CHAPTER **7**

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 an ASCII string 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.

You can configure up to 16 SSIDs on your access point and assign different configuration settings to each SSID. All the SSIDs may be 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 settings

> **Note** For detailed information on client authentication types, see Chapter 11, "Configuring Authentication Types."

- Client authenticated key management settings
- Insert AP authentication parameters (when using AP to AP links, such as bridges)
- Insert Management frame protection settings (802.11w and/or Cisco MFP)
- Maximum number of client associations using the SSID
- RADIUS accounting for traffic using the SSID
- Guest mode (defines if the SSID string should be broadcasted in the beacons
- Define legacy AP to AP authentication method, when using PSK or LEAP security in AP to AP links
- Redirection of packets received from client devices

If you want the access point SSID to be visible to all wireless clients, including clients not having a profile to that particular SSID, you can setup a guest SSID. The access point mentions the guest SSID in its beacon. If the guest mode is disabled, the AP will still send beacons for this SSID, but the SSID string will not be mentioned. If you do not want clients that do not have a preconfigured SSID, disable the guest SSID feature. Note that the SSID will still be available to clients specifically querying for that particular SSID string. Clients sending broadcast probe messages will not receive that SSID string in the AP answer, and will not see the SSID string in the AP beacons. For information on how to configure guest mode SSID and disable Guest mode SSID, see the "Creating an SSID Globally" section on page 7-3.

If your access point is intended to be a repeater or a non-root bridge, you can setup, on the repeater or non-root bridge side, credentials so that the root or primary AP can authenticate the repeater or non-root bridge. 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 each 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:

Note   You need to configure SSIDs globally and then apply them to a specific radio interface. Follow the instructions in the "Creating an SSID Globally" section on page 7-3 to configure SSIDs globally.

Creating an SSID Globally

In Cisco IOS Releases you use the **dot11 ssid** global configuration command to create an SSID, and 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. However, the parameters that you can configure from the radio interface SSID configuration mode are more limited than the parameters you can configure from the SSID global configuration 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	**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.
		The SSID can consist of up to 32 alphanumeric, case-sensitive, characters.
		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 or non-root bridge mode, and using a legacy authentication system, such as LEAP. Set the username and password on the SSID that the repeater access point uses to associate to a root access point, with another repeater or non-root bridge.
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/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfacct.html

	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 several SSIDs to the same VLAN, but you can assign each SSID to only one VLAN.
Step 6	**guest-mode**	(Optional) Designate the SSID as your access point guest-mode SSID. The access point includes the SSID in its beacon and is visible to client devices that do not specify an SSID in their probe requests.
Step 7	**infrastructure-ssid** [**optional**]	This command controls the SSID that access points and bridges use when associating with one another. A root access point only allows a repeater access point to associate using the infrastructure SSID. A root bridge only allows a non-root bridge to associate using the infrastructure SSID. Repeater access points and non-root bridges use this SSID to associate with root devices.
		The access point and bridge GUI requires the configuration of infrastructure-ssid for repeater, and non-root bridge roles. It is not mandatory to configure infrastructure SSID for workgroup bridge roles. In case you are using legacy IOS code, if you use the CLI to configure the device role, you do not have to configure an infrastructure SSID unless multiple SSIDs are configured on the radio. If multiple SSIDs are configured on the radio, you must use the infrastructure-ssid command to specify which SSID the non-root bridge uses to connect to the root bridge.
		However, from 12.4(21a)JA1 and 12.3(8)JEC release onwards, repeaters do not associate with bridges when infrastructure-ssid is not configured irrespective of the presence of single or multiple SSIDs.
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 and the 2.4-GHz 802.11n radio is 0.
		The 5-GHz radio and the 5-GHz 802.11n radio is 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 authentication options to configure an authentication type for each SSID. See Chapter 9, "Configuring an Access Point as a Local Authenticator," for instructions on configuring authentication types.

> **Note** When you enable guest SSID mode for the 802.11g radio it applies to the 802.11b radio as well since 802.11b and 802.11g operate in the same 2.4Ghz band.

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
AP(config-if)#end
```

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 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. The Cisco 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 for Vendor-Proprietary RADIUS Server Communication" section on page 13-17".

Configuring Multiple Basic SSIDs

Access point 802.11a, 802.11g, 802.11n radios support up to 16 basic SSIDs (BSSIDs). For 1130, 1240, 1300 series APs only up to 8 BSSIDs are supported. The BSSID is the radio mac address associated to a given SSID (network name) string.

You use multiple SSIDs to assign a unique DTIM setting for each SSID to broadcast one beacon per SSID. 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 new BSSID 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 12.3(4)JA or later
- To determine the number of multiple basic SSIDs supported, 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: 16
```

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 optional 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.

Configuring Multiple BSSIDs

Follow these steps to configure multiple BSSIDs (MBSSIDs):

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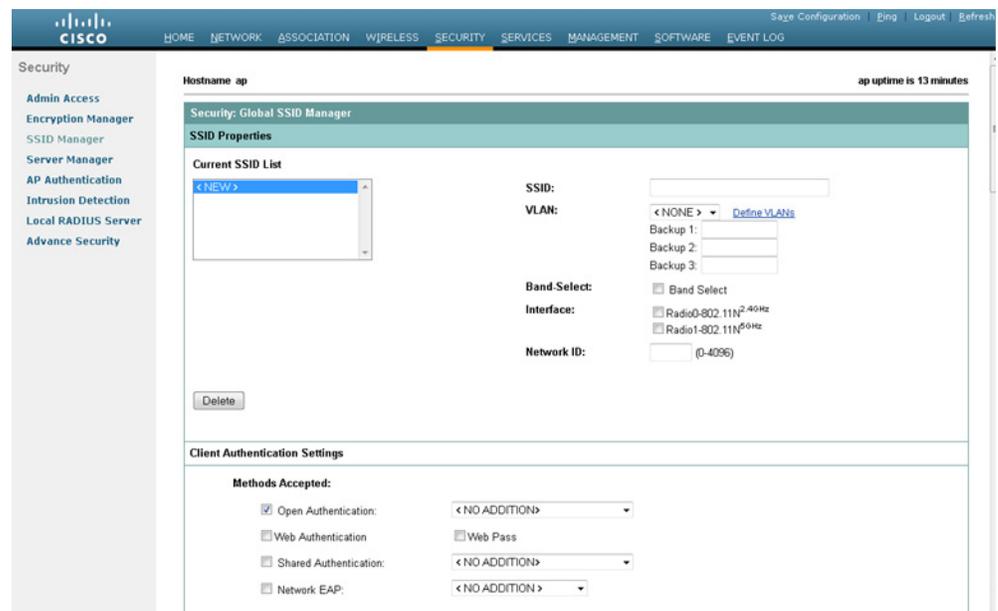
Step 2   Enter the SSID name in the **SSID** field.

Step 3   Use the **VLAN** drop-down list 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 validate the SSID settings and enable the radio interface.

Step 5   (Optional) 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. MBSSIDs 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 do0
ap(config-if)# mbssid
ap(config-if)# exit
ap(config)# dot11 ssid visitor vlan20
ap(config-ssid)# mbssid guest-mode dtim-period 3
ap(config-ssid)# exit
ap(config)# interface do0
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:

```
AP1230#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 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 7-2 shows the processing flow that occurs when the access point receives client packets from clients associated using an IP-redirect SSID.

Figure 7-2   Processing Flow for IP Redirection
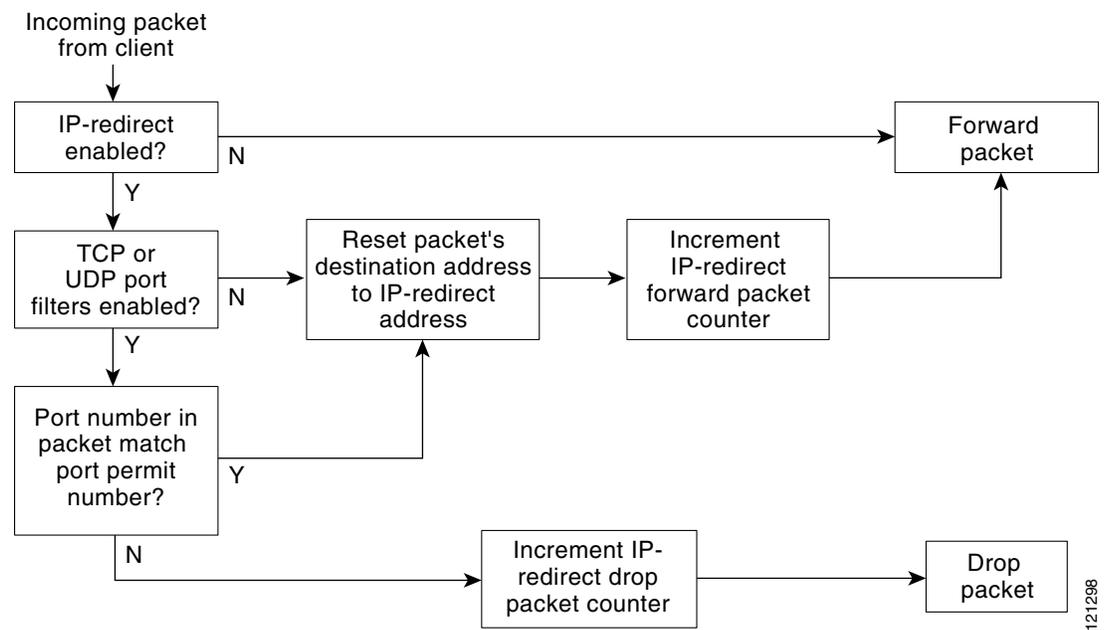
Guidelines for Using IP Redirection

Keep these guidelines in mind when using IP redirection:

- The access point 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	**dot11 ssid** *ssid-string*	Enter configuration mode for a specific SSID.
Step 3	**ip redirection host** *ip-address*	Enter IP redirect configuration mode for the IP address. Enter the IP address with decimals, for 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 4	**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 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 incoming interface for the access point.

Note ACL logging is not supported on the bridging interfaces of access point platforms. When applied on a bridging interface, it works as if the interface were configured without the log option, and logging does not take effect. However ACL logging does work for the BVI interfaces as long as a separate ACL is used for the BVI 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)# dot11 ssid batman
AP(config-if-ssid)# ip redirection host 10.91.104.91
AP(config-if-ssid-redirect)# end
```

Including SSIDL IE in an SSID Beacon

The access point broadcasts one beacon per SSID. By default, only one of the SSID beacons will mention the relevant SSID name. The beacons for the other SSIDs on the same radio leave the SSID field empty, unless you use the MBSSID feature.

Note 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 SSIDL IE in an SSID beacon:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 ssid** *ssid-string*	Enter configuration mode for a specific SSID. You are recommended to choose the SSID that is set to guest-mode (i.e. advertises its SSID string into its beacon)
Step 3	**information-element ssidl** [**advertisement**] [**wps**]	Include an SSIDL IE in the access point beacon that advertises the extended capabilities for the access point, 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. By default SSIDL IEs are disabled.

NAC Support for MBSSID

Networks must be protected from security threats, such as viruses, worms, and spyware. These security threats disrupt business, causing downtime and continual patching. Endpoint visibility and control is needed to help ensure that all wired and wireless devices attempting to access a network meet corporate security policies. Infected or vulnerable endpoints need to be automatically detected, isolated, and cleaned.

NAC is designed specifically to help ensure that all wired and wireless endpoint devices (such as PCs, laptops, servers, and PDAs) accessing network resources are adequately protected from security threats. NAC allows organizations to analyze and control all devices coming into the network. By ensuring that every endpoint device complies with corporate security policy and is running the latest and most relevant security protections, organizations can significantly reduce or eliminate endpoint devices as a common source of infection or network compromise.

WLANs need to be protected from security threats such as viruses, worms, and spyware. Both the NAC Appliance and the NAC Framework provide security threat protection for WLANs by enforcing device security policy compliance when WLAN clients attempt to access the network. These solutions quarantine non-compliant WLAN clients and provide remediation services to help ensure compliance.

A client, based on its health (software version, virus version, and so on) is placed on a separate VLAN that is specified to download the required software to upgrade the client to the software versions required to access the network. Four VLANs are specified for NAC support, one of which is the normal VLAN where clients having the correct software version are placed. The other VLANs are reserved for specific quarantine action and all infected clients are placed on one of these VLANs until the client is upgraded.

Each SSID has up to 3 additional VLANs configured as "unhealthy" VLANs. Infected clients are placed on one of these VLANs, based on how the client is infected. When a client sends an association request, it includes its infected status in the request to the RADIUS server. The policy to place the client on a specific VLAN is provisioned on the RADIUS server.

When an infected client associates with an access point and sends its state to the RADIUS server, the RADIUS server puts it into one of the quarantine VLANs based on its health. This VLAN is sent in the RADIUS server Access Accept response during the dot1x client authentication process. If the client is healthy and NAC compliant, the RADIUS server returns a normal VLAN assignment for the SSID and the client is placed in the correct VLAN and BSSID.

Each SSID is assigned a normal VLAN, which is the VLAN on which healthy clients are placed. The SSID can also be configured to have up to 3 backup VLANs that correspond to the quarantine VLANs on which clients are placed based on their state of health. These VLANs for the SSID use the same BSSID as assigned by the MBSSID for the SSID.

The configured VLANs are different and no VLAN overlap within an SSID is allowed. Therefore, a VLAN can be specified once and cannot be part of 2 different SSIDs per interface.

Quarantine VLANs are automatically configured under the interface on which the normal VLAN is configured. A quarantine VLAN inherits the same encryption properties as that of the normal VLAN. VLANs have the same key/authentication type and the keys for the quarantine VLANs are derived automatically.

Dot11 sub-interfaces are generated and configured automatically along with the dot1q encapsulation VLAN (equal to the number of configured VLANs). The sub-interfaces on the wired side is also configured automatically along with the bridge-group configurations under the Gigabit Ethernet 0 sub-interface.

When a client associates and the RADIUS server determines that it is unhealthy, the server returns one of the quarantine NAC VLANs in its RADIUS authentication response for dot1x authentication. This VLAN should be one of the configured backup VLANs under the client SSID. If the VLAN is not one of the configured backup VLANs, the client is disassociated.

Data corresponding to the all the backup VLANs are sent and received using the BSSID that is assigned to the SSID. Therefore, all clients (healthy and unhealthy) listening to the BSSID corresponding the the SSID wake up. Based on the multicast key being used corresponding to the VLAN (healthy or unhealthy), packet decrypting takes place on the client. Wired side traffic is segregated because different VLANs are used, thereby ensuring that traffic from infected and uninfected clients do not mix.

A new keyword, **backup**, is added to the existing **vlan** *<name>* | *<id>* under **dot11 ssid** *<ssid>* as described below:

```
vlan <name>|<id> [backup <name>|<id>, <name>|<id>, <name>|<id>
```
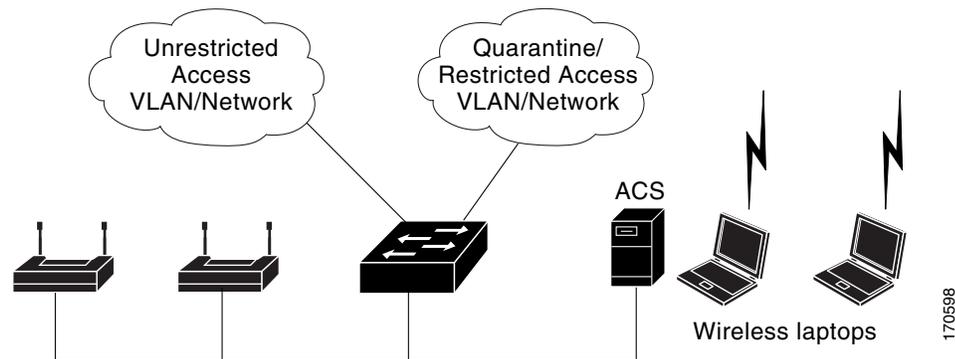
Configuring NAC for MBSSID

✎
Note   This feature supports only Layer 2 mobility within VLANs. Layer 3 mobility using network ID is not supported in this feature.

✎
Note   Before you attempt to enable NAC for MBSSID on your access points, you should first have NAC working properly. Figure 7-3 shows a typical network setup.

Figure 7-3   Typical NAC Network Setup

For additional information, see the documentation for deploying NAC for Cisco wireless networks.

Follow these steps to configure NAC for MBSSID on your access point:

Step 1   Configure your network as shown in Figure 7-3.

Step 2   Configure standalone access points and NAC-enabled client-EAP authentication.

Step 3   Configure the local profiles on the ACS server for posture validation.

Step 4   Configure the client and access point to allow the client to successful authenticate using EAP-FAST.

Step 5   Ensure that the client posture is valid.

Step 6   Verify that the client associates to the access point and that the client is placed on the unrestricted VLAN after successful authentication and posture validation.

A sample configuration is shown below.

```
dot11 mbssid
dot11 vlan-name engg-normal vlan 100
dot11 vlan-name engg-infected vlan 102
dot11 vlan-name mktg-normal vlan 101
dot11 vlan-name mktg-infected1 vlan 103
dot11 vlan-name mktg-infected2 vlan 104
dot11 vlan-name mktg-infected3 vlan 105
!
dot11 ssid engg
   vlan engg-normal backup engg-infected
```

```
        authentication open
        authentication network-eap eap_methods
    !
    dot11 ssid mktg
        vlan mktg-normal backup mktg-infected1, mktg-infected2, mktg-infected3
        authentication open
        authentication network-eap eap_methods
    !
    interface Dot11Radio0
    !
    encryption vlan engg-normal key 1 size 40bit 7 482CC74122FD transmit-key
    encryption vlan engg-normal mode ciphers wep40
    !
    encryption vlan mktg-normal key 1 size 40bit 7 9C3A6F2CBFBC transmit-key
    encryption vlan mktg-normal mode ciphers wep40
    !
    ssid engg
    !
    ssid mktg
    !
    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
    !
    interface Dot11Radio0.100
    encapsulation dot1Q 100 native
    no ip route-cache
    bridge-group 1
    bridge-group 1 subscriber-loop-control
    bridge-group 1 block-unknown-source
    no bridge-group 1 source-learning
    no bridge-group 1 unicast-flooding
    bridge-group 1 spanning-disabled
    !
    interface Dot11Radio0.102
    encapsulation dot1Q 102
    no ip route-cache
    bridge-group 102
    bridge-group 102 subscriber-loop-control
    bridge-group 102 block-unknown-source
    no bridge-group 102 source-learning
    no bridge-group 102 unicast-flooding
    bridge-group 102 spanning-disabled
    !
    interface FastEthernet0
    no ip address
    no ip route-cache
    duplex auto
    speed auto
    !
    interface FastEthernet0.100
    encapsulation dot1Q 100 native
    no ip route-cache
    bridge-group 1
    no bridge-group 1 source-learning
    bridge-group 1 spanning-disabled
    !
    interface FastEthernet0.102
    encapsulation dot1Q 102
    no ip route-cache
    bridge-group 102
    no bridge-group 102 source-learning
    bridge-group 102 spanning-disabled
    !
```