Configure Multiple SSIDs on a Network

Objective

The Service Set Identifier (SSID) is a unique identifier that wireless clients can connect to or share among all devices in a wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters.

The objective of this article is to show you how to properly configure multiple SSIDs on a network using VLANs to properly segment the private and guest network.
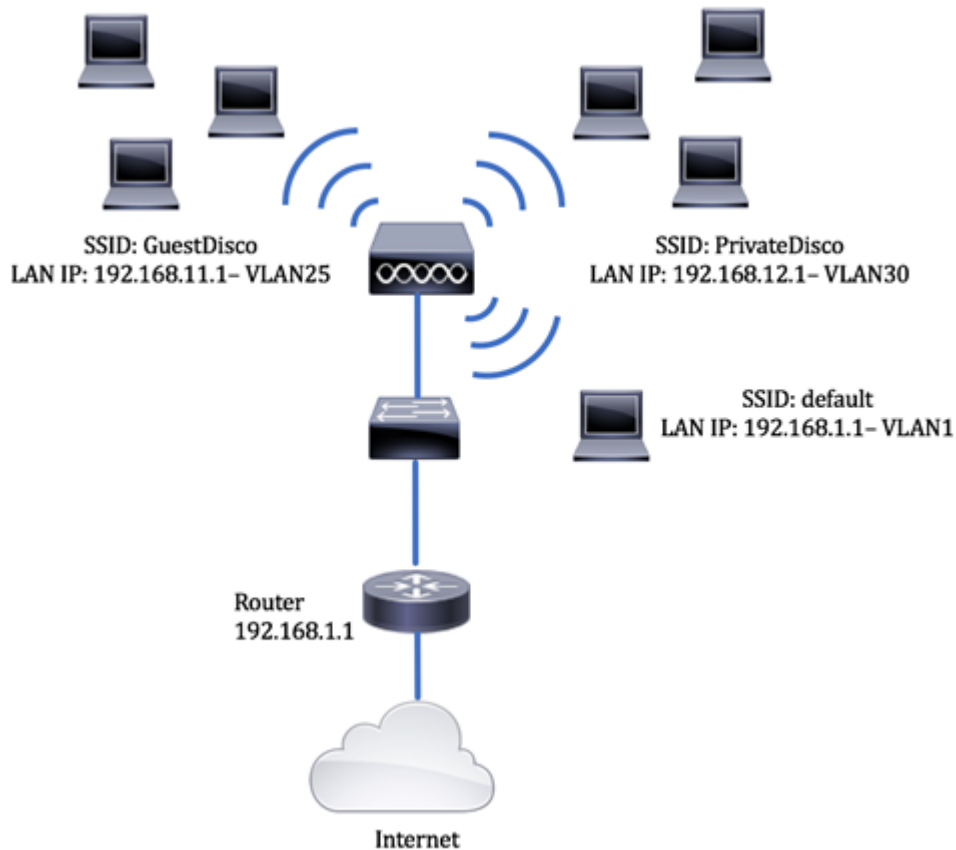
Why would you configure multiple SSIDs?

In a fast-changing and growing work environment, a network needs to be scalable to fit the needs of the company. That would include virtual and physical changes for the most cost-effective methods.

In environments where people come and go such as coffee shops or co-working spaces, it is best practice to segment networks. Create a shared network for the employees where sensitive, corporate data can be exchanged (private network) and another one for the transient workers or customers (guest network).

Note: A captive portal can also be created as a means of additional security for a public network. Captive Portal is a feature on your Wireless Access Point that allows you to set up a guest network where wireless users need to be authenticated first before they can have access to the Internet. It provides wireless access to your visitors while maintaining the security of your internal network. To learn how to configure a Captive Portal, click here.

Network Topology

SSID: GuestDisco
LAN IP: 192.168.11.1– VLAN25

SSID: PrivateDisco
LAN IP: 192.168.12.1– VLAN30

SSID: default
LAN IP: 192.168.1.1– VLAN1

Router
192.168.1.1

Internet

Advantages of using Multiple SSIDs:

1. Secure and persistent connectivity
2. Persistent security and policy enforcement
3. Maximizing network capability by segmenting public and private networks
4. With a public SSID, it grants access to the Internet for guests over the same WAP without crossing over into sensitive network information.

Applicable Devices

- Router — RV340
- Switch — SG220-26P
- Wireless Access Point — WAP150

Software Version

- 1.0.01.17 — RV340
- 1.0.1.7 — WAP150
- 1.1.2.1 — SG220-26P

Configure a VLAN on a Switch

Create a VLAN for Private and Guest Network

Step 1. Login to the web-based utility of the switch and choose **VLAN Management > Create VLAN**.
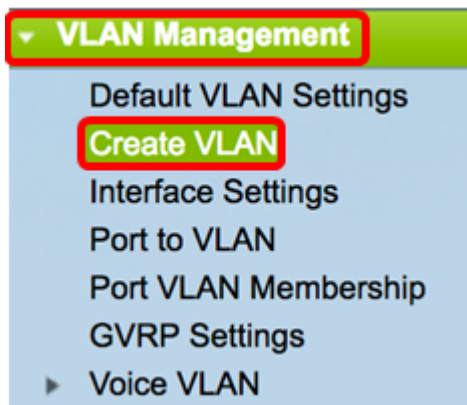
Step 2. In the VLAN table, click **Add** to create a new VLAN.
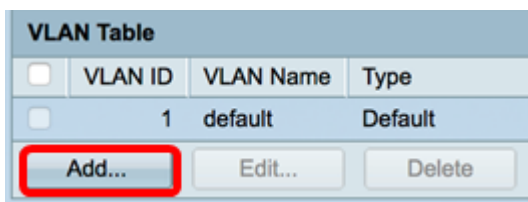
Step 3. In the VLAN ID field, assign a value for your VLAN. Range is 2-4094.

Note: The VLAN ID 25 will be the example used throughout the configuration.
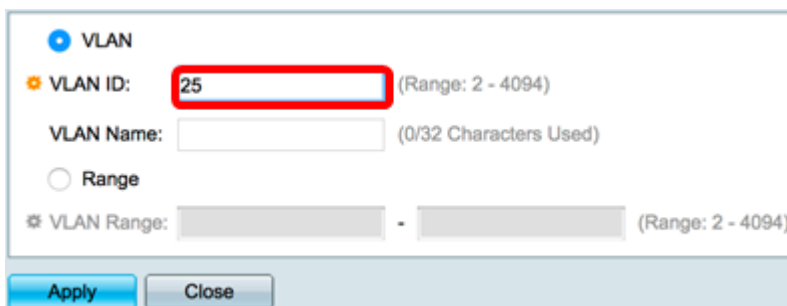
Step 4. In the VLAN Name field, enter a name within the 32-character limit.

Note: In this example, GuestDisco is used.

Step 5. Click **Apply.**

Step 6. Repeat Steps 2 to 5 to create multiple SSIDs.

Note: In this example, a private VLAN network with SSID PrivateDisco has been additionally created.

You should now have successfully created VLANs for both private and guest networks.

Assign a Port to a VLAN

Step 1. Choose **VLAN Management > Port to VLAN**.

Step 2. In the Filter area, from VLAN ID equals to drop-down list, choose a VLAN ID to assign to an interface.

Note: In this example, 25 is chosen.

Step 3. In the Filter area, from the Interface type equals To drop-down list, choose the type of interface you would like to add to the VLAN. The available options are either a port or a Link Aggregation Group (LAG).

Note: In this example, Port is chosen.

Step 4. Click **Go**.

Step 5. Choose an interface to apply the VLAN to. The options are:

- Forbidden — The interface is not allowed to join the VLAN even from Generic VLAN Registration Protocol (GVRP) registration. When a port is not a member of any other VLAN, enabling this option on the port makes the port part of internal VLAN 4095 (a reserved VID).
- Excluded — The interface is currently not a member of the VLAN. This is the default for all the ports and LAGs. The port can join the VLAN through GVRP registration.
- Tagged — The interface is a tagged member of the VLAN.
- Untagged — The interface is an untagged member of the VLAN. Frames of the VLAN are sent untagged to the interface VLAN.
- PVID — Check to set the PVID of the interface to the VID of the VLAN. PVID is a per-port setting.

Note: In this example, GE8 is the chosen interface for the VLAN ID 25 to be tagged. This is also chosen because an existing WAP is connected through this port.

Step 6. Click **Apply**.

Step 7. (Optional) Click the **Port VLAN Membership Table** button to view the assigned VLANs to a port.
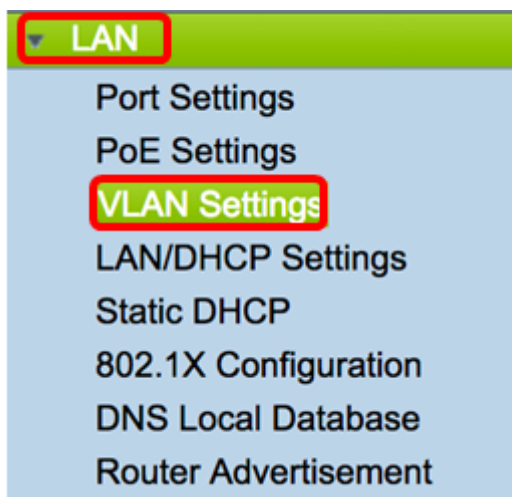

You should now have successfully assigned a VLAN to a port.

Create a VLAN on a Router

Note: The router used in this example is an RV34x Series Router.

Step 1. Log in to the web-based utility of the router and choose **LAN > VLAN Settings**.

Step 2. In the VLAN Table, click **Add** to create a new VLAN.

Step 3. In the *VLAN ID* field, enter a number between 2-4094 to be the VLAN ID.

Note: In this example, the VLAN ID is 25. The VLAN name will automatically populate in accordance to the entered VLAN ID.

Step 4. (Optional) Check the Enable Inter-VLAN Routing check box to allow communication between different VLANs. This is checked by default.

Note: VLANs divide broadcast domains in a LAN environment. Whenever hosts in one VLAN need to communicate with hosts in another VLAN, the traffic must be routed between them.

Step 5. In the *IPv4 Address* field, enter an IPv4 address.

Note: In this example, 192.168.11.1 is used as the IPv4 address.

Step 6. Enter the prefix length for the IPv4 address in the *Prefix Length* field. This determines the number of hosts in the subnetwork.

Note: In this example, 24 is used.

	VLAN ID	Name	Inter-VLAN Routing	IPv4 Address/Mask
☐	1	VLAN1	Enabled	192.168.1.1 / 24
☑	25	VLAN25	☑	IPv4 Address: 192.168.11. Prefix Length 24

VLAN Table

Step 7. Click **Apply**.

Step 8. Repeat the steps as necessary for the VLANs.

Note: In this example, an additional VLAN was created with VLAN ID 30.

VLAN Table

	VLAN ID	Name	Inter-...	IPv4 Address/Mask	IPv6 Address/Mask
☐	1	VLAN1	Enab...	192.168.1.1 / 24	fec0::1 / 64
☐	25	VLAN25	Enab...	192.168.11.1 / 25	fec0:2::1 / 64
☐	30	VLAN30	Enab...	192.168.12.1 / 24	fec0:3::1 / 64

You should now have successfully configured an IPv4-based VLAN on a router.

Configure a VLAN on a Wireless Access Point

This article assumes that the basic radio settings have been configured. To learn how to configure the basic radio settings on a WAP, click here.

In this series of steps, we are modifying an existing network on a single radio on the WAP150.

Step 1. Login to the web-based utility of the WAP and choose **Wireless > Networks**.
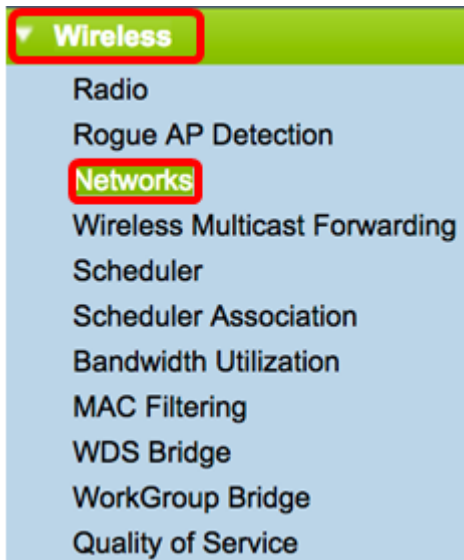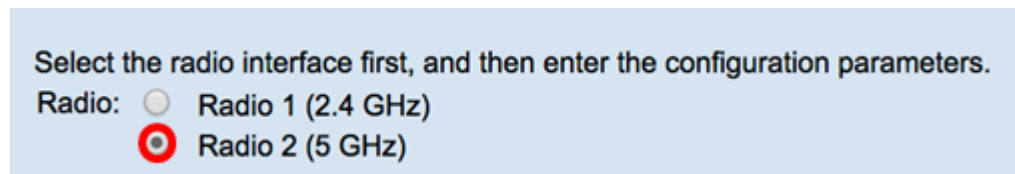
Step 2. Click a radio button to choose a radio band to create and broadcast a wireless network. The options are:

- 2.4 GHz — Wider range, better for legacy devices that support only 2.4 GHz.
- 5 GHz — Provides a more secure coverage and provides better compatibility with newer devices.

Note: In this example, Radio 2 (5 GHz) is chosen.

Step 3. In this step, you can opt to create or edit an SSID. Check the check box of the SSID or Virtual Access Point (VAP) you want to edit.

Note: In this example, VAP 0, VAP 1, and VAP2 are chosen.

Step 4. Click **Edit**.

Step 5. Check the Enable check box to enable the SSID.

Note: In this example, the GuestDisco and Private Disco are checked.

Step 6. In the *VLAN ID* field, enter the recently configured VLAN ID that was configured on both the router and switch.

Note: In this example, it would be 25 and 30.

Step 7. (Optional) In the *SSID Name* field, rename the existing SSID name.

Note: In this example, no changes were made.

Step 8. Check the Enable SSID Broadcast check box to enable visibility to your wireless client devices.

Step 9. From the Security drop-down list, choose the type of security to enforce on the network. The options are:

- None — This is the default setting. Choosing None will leave the wireless network unsecured so anybody with a wireless client device can connect to the network easily.
- WPA Personal — Wi-Fi Protected Access (WPA) uses Advanced Encryption Standard (AES) cipher to protect the wireless network. It uses a combination of case-sensitive letters and numbers for the password. This security type is recommended.
- WPA Enterprise — WPA Enterprise is typically used in enterprise structured networks. It requires a Remote Authentication Dial-In User Service (RADIUS) to complete this type of wireless security setup.

Note: In this example, WPA Personal is applied to both SSIDs.

Step 10. Choose an option from the MAC Filtering drop-down list to assign an action to the router to filter hosts according to their Media Access Control (MAC) address. The options are:

- Disabled — MAC Filtering is disabled on the network.
- Local — Uses a list created on the WAP to filter MAC addresses from accessing the network.
- RADIUS — This option makes use of a RADIUS server to filter MAC addresses.

Step 11. Check the Channel Isolation check box to disable communication between clients.

Step 12. (Optional) Check the **Band Steer** check box to steer and direct devices to a more optimal radio frequency, thus, improving network performance.

Step 13. Click [Save].

Step 14. A window will pop up to inform you that your wireless settings are about to be updated and that you may be disconnected. Click **OK** to continue.
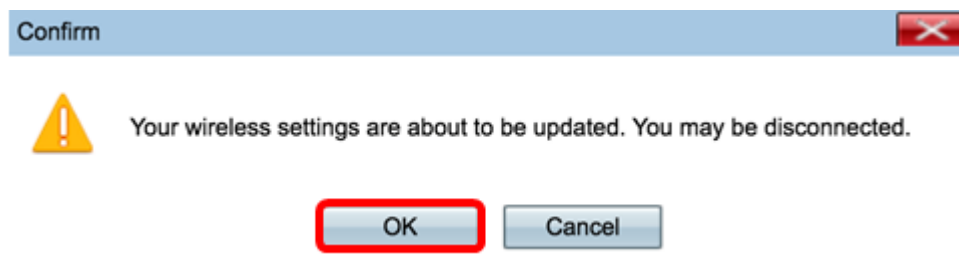
You should now have successfully configured multiple SSIDs with the proper VLANs/segmentation on an access point.