C H A P T E R 7

Configuring Multiple SSIDs

This chapter describes how to configure and manage multiple service set identifiers (SSIDs) on the access point/bridge. This chapter contains these 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 sub-network 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 access point/bridge 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/bridge 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 10, "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/bridge 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/bridge includes the guest SSID in its beacon. The default SSID, *tsunami*, is set to guest mode. However, to keep your network secure, you should disable the guest mode SSID.

If your access point/bridge 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.

Effect of Software Versions on SSIDs

Cisco introduced global-mode SSID configuration in Cisco IOS Release 12.3(2)JA to simplify configuration of SSID parameters under multiple interfaces. Configuration of SSID parameters at the interface level was supported in Cisco IOS Release 12.3(2)JA release for backward compatibility, but configuration of SSID parameters at the interface level will be totally disabled in releases after Cisco IOS Release 12.3(4)JA. Table 7-1 lists the SSID configuration methods supported in Cisco IOS Releases.

Table 7-1   SSID Configuration Methods Supported in Cisco IOS Releases

Cisco IOS Release	Supported SSID Configuration Method
12.2(15)JA	Interface-level only
12.3(2)JA	Both interface-level and global

Table 7-1   SSID Configuration Methods Supported in Cisco IOS Releases (continued)

Cisco IOS Release	Supported SSID Configuration Method
12.3(4)JA and 12.3(7)JA	Both interface-level and global; all SSIDs saved in global mode
post-12.3(4)JA	Global only

Cisco IOS Release 12.3(7)JA 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 12.3(7)JA.

If you need to upgrade from Cisco IOS Release 12.3(2)JA or earlier to a release later than 12.3(4)JA, you should first upgrade to Cisco IOS Release 12.3(4)JA, 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 a pre-12.3(4)JA release to a post-12.3(4)JA release, your interface-level SSID configuration is deleted.

If you downgrade the software version from Cisco IOS Release 12.3(7)JA, any SSIDs that you created become invalid. To avoid reconfiguring the SSIDs after a downgrade, save a copy of a configuration file in an earlier software version before you upgrade to Cisco IOS Release 12.3(7)JA; if you downgrade software versions from Cisco IOS Release 12.3(7)JA, load the saved configuration file after the downgrade.

Table 7-2 shows an example SSID configuration on an access point/bridge running Cisco IOS Release 12.2(15)JA and the configuration as it appears after upgrading to Cisco IOS Release 12.3(7)JA.

Table 7-2   Example: SSID Configuration Converted to Global Mode After Upgrade

SSID Configuration in 12.2(15)JA	SSID Configuration After Upgrade to 12.3(7)JA
| ```
interface dot11Radio 0
   ssid engineering
   authentication open
   vlan 4

interface dot11Radio 1
  ssid engineering
   authentication open
   vlan 5
``` | ```
dot11 ssid engineering
  authentication open
  vlan 5
!
interface dot11Radio 0
  ssid engineering

interface dot11Radio 1
   ssid engineering
``` |

Note that the VLAN configuration under each interface is retained in the global SSID configuration.

Note   SSIDs, VLANs, and encryption schemes are mapped together on a one-to-one-to-one basis; one SSID can be mapped to one VLAN, and one VLAN can be mapped to one encryption scheme. When using a global SSID configuration, you cannot configure one SSID with two different encryption schemes. For example, you cannot apply SSID *north* with TKIP on interface dot11 0 and also apply SSID *north* with WEP128 on interface dot11 1.

Configuring Multiple SSIDs

These sections contain configuration information for multiple SSIDs:

> **Note** In Cisco IOS Release 12.3(4)JA 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 7-4 to configure SSIDs globally.

Default SSID Configuration

In Cisco IOS Release 12.3(7)JA there is no default SSID. You must configure a minimum of one SSID to establish a Wireless LAN connection. This section explains how to configure the SSID globally.

Creating an SSID Globally

In Cisco IOS Releases 12.3(2)JA 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.

	Command	Purpose
Step 3	**authentication client** **username** *username* **password** *password*	(Optional) Set an authentication username and password that the access point/bridge 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/en/US/docs/ios/12_2/security/configuration/guide/scfacct.html
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/bridge's guest-mode SSID. The access point/bridge 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**	Enter interface configuration mode for the radio interface to which you want to assign the SSID.
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 10, "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

```
AP# configure terminal
AP(config)# dot11 ssid batman
```

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

Viewing SSIDs Configured Globally

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

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

Using Spaces in SSIDs

In Cisco IOS Release 12.3(7)JA, 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/bridge 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 poin/bridget using any SSID configured on the access point/bridge.
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/bridge 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/bridge 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/bridge does not find a match for the client in the allowed list of SSIDs, the access point/bridge 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/bridge 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/bridge to recognize and use VSAs, see Chapter 12 of the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

Configuring Multiple Basic SSIDs

Access point 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 point/bridge must meet these minimum requirements:

- VLANs must be configured
- The access point/bridge must run Cisco IOS Release 12.3(4)JA or later
- The access point/bridge must contain an 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/bridge 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/bridge, 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/bridge using multiple BSSIDs.

- You can enable multiple BSSIDs on access point/bridges that participate in WDS.

Configuring Multiple BSSIDs

Follow these steps to configure multiple BSSIDs:

Step 1 Browse to the Global SSID Manager page on the access point GUI. (If you use the CLI instead of the GUI, refer to the CLI commands listed in the CLI Configuration Example at the end of this section.) Figure 7-1 shows the top portion of the Global SSID Manager page.

Figure 7-1   Global SSID Manager Page

Step 2   Enter the SSID name in the **SSID** field.

Step 3   Use the **VLAN** drop-down menu to select the VLAN to which the SSID is assigned.

Step 4   Select the radio interfaces on which the SSID is enabled. The SSID remains inactive until you enable it for a radio interface.

Step 5   Enter a Network ID for the SSID in the **Network ID** field.

Step 6   Assign authentication, authenticated key management, and accounting settings to the SSID in the Authentication Settings, Authenticated Key Management, and Accounting Settings sections of the page. BSSIDs support all the authentication types that are supported on SSIDs.

Step 7   (Optional) In the Multiple BSSID Beacon Settings section, select the **Set SSID as Guest Mode** check box to include the SSID in beacons.

Step 8   (Optional) To increase the battery life for power-save clients that use this SSID, select the **Set Data Beacon Rate (DTIM)** check box and enter a beacon rate for the SSID. The beacon rate determines how often the access point sends a beacon containing a Delivery Traffic Indicator Message (DTIM).

When client devices receive a beacon that contains a DTIM, they normally wake up to check for pending packets. Longer intervals between DTIMs let clients sleep longer and preserve power. Conversely, shorter DTIM periods reduce the delay in receiving packets but use more battery power because clients wake up more often.

The default beacon rate is 2, which means that every other beacon contains a DTIM. Enter a beacon rate between 1 and 100.

✎
Note   Increasing the DTIM period count delays the delivery of multicast packets. Because multicast packets are buffered, large DTIM period counts can cause a buffer overflow.

Step 9   In the Guest Mode/Infrastructure SSID Settings section, select **Multiple BSSID**.

Step 10   Click **Apply**.

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:

```
ap(config)# interface d0
ap(config-if)# mbssid
ap(config-if)# exit
ap(config)# dot11 ssid visitor
ap(config-ssid)# mbssid guest-mode dtim-period 75
ap(config-ssid)# exit
ap(config)# interface d0
ap(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:

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

Assigning IP Redirection for an SSID

When you configure IP redirection for an SSID, the access point/bridge redirects all packets sent from client devices associated to that SSID to a specific IP address. IP redirection is used mainly on wireless LANs serving handheld devices that use a central software application and are statically configured to communicate with a specific IP address. For example, the wireless LAN administrator at a retail store or warehouse might configure IP redirection for its bar code scanners, which all use the same scanner application and all send data to the same IP address.
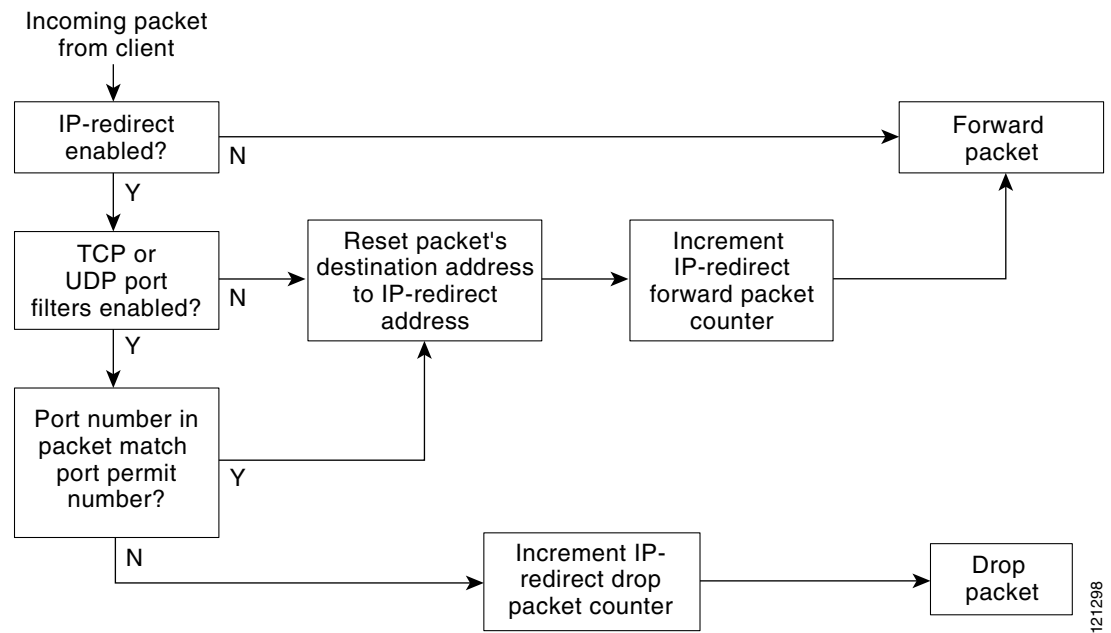
You can redirect all packets from client devices associated using an SSID or redirect only packets directed to specific TCP or UDP ports (as defined in an access control list). When you configure the access point/bridge to redirect only packets addressed to specific ports, the access point/bridge redirects those packets from clients using the SSID and drops all other packets from clients using the SSID.

Note   When you perform a ping test from the access point/bridge to a client device that is associated using an IP-redirect SSID, the response packets from the client are redirected to the specified IP address and are not received by the access point/bridge.

Figure 7-2 shows the processing flow that occurs when the access point/bridge receives client packets from clients associated using an IP-redirect SSID.

Figure 7-2   Processing Flow for IP Redirection

Guidelines for Using IP Redirection

Keep these guidelines in mind when using IP redirection:

- The access point/bridge does not redirect broadcast, unicast, or multicast BOOTP/DHCP packets received from client devices.
- Existing ACL filters for incoming packets take precedence over IP redirection.

Configuring IP Redirection

Beginning in privileged EXEC mode, follow these steps to configure IP redirection for an SSID:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio 0**	Enter interface configuration mode for the radio interface.
Step 3	**ssid** *ssid-string*	Enter configuration mode for a specific SSID.

	Command	Purpose
Step 4	**ip redirection host** *ip-address*	Enter IP redirect configuration mode for the IP address. Enter the IP address with decimals, as in this example: 10.91.104.92
		If you do not specify an access control list (ACL) which defines TCP or UDP ports for redirection, the access point/bridge redirects all packets that it receives from client devices.
Step 5	**ip redirection host** *ip-address* **access-group** *acl* **in**	(Optional) Specify an ACL to apply to the redirection of packets. Only packets sent to the specific UDP or TCP ports defined in the ACL are redirected. The access point/bridge discards all received packets that do not match the settings defined in the ACL. The **in** parameter specifies that the ACL is applied to the access point/bridge's incoming interface.

This example shows how to configure IP redirection for an SSID without applying an ACL. The access point/bridge redirects all packets that it receives from client devices associated to the SSID *batman*:

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# ssid batman
sp(config-if-ssid)# ip redirection host 10.91.104.91
sp(config-if-ssid-redirect)# end
```

This example shows how to configure IP redirection only for packets sent to the specific TCP and UDP ports specified in an ACL. When the access point receives packets from client devices associated using the SSID *robin*, it redirects packets sent to the specified ports and discards all other packets:

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# ssid robin
ap(config-if-ssid)# ip redirection host 10.91.104.91 access-group redirect-acl in
ap(config-if-ssid)# end
```

Including an SSID in an SSIDL IE

The access point/bridge beacon can advertise only one broadcast SSID. However, you can use SSIDL information elements (SSIDL IEs) in the access point/bridge beacon to alert client devices of additional SSIDs on the access point/bridge. When you designate an SSID to be included in an SSIDL IE, client devices detect that the SSID is available, and they also detect the security settings required to associate using that SSID.

Note When multiple BSSIDs are enabled on the access point/bridge, 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**	Enter interface configuration mode for the radio interface.

	Command	Purpose
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/bridge beacon that advertises the access point/bridge'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.