



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 7-2](#)
- [Configuring Multiple SSIDs, page 7-2](#)

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 10, “Configuring Authentication Types.”](#)

- Maximum number of client associations using the SSID
- Proxy mobile IP
- RADIUS accounting for traffic using the SSID
- Guest mode
- Repeater mode, including authentication username and password

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 7-3](#)
- [Creating an SSID, page 7-3](#)
- [Using a RADIUS Server to Restrict SSIDs, page 7-5](#)

Default SSID Configuration

Table 7-1 shows the default SSID configuration:

Table 7-1 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

Beginning in privileged EXEC mode, follow these steps to create an SSID:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio { 0 1 }	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	ssid <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 4	authentication client username <i>username</i> password <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 5	accounting <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: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfacct.htm#xtocid2
Step 6	vlan <i>vlan-id</i>	(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	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.

	Command	Purpose
Step 8	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 9	end	Return to privileged EXEC mode.
Step 10	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

```
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 12-14.

