Configuring Multiple SSIDs

This chapter describes how to configure and manage multiple service set identifiers (SSIDs) on the access point. This chapter contains the following sections:

Understanding Multiple SSIDs

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or subnetwork can use the same SSIDs. SSIDs are case sensitive and can contain up to 32 alphanumeric characters. Do not include spaces in your SSIDs.

You can configure up to 16 SSIDs on your HWIC-APs and assign different configuration settings to each SSID. All the SSIDs are active at the same time; that is, client devices can associate to the access point using any of the SSIDs. These are the settings you can assign to each SSID:

- VLAN
- Client authentication method

Note For detailed information on client authentication types, see Chapter 6, "Configuring Authentication Types."

- Maximum number of client associations using the SSID
- RADIUS accounting for traffic using the SSID
- Guest mode
- Repeater mode, including authentication username and password
- Redirection of packets received from client devices

If you want the access point to allow associations from client devices that do not specify an SSID in their configurations, you can set up a guest SSID. The access point includes the guest SSID in its beacon.

If your access point will be a repeater or will be a root access point that acts as a parent for a repeater, you can set up an SSID for use in repeater mode. You can assign an authentication username and password to the repeater-mode SSID to allow the repeater to authenticate to your network like a client device.

If your network uses VLANs, you can assign one SSID to a VLAN, and client devices using the SSID are grouped in that VLAN.

SSID Configuration Methods Supported by Cisco IOS Releases

Cisco introduced global-mode SSID configuration in a prior Cisco IOS Release to simplify configuration of SSID parameters under multiple interfaces. Configuration of SSID parameters at the interface level was supported in some Cisco IOS releases for backward compatibility, but configuration of SSID parameters at the interface level will be totally disabled in releases after Cisco IOS Release 12.4(15)T.

Cisco IOS Release 12.4(15)T supports configuration of SSID parameters at the interface level on the CLI, but the SSIDs are stored in global mode. Storing all SSIDs in global mode ensures that the SSID configuration remains correct when you upgrade to release later than Cisco IOS Release 12.4(15)T.

If you need to upgrade to a release later than 12.4(15)T, you should first upgrade to Cisco IOS Release 12.4(15)T, save the configuration file, upgrade to the target release, and load the saved configuration file. This process ensures that your interface-level SSID configuration correctly translates to global mode. If you upgrade directly from 12.4(15)T release or earlier to a 12.4(15)T or later release, your interface-level SSID configuration is deleted.

Configuring Multiple SSIDs

This section contains configuration information for multiple SSIDs:

Note In Cisco IOS Release 12.4(15)T and later, you configure SSIDs globally and then apply them to a specific radio interface. Follow the instructions in the "Creating an SSID Globally" section on page 3-3 to configure SSIDs globally.

Creating an SSID Globally

In Cisco IOS Releases 12.4 and later, you can configure SSIDs globally or for a specific radio interface. When you use the **dot11 ssid** global configuration command to create an SSID, you can use the **ssid** configuration interface command to assign the SSID to a specific interface.

When an SSID has been created in global configuration mode, the **ssid** configuration interface command attaches the SSID to the interface but does not enter ssid configuration mode. However, if the SSID has not been created in global configuration mode, the **ssid** command puts the CLI into SSID configuration mode for the new SSID.

Note SSIDs created in Cisco IOS Releases 12.3(7)JA and later become invalid if you downgrade the software version to an earlier release.

Beginning in privileged EXEC mode, follow these steps to create an SSID globally. After you create an SSID, you can assign it to specific radio interfaces.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 ssid** *ssid-string*	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. **Note** +, .,], ?, $, TAB, and trailing spaces are invalid characters for SSIDs.
Step 3	**authentication client username** *username* **password** *password*	(Optional) Set an authentication username and password that the access point uses to authenticate to the network when in repeater mode. Set the username and password on the SSID that the repeater access point uses to associate to a root access point, or with another repeater.
Step 4	**accounting** *list-name*	(Optional) Enable RADIUS accounting for this SSID. For *list-name*, specify the accounting method list. Click this link for more information on method lists: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfacct.htm#xtocid2

	Command	Purpose
Step 5	**vlan** *vlan-id*	(Optional) Assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. You can assign only one SSID to a VLAN.
Step 6	**guest-mode**	(Optional) Designate the SSID as your access point's guest-mode SSID. The access point includes the SSID in its beacon and allows associations from client devices that do not specify an SSID.
Step 7	**infrastructure-ssid** [**optional**]	(Optional) Designate the SSID as the SSID that other access points and workgroup bridges use to associate to this access point. If you do not designate an SSID as the infrastructure SSID, infrastructure devices can associate to the access point using any SSID. If you designate an SSID as the infrastructure SSID, infrastructure devices must associate to the access point using that SSID unless you also enter the **optional** keyword.
Step 8	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface to which you want to assign the SSID. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 9	**ssid** *ssid-string*	Assign the global SSID that you created in Step 2 to the radio interface.
Step 10	**end**	Return to privileged EXEC mode.
Step 11	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note You use the **ssid** command's authentication options to configure an authentication type for each SSID. See Chapter 6, "Configuring Authentication Types," for instructions on configuring authentication types.

Use the **no** form of the command to disable the SSID or to disable SSID features.

This example shows how to:

- Name an SSID
- Configure the SSID for RADIUS accounting
- Set the maximum number of client devices that can associate using this SSID to 15
- Assign the SSID to a VLAN
- Assign the SSID to a radio interface

```
router# configure terminal
router(config)# dot11 ssid batman
router(config-ssid)# accounting accounting-method-list
router(config-ssid)# max-associations 15
router(config-ssid)# vlan 3762
router(config-ssid)# exit
router(config)# interface dot11radio 0
router(config-if)# ssid batman
```

Viewing SSIDs Configured Globally

Use this command to view configuration details for SSIDs that are configured globally:

```
router# show running-config ssid ssid-string
```

Using Spaces in SSIDs

In Cisco IOS Release 12.4(15)T, you can include spaces in an SSID, but trailing spaces (spaces at the end of an SSID) are invalid. However, any SSIDs created in previous versions having trailing spaces are recognized. Trailing spaces make it appear that you have identical SSIDs configured on the same access point. If you think identical SSIDs are on the access point, use the **show dot11 associations** privileged EXEC command to check any SSIDs created in a previous release for trailing spaces.

For example, this sample output from a **show configuration** privileged EXEC command does not show spaces in SSIDs:

```
ssid buffalo
    vlan 77
    authentication open

ssid buffalo
    vlan 17
    authentication open

ssid buffalo
    vlan 7
    authentication open
```

However, this sample output from a **show dot11 associations** privileged EXEC command shows the spaces in the SSIDs:

```
SSID [buffalo] :
SSID [buffalo ] :
SSID [buffalo  ] :
```

Using a RADIUS Server to Restrict SSIDs

To prevent client devices from associating to the access point using an unauthorized SSID, you can create a list of authorized SSIDs that clients must use on your RADIUS authentication server.

The SSID authorization process consists of these steps:

1. A client device associates to the access point using any SSID configured on the access point.
2. The client begins RADIUS authentication.
3. The RADIUS server returns a list of SSIDs that the client is allowed to use. The access point checks the list for a match of the SSID used by the client. There are three possible outcomes:
   a. If the SSID that the client used to associate to the access point matches an entry in the allowed list returned by the RADIUS server, the client is allowed network access after completing all authentication requirements.
   b. If the access point does not find a match for the client in the allowed list of SSIDs, the access point disassociates the client.
   c. If the RADIUS server does not return any SSIDs (no list) for the client, then the administrator has not configured the list, and the client is allowed to associate and attempt to authenticate.

The allowed list of SSIDs from the RADIUS server are in the form of Cisco VSAs. The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the access point and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named *cisco-avpair*. The Radius server is allowed to have zero or more SSID VSAs per client.

In this example, the following AV pair adds the SSID *batman* to the list of allowed SSIDs for a user:

```
cisco-avpair= "ssid=batman"
```

For instructions on configuring the access point to recognize and use VSAs, see the "Configuring the Access Point to Use Vendor-Specific RADIUS Attributes" section on page 7-14.

Configuring Multiple Basic SSIDs

Access point 802.11a and 802.11g radios now support up to 8 basic SSIDs (BSSIDs), which are similar to MAC addresses. You use multiple BSSIDs to assign a unique DTIM setting for each SSID and to broadcast more than one SSID in beacons. A large DTIM value increases battery life for power-save client devices that use an SSID, and broadcasting multiple SSIDs makes your wireless LAN more accessible to guests.

Note Devices on your wireless LAN that are configured to associate to a specific access point based on the access point MAC address (for example, client devices, repeaters, hot standby units, or workgroup bridges) might lose their association when you add or delete a multiple BSSID. When you add or delete a multiple BSSID, check the association status of devices configured to associate to a specific access point. If necessary, reconfigure the disassociated device to use the BSSID's new MAC address.

Requirements for Configuring Multiple BSSIDs

To configure multiple BSSIDs, your access points must meet these minimum requirements:

- VLANs must be configured
- Access points must run Cisco IOS Release 12.4(15)T or later
- Access points must contain an 802.11a or 802.11g radio that supports multiple BSSIDs. To determine whether a radio supports multiple basic SSIDs, enter the **show controllers** *radio_interface* command. The radio supports multiple basic SSIDs if the results include this line:

  ```
  Number of supported simultaneous BSSID on radio_interface: 8
  ```

Guidelines for Using Multiple BSSIDs

Keep these guidelines in mind when configuring multiple BSSIDs:

- RADIUS-assigned VLANs are not supported when you enable multiple BSSIDs.
- When you enable BSSIDs, the access point automatically maps a BSSID to each SSID. You cannot manually map a BSSID to a specific SSID.

- When multiple BSSIDs are enabled on the access point, the SSIDL IE does not contain a list of SSIDs; it contains only extended capabilities.
- Any Wi-Fi certified client device can associate to an access point using multiple BSSIDs.
- You can enable multiple BSSIDs on access points that participate in WDS.

CLI Configuration Example

This example shows the CLI commands that you use to enable multiple BSSIDs on a radio interface, create an SSID called *visitor*, designate the SSID as a BSSID, specify that the BSSID is included in beacons, set a DTIM period for the BSSID, and assign the SSID *visitor* to the radio interface:

```
router(config)# interface dot11 0
router(config-if)# mbssid
router(config-if)# exit
router(config)# dot11 ssid visitor
router(config-ssid)# mbssid guest-mode
router(config-ssid)# exit
router(config)# interface dot11 0
router(config-if)# ssid visitor
```

You can also use the **dot11 mbssid** global configuration command to simultaneously enable multiple BSSIDs on all radio interfaces that support multiple BSSIDs.

Displaying Configured BSSIDs

Use the **show dot11 bssid** privileged EXEC command to display the relationship between SSIDs and BSSIDs or MAC addresses. This example shows the command output:

```
router1230#show dot11 bssid
Interface     BSSID           Guest  SSID
Dot11Radio1   0011.2161.b7c0  Yes  atlantic
Dot11Radio0   0005.9a3e.7c0f  Yes  WPA2-TLS-g
```

Enabling MBSSID and SSIDL at the same time

When multiple BSSIDs are enabled on the access point, the SSIDL IE does not contain a list of SSIDs; it contains only extended capabilities.

Beginning in privileged EXEC mode, follow these steps to include an SSID in an SSIDL IE:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface.
Step 3	**ssid** *ssid-string*	Enter configuration mode for a specific SSID.
Step 4	**information-element ssidl** [**advertisement**] [**wps**]	Include an SSIDL IE in the access point beacon that advertises the access point's extended capabilities, such as 802.1x and support for Microsoft Wireless Provisioning Services (WPS). Use the **advertisement** option to include the SSID name and capabilities in the SSIDL IE. Use the **wps** option to set the WPS capability flag in the SSIDL IE.

Use the **no** form of the command to disable SSIDL IEs.

Sample Configuration for Enabling MBSSID and SSIDL

Below is a sample configuration for enabling MBSSID:

```
dot11 ssid 181x_gvlan01
   vlan 1
   authentication open
   mbssid guest-mode
!
dot11 ssid 181x_gvlan02
   vlan 2
   authentication open
   wpa-psk ascii 0 12345678
   mbssid guest-mode
!
dot11 ssid 181x_gvlan03
   vlan 3
   authentication open
   authentication key-management wpa
   wpa-psk ascii 0 12345678
!
dot11 ssid 181x_gvlan04
   vlan 4
   authentication open
   authentication key-management wpa
   wpa-psk ascii 0 12345678
!
interface Dot11Radio0
 no ip address
 !
 encryption vlan 1 key 1 size 40bit 0 1234567890 transmit-key
 encryption vlan 1 mode ciphers wep40
 !
 encryption vlan 2 mode ciphers tkip
 !
 encryption vlan 3 mode ciphers tkip
 !
 encryption vlan 4 mode ciphers tkip
 !
 ssid 181x_gvlan01
 !
 ssid 181x_gvlan02
 !
 ssid 181x_gvlan03
 !
 ssid 181x_gvlan04
 !
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 mbssid
 station-role root
!
```

Below is a sample configuration for enabling SSIDL:

```
dot11 ssid 1841-wep128
   vlan 1
   authentication open
   information-element ssidl advertisement
```

```
!
dot11 ssid 1841-tkip-psk
   vlan 2
   authentication open
   authentication key-management wpa
   wpa-psk ascii 0 12345678
   information-element ssidl advertisement
!
dot11 ssid 1841-aes-psk
   vlan 3
   authentication open
   authentication key-management wpa
   wpa-psk ascii 0 12345678
   information-element ssidl advertisement wps
!
interface Dot11Radio0/0/0
 no ip address
 no snmp trap link-status
 !
 encryption vlan 1 key 1 size 128bit 0 12345678901234567890123456 transmit-key
 encryption vlan 1 key 2 size 128bit 0 12345678901234567890123456
 encryption vlan 1 mode ciphers wep128
 !
 encryption vlan 2 mode ciphers tkip
 !
 encryption vlan 3 mode ciphers aes-ccm
 !
 ssid 1841-wep128
 !
 ssid 1841-tkip-psk
 !
 ssid 1841-aes-psk
 !
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 station-role root
```