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

-
-
-

Note

Default SSID Configuration

Creating an SSID Globally

dot11 ssid

ssid

ssid

ssid

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*	**Note** +.], ?, $, TAB, and trailing spaces are invalid characters for SSIDs.

	Command	Purpose
Step 3	**authentication client username** *username* **password** *password*	
Step 4	**accounting** *list-name*	*list-name* 122/122cgcr/fsecur_c/fsaaa/scfacct.htm#xtocid2
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**	
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**	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.

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

show running-config ssid *ssid-string*

Using Spaces in SSIDs

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 privileged EXEC command to check any SSIDs created in a previous release for trailing spaces.

For example, this sample output from a 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
```

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

Using a RADIUS Server to Restrict SSIDs

1.

2.

3.

a.

b.

c.

vendor-ID is 9, and the supported option has vendor-type 1, which is named *cisco-avpair*

batman

```
cisco-avpair= ″ssid=batman″
```

Cisco IOS Software Configuration Guide for Cisco Aironet Access Points.

Configuring Multiple Basic SSIDs

Note

Requirements for Configuring Multiple BSSIDs

-
-
-

radio_interface

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

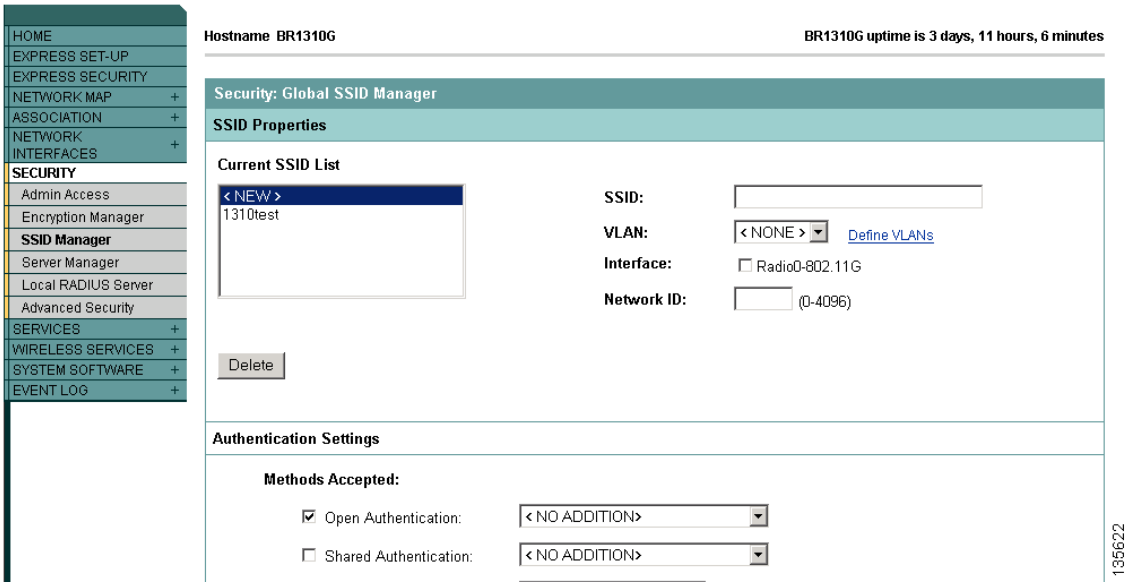
Guidelines for Using Multiple BSSIDs

-
-
-
-
-

Configuring Multiple BSSIDs

Step 1

Figure 7-1 Global SSID Manager Page



SSID

VLAN

Network ID

Set SSID as Guest Mode

Set Data

Beacon Rate (DTIM)

Multiple BSSID

Apply

CLI Configuration Example

```
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
```

dot11 mbssid

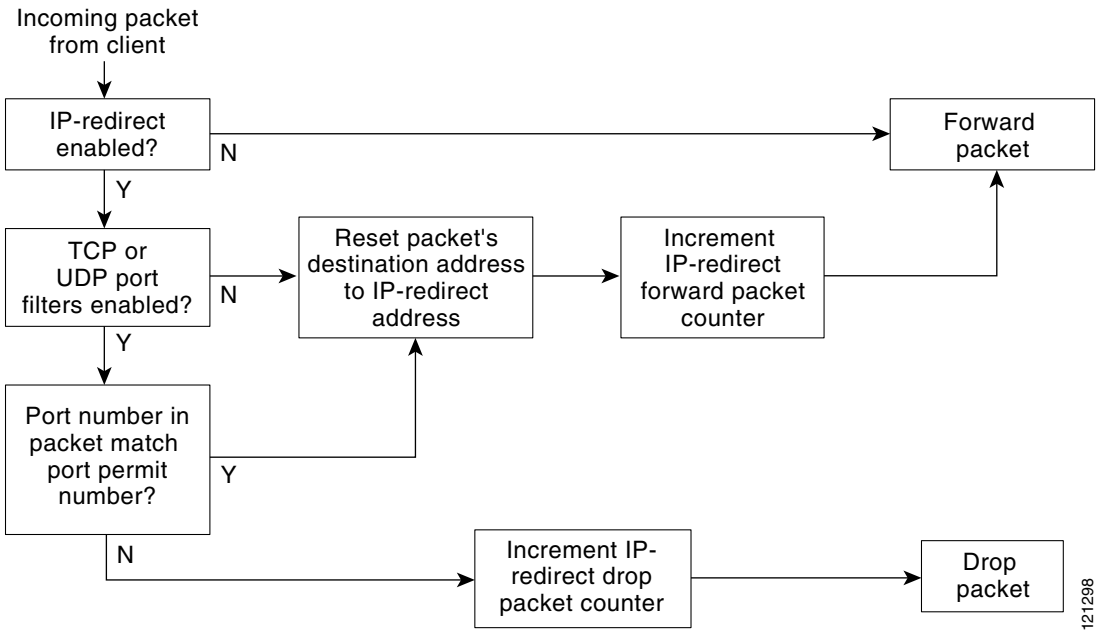
Displaying Configured BSSIDs

```
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

Note

Processing Flow for IP Redirection



Guidelines for Using IP Redirection

-
-

Configuring IP Redirection

	Command	Purpose
Step 4		
Step 5		

```
ip redirection host 10.91.104.91
          end
```

```
configure terminal
        interface dot11radio 0
           ssid robin
                ip redirection host 10.91.104.91 access-group redirect-acl in
                end
```

Including an SSID in an SSIDL IE

Note

	Command	Purpose
Step 1		
Step 2		

	Command	Purpose
Step 3		
Step 4		