
<td>31</td>
<td>Calling-Station-Id</td>
<td>Phone number that the call came in to the server, using automatic number identification (ANI) or similar technology.</td>
</tr>
<tr>
<td>40</td>
<td>Acct-Status-Type</td>
<td>Mark the beginning and end of an accounting request.</td>
</tr>
<tr>
<td>44</td>
<td>Acct-Session-Id</td>
<td>Unique accounting identifier used to match the start and stop records in a log file.</td>
</tr>
<tr>
<td>45</td>
<td>Acct-Authentic</td>
<td>How the user was authenticated.</td>
</tr>
<tr>
<td>Attribute Number</td>
<td>Attribute Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>61</td>
<td>NAS-Port-Type</td>
<td>Type of physical port on the vEdge router that is authenticating the user.</td>
</tr>
<tr>
<td>77</td>
<td>Connect-Info</td>
<td>Nature of the user's connection.</td>
</tr>
</tbody>
</table>

Several configuration commands allow you to add additional attribute information to RADIUS packets.

To include the NAS-IP-Address (attribute 4) in messages sent to the RADIUS server, to indicate the IP address of the vEdge router that is acting as a NAS server:

```plaintext
vEdge(config-dot1x) nas-ip-address ip-address
```

To include the NAS-Identifier (attribute 32) in messages sent to the RADIUS server, use the following command:

```plaintext
vEdge(config-dot1x)# nas-identifier string
```

The NAS identifier is a unique string from 1 through 255 characters long that identifies the vEdge router that is acting as a NAS server.

To include a RADIUS authentication or accounting attribute of your choice in messages sent to the RADIUS server, use the following commands:

```plaintext
vEdge(config-dot1x)# auth-req-attr attribute-number {integer integer | octet octet | string string}
vEdge(config-dot1x)# acct-req-attr attribute-number {integer integer | octet octet | string string}
```

Specify the desired value of the attribute as an integer, octet value, or string, depending on the attribute. For example, to set the Service-Type attribute to be authenticate-only:

```plaintext
vEdge(config-dot1x)# auth-req-attr 6 integer 8
```

---

### Configure IEEE 802.11i Authentication

For Viptela routers that support wireless LANs (WLANs), you can configure the router to support either a 2.4-GHz or 5-GHz radio frequency. Then, you segment the WLAN into multiple broadcast domains, which are called virtual access points, or VAPs. Users who connect to a VAP can be unauthenticated, or you can configure IEEE 802.11i authentication for each VAP.

For information about configuring the WLAN interface itself, see [Configuring WLAN Interfaces](https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.1/02System_and_Interfaces/09Configuring_IEEE_802.1X_and_IEEE_802.11i_Authentication).

To enable user authentication on the WLAN, you create a VAP on the desired radio frequency and then you configure Wi-Fi protected access (WPA) or WPA2 data protection and network access control for the VAP. WPA authenticates individual users on the WLAN using a username and password. WPA uses the Temporal Key Integrity Protocol (TKIP), which is based on the RC4 cipher. WPA2 implements the NIST FIPS 140-2–compliant AES encryption algorithm along with IEEE 802.1X-based authentication, to enhance user access security over WPA. WPA2 uses the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), which is based on the AES cipher.

Authentication is done either using preshared keys or through RADIUS authentication.
To enable personal authentication, which requires users to enter a password to connect to the WLAN, configure the authentication and password:

```
  vEdge(config)# wlan frequency
  vEdge(config-wlan)# interface vap.number
  vEdge(config-vap)# no shutdown
  vEdge(config-vap)# data-security (wpa-personal | wpa/wpa2-personal | wpa2-personal)
  vEdge(config-vap)# wpa-personal-key password
```

For the security, configure either WPA, WPA2, or both (WPA/WPA2). Enter the password either as clear text or an AES-encrypted key.

For each VAP, you can customize the security mode to control wireless client access.

To enable enterprise WPA security, configure the authentication and the RADIUS server to perform the authentication:

```
  vEdge(config-vap)# data-security (wpa-enterprise | wpa/wpa2-enterprise | wpa2-enterprise)
  vEdge(config-vap)# radius-servers tag
```

For the security, configure either WPA, WPA2, or both (WPA/WPA2). Enter the password either as clear text or an AES-encrypted key.

In the `radius-servers` command, enter the tags associated with one or two RADIUS servers to use for 802.11i authentication. (You configure the tags with the `system radius server tag` command.) If you specify tags for two RADIUS servers, they must both be reachable in the same VPN. If you do not configure a priority value when you configure the RADIUS server with the `system radius server priority` command, the order in which you list the IP addresses is the order in which the RADIUS servers are tried.

By default, management frames sent on the WLAN are not encrypted. For each VAP, you can configure the encryption to be optional or required:

```
  vEdge(config-vap)# mgmt-security (none | optional | required)
```

---

**Additional Information**

- Configuring Network Interfaces
- Configuring WLAN Interfaces