
Configuring WLAN Interfaces

vEdge 100wm routers include a wireless LAN (WLAN) radio for providing access point (AP) functionality for teleworkers, small offices, stores, and branch offices. You can configure the radio to operate at either 2.4 GHz or 5 GHz. In 2.4-GHz mode, the radio can support IEEE 802.11b, 802.11g and 802.11n clients, and in 5-GHz mode, the radio can support IEEE 802.11a, 802.11n and 802.11ac clients. vEdge100wm routers support 3x3 MIMO with three spatial streams, and they use an internal antenna. For WLAN security, you can use preshared key and RADIUS server-based methods.

This article describes how to configure the WLAN interfaces. To configure IEEE 802.11i authentication for the VAPs, see [Configuring IEEE 802.1x and IEEE 802.11i Authentication](#).

Configure SSIDs

On a vEdge100wm router, you can configure up to four service set identifiers (SSIDs) on the WLAN radio. Each SSID is referred to by a virtual access point (VAP) interface. To a client, each VAP interface appears as a different access point (AP) with its own SSID. To provide access to different networks, you can assign each VAP to a different VLAN.

To configure a VAP interface that autoselects its channel and uses no authentication and no encryption, create a VAP, assign it a number and an SSID, and enable it:

```
vEdge(config)# wlan radio-band
vEdge(config-wlan)# country country
vEdge(config-wlan)# interface vapnumber
vEdge(config-vap)# no shutdown
vEdge(config-vap)# ssid ssid
```

For the radio band, specify one of the following:

- **2.4GHz**—Consists of fourteen 20-MHz channels with overlapping frequency space. The allowable channels and maximum allowed output power are country specific and restricted by regulatory agencies. In the United States and Canada, channels 1, 6, and 11 are the only non-overlapping channels. This radio band supports IEEE 802.11b, 802.11g, and 802.11n clients..
- **5GHz**—Consists of four 20-MHz channels in UNII-1, four in UNII-2, twelve in UNII-2 Extended, four in UNII-3 and one in ISM band. The allowable channels, their indoor or outdoor usage, and the maximum allowed output power are country specific and are restricted by regulatory agencies. This radio band supports IEEE 802.11a, 802.11n, and 802.11ac clients.

Configuring the country where the router is installed is mandatory, to ensure that the router complies to local regulatory requirements.

For each SSID, configure one VAP interface. *number* can be from 0 through 3. To reduce RF congestion, it is recommended that you do not configure more than two VAP interfaces on the router.

To activate (enable) the VAP interface, include the **no shutdown** command.



Each VAP has an SSID. For *ssid*, enter the name of the SSID. It can be a string from 4 through 32 characters. The SSID must be unique.

By default, a maximum of 25 clients can connect to a single VAP. You can change the maximum number of clients to a value from 1 through 50:

```
vEdge(config-vap) # max-clients number
```

It is recommended that you do not configure more than 50 clients across all the VAPs.

Configure Radio-Specific Parameters

For each radio band, you can configure radio-specific parameters.

Specify the country where the router is installed. This configuration is mandatory and ensures that the router complies to local regulatory requirements, and it enforces country-specific allowable channels and maximum allowed output power. By default, the country is the United States. To set a different country, specify the country where the router is installed:

```
vEdge(config-wlan) # country country
```

You can use the Viptela wireless router software for the following countries: Australia, Austria, Belgium, Brazil, Bulgaria, Canada, China, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malaysia, Malta, Mexico, Netherlands, New Zealand, Norway, Pakistan, Panama, Philippines, Poland, Portugal, Puerto Rico, Romania, Saudi Arabia, Singapore, Slovakia, Slovenia, South Africa, South Korea, Spain, Sri Lanka, Sweden, Switzerland, Taiwan, Thailand, Turkey, United Kingdom, United States, and Vietnam.

Note: Check the release notes for your software release to determine the countries in which the vEdge 100wm router is certified.

By default, the best radio channel is selected automatically. To explicitly configure automatic channel selection, use the following command:

```
vEdge(config-wlan) # channel auto
```

To configure automatic channel selection that excludes channels with dynamic frequency selection (DFS) capabilities, use the following command:

```
vEdge(config-wlan) # channel auto-no-dfs
```

To explicitly configure the radio channel to use:

```
vEdge(config-wlan) # channel channel
```

For 2.4-GHz WLANs, the channel can be 1 through 13, depending on the country configuration.

For 5-GHz WLANs, the channel, including DFS channels, can be one of 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161, and 165, depending on the country configuration.

Note: Airport radar uses frequencies that overlap DFS channels. If you are using a 5-GHz radio band, and if your installation is near an airport, it is recommended that you configure **channel auto-no-dfs**, to remove DFS channels from the list of available channels.



By default, 2.4-GHz radio bands are allocated a channel bandwidth of 20 MHz, and 5-GHz radio bands have a channel bandwidth of 80 MHz. You can set the bandwidth to 20, 40, or 80 MHz:

```
vEdge(config-wlan) # channel-bandwidth megahertz
```

The guard interval is the time between symbol transmissions on the WLAN. For 2.4-GHz radio frequencies, the default guard interval is 800 nanoseconds (which is the normal guard interval), and for 5-GHz frequencies it is 400 nanoseconds (which is the short guard interval). These are the only two guard intervals available. The short guard interval can increase throughput, but it can also increase the error rate because of increased sensitivity to RF reflections. You can choose to configure the guard interval explicitly:

```
vEdge(config-wlan) # guard-interval nanoseconds
```

Configure a Bridging Domain and IRB

To provide the SSIDs access to different networks, you can assign each VAP to a different VLAN. To do this, create one bridge domain with an untagged VLAN for each SSID:

```
vEdge(config) # bridge number
vEdge(config-bridge) # interface vapnumber
vEdge(config-vap) # no native-vlan
vEdge(config-vap) # no shutdown
```

To allow data traffic to be passed among different VLANs, you create an integrated routing and bridging (IRB) logical interface in a VPN domain that connects to the bridging domain:

```
vEdge(config) # vpn vpn-id
vEdge(config-vpn) # interface irbnumber
vEdge(config-irb) # ip address prefix/length
vEdge(config-irb) # no shutdown
```

Configure a DHCP server on the IRB interface so that clients connecting to the VLAN can receive IP addresses in the VLAN:

```
vEdge(config-irb) # dhcp-server
vEdge(config-dhcp-server) # address-pool prefix/length
vEdge(config-dhcp-server) # admin-state (down | up)
vEdge(config-dhcp-server) # options
vEdge(config-options) # default-gateway ip-address
```

WLAN Interface Configuration Example

The configuration example in this section shows how to configure two SSIDs on a WLAN router. One SSID is called CorporateNetwork, and the second is called GuestNetwork.

First, configure the WLAN radio band, and within it, create two VAP interfaces, one for each SSID:

```
wlan 5GHz
country "United States"
interface vap0
```



```

ssid CorporateNetwork
data-security wpa/wpa2-enterprise
radius-server radius_server1
max-clients 30
no shutdown
!
interface vap1
ssid GuestNetwork
data-security wpa/wpa2-personal
wpa-personal-key GuestPassword
max-clients 10
no shutdown
!
!

```

The CorporateNetwork SSID uses wpa/wpa2-enterprise data security, which works in conjunction with a RADIUS authentication server. Here is the configuration for the RADIUS server:

```

system
radius
server 10.20.24.15
acct-port 0
tag radius_server1
vpn 1
secret-key radiusSecretKey
exit
!
!

```

Next, configuring two bridging domains, one for each VAP interface (that is, one for each SSID):

```

bridge 1
interface vap0
no native-vlan
no shutdown
!
!
bridge 2
interface vap1
no native-vlan
no shutdown
!
!

```

Finally, configure IRB interfaces and the DHCP server. Here, the SSID CorporateNetwork uses VPN 1, and the GuestNetwork uses VPN 100:

```

vpn 1
name "Corporate Network"
interface irb1
ip address 10.30.30.1/24
no shutdown
dhcp-server
address-pool 10.30.30.0/24
offer-time 600
lease-time 86400
admin-state up
options
default-gateway 10.30.30.1
dns-servers 8.8.8.8
!
!
!
vpn 100
name "Guest Network"
interface irb2
ip address 192.168.30.1/24
no shutdown
dhcp-server
address-pool 192.168.30.0/24
offer-time 600
lease-time 86400
admin-state up
options
default-gateway 192.168.30.1
dns-servers 8.8.8.8
!
!
!

```



```
!
ip route 0.0.0.0/0 vpn 0
!
```

Additional Information

[Configuring Cellular Interfaces](#)

[Configuring DHCP](#)

[Configuring IEEE 802.1x and IEEE 802.11i Authentication](#)

[Configuring Network Interfaces](#)

[Configuring PPPoE](#)

[Configuring VRRP](#)



https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_17.1/02System_and_Interface...

Created on: Sat, 22 May 2021 22:42:04 GMT

Generated by: Anonymous