



## Configuring Multiple SSIDs

---

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

- [Understanding Multiple SSIDs, page 4-2](#)
- [Configuring Multiple SSIDs, page 4-2](#)
- [Assigning IP Redirection for an SSID, page 4-7](#)
- [Including an SSID in an SSIDL IE, page 4-9](#)

# 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 1200 series access point 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 7, “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. The access point’s default SSID, *tsunami*, is set to guest mode. However, to keep your network secure, you should disable the guest mode SSID on most access points.

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.

# Configuring Multiple SSIDs

These sections contain configuration information for multiple SSIDs:

- [Default SSID Configuration, page 4-3](#)
- [Creating an SSID Globally, page 4-3](#)
- [Using a RADIUS Server to Restrict SSIDs, page 4-7](#)



**Note**

---

In Cisco IOS Release 12.3(2)JA, you can configure SSIDs globally or for a specific radio interface. Follow the instructions in the [“Creating an SSID Globally”](#) section on page 4-3 to configure SSIDs globally. Follow the instructions in the [“Creating an Interface-Specific SSID”](#) section on page 4-5 to configure SSIDs for a specific interface.

---

## Default SSID Configuration

Table 4-1 shows the default SSID configuration:

**Table 4-1 Default SSID Configuration**

Feature	Default Setting
SSID	tsunami
Guest Mode SSID	tsunami (The access point broadcasts this SSID in its beacon and allows client devices with no SSID to associate.)

## Creating an SSID Globally

In Cisco IOS Release 12.3(2)JA, 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** When you create an SSID in global configuration mode, you can assign or change the SSID attributes only in global configuration mode. Similarly, when you create an SSID in configuration interface mode, you can assign or change the SSID attributes only in configuration interface mode.

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	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>dot11 ssid</b> <i>ssid-string</i>	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.
Step 3	<b>authentication client</b> <b>username</b> <i>username</i> <b>password</b> <i>password</i>	(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	<b>accounting</b> <i>list-name</i>	(Optional) Enable RADIUS accounting for this SSID. For <i>list-name</i> , specify the accounting method list. Click this link for more information on method lists: <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfacct.htm#xtocid2">http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfacct.htm#xtocid2</a>

	Command	Purpose
Step 5	<code>vlan <i>vlan-id</i></code>	(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	<code>guest-mode</code>	(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	<code>infrastructure-ssid [optional]</code>	(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 <b>optional</b> keyword.
Step 8	<code>interface dot11radio { 0   1 }</code>	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	<code>ssid <i>ssid-string</i></code>	Assign the global SSID that you created in <a href="#">Step 2</a> to the radio interface.
Step 10	<code>end</code>	Return to privileged EXEC mode.
Step 11	<code>copy running-config startup-config</code>	(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 7, "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
```

## Creating an Interface-Specific SSID

Beginning in privileged EXEC mode, follow these steps to create an SSID for a specific radio interface.



**Note** When you create an interface-specific SSID, you cannot change the SSID attributes in global configuration mode.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface dot11radio { 0   1 }</b>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	<b>ssid ssid-string</b>	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.
Step 4	<b>authentication client</b> <b>username username</b> <b>password password</b>	(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 5	<b>accounting list-name</b>	(Optional) Enable RADIUS accounting for this SSID. For <i>list-name</i> , specify the accounting method list. Click this link for more information on method lists: <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfacct.htm#xtocid2">http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfacct.htm#xtocid2</a>
Step 6	<b>vlan vlan-id</b>	(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 7	<b>guest-mode</b>	(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 8	<b>infrastructure-ssid [optional]</b>	(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 <b>optional</b> keyword.

	Command	Purpose
Step 9	<b>end</b>	Return to privileged EXEC mode.
Step 10	<b>copy running-config startup-config</b>	(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 7, "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

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

## Using Spaces in SSIDs

You can include spaces in an SSID, but be careful not to add spaces to an SSID accidentally, especially trailing spaces (spaces at the end of an SSID). If you add trailing spaces, it might appear that you have identical SSIDs configured on the same access point. If you think you configured identical SSIDs on the access point, use the **show dot11 associations** privileged EXEC command to check your SSIDs 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 8-14.

## Assigning IP Redirection for an SSID

When you configure IP redirection for an SSID, the access point 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.

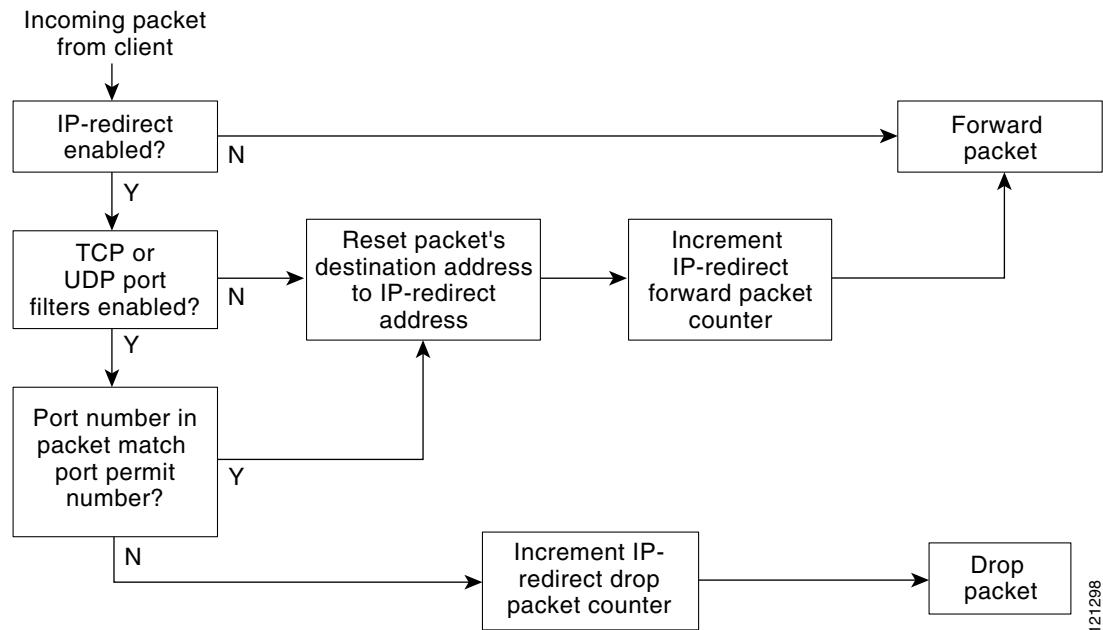
You can redirect all packets from client devices associated using an SSID or redirect only packets directed to specific TCP or UDP ports (as defined in an access control list). When you configure the access point to redirect only packets addressed to specific ports, the access point redirects those packets 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 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.

Figure 4-1 shows the processing flow that occurs when the access point receives client packets from clients associated using an IP-redirect SSID.

**Figure 4-1 Processing Flow for IP Redirection**



121298

## Guidelines for Using IP Redirection

Keep these guidelines in mind when using IP redirection:

- The access point 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	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface dot11radio { 0   1 }</code>	Enter interface configuration mode for the radio interface.
Step 3	<code>ssid ssid-string</code>	Enter configuration mode for a specific SSID.

	Command	Purpose
Step 4	<b>ip redirection host</b> <i>ip-address</i>	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 redirects all packets that it receives from client devices.
Step 5	<b>ip redirection host</b> <i>ip-address</i> <b>access-group</b> <i>acl</i> <b>in</b>	(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 discards all received packets that do not match the settings defined in the ACL. The <b>in</b> parameter specifies that the ACL is applied to the access point's incoming interface.

This example shows how to configure IP redirection for an SSID without applying an ACL. The access point 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
AP(config-if-ssid)# ip redirection host 10.91.104.91
AP(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 beacon can advertise only one broadcast SSID. However, you can use SSIDL information elements (SSIDL IEs) in the access point beacon to alert client devices of additional SSIDs on the access point. 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.

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

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface dot11radio</b> { 0   1 }	Enter interface configuration mode for the radio interface.

	Command	Purpose
Step 3	<code>ssid <i>ssid-string</i></code>	Enter configuration mode for a specific SSID.
Step 4	<code>information-element ssidl [advertisement] [wps]</code>	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 <b>advertisement</b> option to include the SSID name and capabilities in the SSIDL IE. Use the <b>wps</b> option to set the WPS capability flag in the SSIDL IE.

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